UNIVERZITA KARLOVA

Právnická fakulta

Veronika Hájková

Využití systémů na rozpoznávání obličeje k identifikaci pachatelů trestných činů

Diplomová práce

Vedoucí diplomové práce: JUDr. Martin Richter, Ph.D.

Katedra trestního práva

Datum vypracování práce (uzavření rukopisu): 04.10.2024

Prohlašuji, že jsem předkládanou diplomovou práci vypracovala samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 150 284 znaků včetně mezer.

V Ostravě dne 4.10.2024 Veronika Hájková

Poděkování

Ráda bych poděkovala panu JUDr. Martinu Richterovi, Ph.D. za vedení mé práce a cenné rady během konzultací. Také děkuji své rodině a partnerovi, bez jejichž podpory bych tuto práci nemohla dokončit

Obsah

Seznam použitých zkratek

AI	Umělá inteligence
Akt o AI	Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci)
ESLP	Evropský soud pro lidská práv
EU	Evropská Unie
FR systém	Systém rozpoznávající obličeje
GDPR	Nařízení Evropského parlamentu a Rady (EU) č. 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
Listina	Listina základních práv a svobod vyhlášená usnesením č. 2/1993 Sb. jako součást ústavního pořádku České republiky
OČTŘ	Orgány činné v trestním řízení
Policie	Policie České republiky
TRŘ	Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
Úmluva	Úmluva o ochraně lidských práv a základních svobod, sdělení č. 209/1992 Sb.

Úvod

V posledních letech jsme svědky rychlého rozvoje technologií spojených s AI. Jednou z klíčových oblastí, která získává čím dál více pozornosti, jsou FR systémy založené na principech strojového učení a analýze obrazových dat. Tyto systémy představují zásadní inovaci v oblasti automatizovaného zpracování biometrických údajů, konkrétně pak v oblasti identifikace osob na základě jejich obličejových rysů. Ačkoli FR systémy mohou přinášet významné přínosy v mnoha oblastech, jejich užívání však s sebou přináší spoustu otázek, na které by měla právní úprava reagovat. Tato technologie nachází uplatnění v celé řadě odvětví. V komerčním sektoru je používána například k odemykání chytrých telefonů či personalizaci služeb. V oblasti dopravy ji využívají letiště a hromadná doprava pro automatizovanou kontrolu totožnosti cestujících.

Jednou z klíčových oblastí, kde FR systémy získávají na významu, je prevence kriminality, bezpečnost a vyšetřování trestné činnosti. Policie a bezpečnostní složky po celém světě stále častěji využívají FR systémy pro svůj potenciál zefektivnit proces pátrání po osobách a vyšetřování trestných činů. V současné době je FR systém využíván také Policií České republiky. Otázka legálnosti využívání FR systémů Policií je v současné době velmi aktuálním a kontroverzním tématem, které zasluhuje pozornost jak z technického, tak zejména z právního hlediska, jelikož česká právní úprava přímo neupravuje ani nezmiňuje možnost užití FR systémů. Největší obavy vyvolává otázka, zdali je užívání FR systémů v souladu s právními předpisy České republiky, zejména vzhledem k zásahu do práva na soukromí a ochraně před neodůvodněnými zásahy ze strany státních orgánů. Identifikace osob za pomocí FR systémů mimo jiné zahrnuje rozsáhlé zpracovávání biometrických údajů, které s sebou přináší riziko zneužití tohoto systému spolu s rizikem zneužití těchto dat, a proto je nezbytné, aby právní úprava na tuto problematiku adekvátně reagovala.

Pro aktuálnost této problematiky jsem si zvolila téma diplomové práce *Využití systémů na rozpoznávání obličeje k identifikaci pachatelů trestných činů*. Konkrétně se pak v této práci budu snažit odpovědět na výzkumnou otázku: *Je užívání systémů na rozpoznávání obličeje Policií České republiky v souladu s českým právním řádem?* Tuto otázku budu ve své práci zkoumat z několika perspektiv, konkrétně v návaznosti na různé způsoby využití FR systémů.

Ačkoli technologie může výrazně přispět k efektivitě práce Policie, není vyloučeno, že její užívání může vést k nepřiměřenému zásahu do základních práv jednotlivců. Je proto třeba stanovit jasné a přehledné hranice, za jakých podmínek a jakým způsobem mohou být FR

systémy používány. Proto se v této práci zaměřím nejen na trestněprávní úpravu, ale také ústavní a mezinárodní závazky České republiky.

První kapitola této práce bude věnována teoretickému základu fungování FR systémů. Vysvětlím zde, jaké principy AI a biometrické identifikace se u těchto technologií využívají, jak probíhá proces identifikace či verifikace a jaké technické a vědecké principy stojí za přesností a spolehlivostí těchto systémů. Druhá kapitola se zaměří na praktické využití FR systémů v České republice. Zároveň se podívám na to, jak jsou tyto technologie používány v zahraničí, přičemž na konkrétních případech ukážu, jak mohou tyto systémy představovat efektivní, ale zároveň velmi nebezpečný nástroj, pokud nejsou dostatečně regulovány v návaznost na ochranu základních práv a svobod. Třetí kapitola bude věnována využití FR systémů k vyhledávání osob v kontextu české právní úpravy, zejména zákona o Policii České republiky. Klíčovým tématem této části bude také proporcionalita užití této technologie ve vztahu k ochraně základních práv a svobod. Ve čtvrté kapitole se zaměřím na problematiku vyhledávání a zajištění důkazů pomocí FR systémů. Představím, jaké právní požadavky musí být splněny, aby bylo možné využít FR systémy k vyhledávání důkazů, provedu test proporcionality, a analyzuji, jaké právní limity by měly být zavedeny pro to, aby bylo užívání těchto systémů zcela v souladu s právními předpisy. Pátá kapitola bude zaměřena na otázku, zda a jak mohou být výstupy FR systémů použity jako důkazní prostředek v trestním řízení. V šesté kapitole bude řešena problematika uchovávání dat v referenčních databází FR systémů. V této části se zaměřím na otázku, jak dlouho a za jakých podmínek mohou být fotografie osob z civilních registrů uchovávány v databázích FR systémů a zda tato praxe odpovídá požadavkům na ochranu soukromí a osobních údajů. Závěrečná kapitola pak představí novou právní úpravu Evropské unie, která se přímo dotýká užívání FR systémů bezpečnostními složkami členských států EU.

1. Technologie FR systémů

FR systémy představují pokročilou formu biometrického systému fungující na bázi AI, která je užívána nejen v kriminalistice, ale také v bezpečnosti, zdravotnictví a spoustě jiných oblastech. Pro přiblížení užívání FR systémů v kriminalistice je zapotřebí pochopit fungování AI, základy biometrie, biometrických systémů a uvědomit si, jaké údaje a jakým způsobem jsou zpracovány. Až následně tak bude možné zaměřit se na samotné fungování biometrických systémů rozpoznávající obličeje, respektive technické aspekty těchto systémů a samotný proces, který vede až k identifikaci osob.

1.1. Definice AI

AI zaujímá klíčovou roli v moderním technologickém světě. Může však být matoucí, co si pod pojmem AI představit. Na začátku je třeba si uvědomit, že AI je na jedné straně chápána jakožto inteligence strojů a systémů, která dokáže plně fungovat bez lidského zásahu a která částečně překračuje i lidského chápání toho, jak tato inteligence funguje. Takováto inteligence poháněná algoritmy a daty může vykonávat složité úkoly a rozhodovat se bez přímého dohledu lidí.

Na druhé straně však umělá inteligence reprezentuje samostatný vědní obor, který se snaží strojům a systémům AI nejen porozumět, ale také je i vytvářet. Skládá se z mnoha podoborů, přičemž mezi nejvýznamnější podobory patří podobor strojového učení, díky čemuž se systémy a stroje dokáží nejen samy učit a zlepšovat, ale také samostatně rozhodovat. Tato metoda se stala základem pro užívání FR systémů.

Definovat AI je tak poměrně složité. Přestože neexistuje jedna univerzální, komplexní, všemi uznávaná definice, mezi nejvíce zmiňovanou můžeme zařadit definici Marvina Lee Minskyho: *„Umělá inteligence je věda o tom, jak přimět stroje dělat věci, které by vyžadovaly takovou inteligenci, jako kdyby je dělali lidé.“*[1] Přestože se jedná o velmi zjednodušenou definici, shrnuje podstatu všech ostatních definic, tedy představuje prvek programu nebo stroje, který je schopen napodobovat lidské myšlení a chování. Komparatistika současné AI s člověkem se však zdá být dle mého názoru i v dnešní době irelevantní, jelikož žádná AI není schopna komplexně napodobit lidské myšlení či chování. Přestože existují systémy porážející lidi ve vědomostních či šachových soutěžích, autonomní auta či chatboty generující informace, jedná se vždy o úzký okruh činností, které tyto systémy dokáží ovládat.

[1] ANTEBI, Liran. *What is Artificial Intelligence?* Institute for National Security Studies, 2021, s. 31. [cit. 27.09.2024]. Dostupné také z: https://www.jstor.org/stable/resrep30590.7 (vlastní předklad).

Do dnešního dne totiž nebyla vytvořena AI, která by se ve své komplexnosti člověku vyrovnala.

O definici AI se pokusila i Evropská unie, konkrétně pak Evropský hospodářský a sociální výbor, dle kterého je *„umělá inteligence zastřešující pojem pro velké množství (pod)oblastí, jako např.: kognitivní informatika, strojové učení, rozšířená inteligence, robotika v oblasti UI. Ústředním cílem výzkumu a vývoje v oblasti UI je však automatizace inteligentního jednání, jako je argumentace, shromažďování informací, plánování, učení, komunikace, manipulace, vysílání signálů a samostatná tvorba, snění a vnímání.“*[2]

Definice Evropského hospodářského a sociálního výboru je však velice široká, proto se o její zestručnění pokusila v roce 2019 i Evropskou komisí zřízená Odborná komise: *„Systémy umělé inteligence (UI) jsou softwarové (a případně také hardwarové) systémy navržené lidmi, které mají zadán složitý cíl a jednají ve fyzické nebo digitální dimenzi, přičemž vnímají své prostředí tím, že získávají data, interpretují shromážděná strukturovaná nebo nestrukturovaná data, usuzují ze znalostí nebo zpracovávají informace odvozené z těchto dat a rozhodují o nejlepší akci či akcích k dosažení daného cíle…Jako vědní obor zahrnuje UI řadu přístupů a technik, jako je strojové učení (…), strojové usuzování (…) a robotika (…).“*[3]

I přes to, že tato nová definice je také poměrně široká, rozlišuje mezi AI jakožto softwarovými/hardwarovými systémy a vědním oborem využívající různé techniky. Přestože jsou dle této definice systémy AI tvořeny lidmi, Odborná komise připouští, aby pro optimalizací návrhů vytvořených lidmi byla použita AI. Definice ovšem nenechává prostor pro vytvoření AI jinou inteligencí, což se může v budoucnu s rozvojem technologií jevit jakožto zastaralý pohled.

1.2. Dělení AI

Do dnešního dne existují, ale i nadále vznikají různé přístupy, které umožňují pochopení a kategorizaci této oblasti. Díky těmto kategorizacím tak můžeme lépe chápat různé aspekty AI a její fungování. Základní kategorizací je dělení na „software-based AI“ a „hardware-based AI“.[4] Software-based AI lze pochopit jakožto počítačový program, který využívá AI

[2] Evropský hospodářský a sociální výbor. Bod 2.1. stanoviska Evropského hospodářského a sociálního výboru k tématu Umělá inteligence – dopady umělé inteligence na jednotný trh (digitální), výrobu, spotřebu, zaměstnanost a společnost. 2017. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52016IE5369&from=ES.

[3] *Odborná skupina na vysoké úrovni pro umělou inteligenci.* Definice UI: Hlavní schopnosti a obory. [online] 2018 [cit.03.10.2024]. Dostupné z: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60663.

[4]Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Artificial Intelligence for Europe

k zpracování rozsáhlých dat a řešení úkolů, které by jinak vyžadovaly lidskou inteligenci. Mezi takové softwary patří například virtuální asistenti, softwary na rozpoznávání obrazu, analýzu videa, ale také již zmiňované FR systémy. V případě, kdy je takovýto program plně spjat s hmotným prostředkem, jedná se o hardware-based AI. Nejčastějším příkladem tohoto typu inteligence jsou roboti, drony či autonomní auta.

Jedním z možným dalších dělení je kategorizace AI na základě funkcí, přesněji pak AI reaktivní, s omezenou pamětí, s teorií mysli a s vědomím sebe sama. [5] Reaktivní AI nepoužívá ani neuchovává předešlé zkušenosti při řešení nových úkol, ale místo toho operuje pouze s aktuálními daty v dané situaci, přičemž povědomí tato inteligence o čase nemá. Dokáže řešit pouze předem naprogramované situace, jako je tomu například u spamového emailového filtru. Naproti tomu AI s omezenou pamětí rozhoduje na základě malého množství paměti, která poskytuje zkušenosti a znalosti během různých situací. Je tak schopna se v omezené míře učit ze svých zkušeností a optimalizovat tak své budoucí výkony. Typickým reprezentantem tohoto typu inteligence jsou autonomní vozidla. Naproti tomu inteligence s teorií mysli by již měla rozumět lidským pocitům, emocím a myšlenkám. Přestože se na tomto typu inteligence v současné době pracuje, doposud nebyla žádná taková inteligence vyvinuta. AI s vědomím sebe sama je pak v současné době zcela teoretickým pojmem. [6] Tento druh AI by měl být schopen vnímat a uvědomovat si sám sebe, své myšlenky, pocity či emoce. Pokud tak v budoucnu dojde k jejímu ztělesnění, bude se jednat o robota s vědomím a inteligencí na úrovni člověka.

Další možnou kategorizací je dělení dle schopností na AI úzkou, obecnou a super inteligenci.[7] Úzká AI je ta, která se specializuje na provedení jedné nebo více konkrétních úkolů, avšak není schopna vykonávat nic jiného. Takovýmto příkladem mohou být autonomní auta či chatboti. Oproti tomu obecná AI by měla být schopná vykonávat většinu rozmanitých činností jako lidé, ale do dnešní doby nebyla zcela ještě vyvinuta. Přestože dnes existují AI, které dokáží plnit řadu činností, v komplexitě činností stále zaostávají. Umělá super inteligence by pak nejenže měla být schopna vykonávat rozmanité činnosti stejně jako lidé,

---

[online]. 25. 4. 2018 [cit.03.10.2024]. Dostupné z: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51625.

[5] MARTINEZ, Rex. Artificial Intelligence Distinguishing Between Types & definitions. *Nevada Law Journal*. Vol. 19: Iss. 3, Article 9 s. 1038. Dostupné z: https://scholars.law.unlv.edu/cgi/viewcontent.cgi?article=1799&context=nlj

[6] GŘIVNA, Tomáš a kol. *Vliv nových technologií na trestní právo*. Auditorium, 2022, s. 261. ISBN 978-80-87284-95-7.

[7] STAHL, Bernd Carsten. *Artificial Intelligence for a Better Future: An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies*. Cham: Springer International Publishing, 2021, s. 10. DOI: 10.1007/978-3-030-69978-9.

ale v těchto činnostech by měla být dokonce lepší než samotní lidé. V současné době se jedná o zcela teoretický koncept, ovšem bez nadsázky lze říci, že se jedná o pomyslný cíl, ke kterému vývoj AI směřuje.

1.3. Biometrická identifikace

Biometrie je vědecký obor, který se zabývá měřením a analýzou tělesných a behaviorálních charakteristik jedinců pro účely jejich identifikace či autentizace. Současná biometrická identifikace využívá neměnné charakteristické vlastnosti jednotlivce, které jsou těžce zaměnitelné, díky čemuž je možné jednotlivce snadněji identifikovat. K identifikaci osob dnes však neslouží pouze unikátní obličejové rysy, ale také jiné unikátní charakteristiky, jako je duhovka, sítnice, uši, otisky prstů, ale také fyziologické projevy člověka jako je styl chůze, či podpis jednotlivce, a to v návaznosti na konkrétní biometrické systémy.[8] Biometrickou identifikaci je tak možné definovat jako *„automatizované využití jedinečných, měřitelných anatomických a fyziologických charakteristických projevů člověka k jednoznačnému ověření nebo zjištění jeho identity.“*[9]

Biometrie tak najde široké využití v oblastech od zdravotnictví, finančních služeb, cestování, až po bezpečnost či telekomunikaci. Mimo to však biometrická identifikace může být velice nápomocným nástrojem kriminalistické identifikace, kterou lze chápat jakožto *„proces, během kterého se zjišťuje, kterým konkrétním objektem byla vytvořena konkrétní kriminalistická stopa. Jedná se o proces ztotožňování objektů podle kriminalistických stop a jiných zobrazení, ve kterém se hledá souvislost osoby nebo věci s kriminalisticky relevantní událostí.“*[10]

V 19. století v Paříži vyvinul Alphonse Bertillon metodu zvanou "Bertillonage" neboli antropometrii, postavenou na měření specifických tělesných proporcí pro klasifikaci a identifikaci zločinců. I když tento systém nebyl dokonalý, zahájil využívání unikátních biologických znaků k ověřování identity, což umožňovalo dopadnout i ty zločince, kteří si například změnili svá jména. S postupem vědeckého pokroku došlo také k využívání dalších biologických znaků, jako jsou například otisky prstů. Skutečné biometrické systémy se však

[8] RAK, Roman, MATYÁŠ, Václav, ŘÍHA, Zdeněk. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha : Grada Publishing, 2008, s. 115. ISBN 978-80-247-2365-5.; OLUSHOLA, Bayo. Overview of Biometric and Facial Recognition Techniques, *Journal of Computer Engineering.* Issue 4, Volume 20. s. 1. Dostupné také z: https://www.iosrjournals.org/iosr-jce/papers/Vol20-issue4/Version-1/A2004010105.pdf.

[9] RAK, Roman, MATYÁŠ, Václav, ŘÍHA, Zdeněk. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Grada, 2008, s. 105. ISBN 978-80-247-2365-5.

[10] STRAUS, Jiří, NĚMEC, Miroslav, a kol. *Teorie a metodologie kriminalistiky*. Plzeň: Aleš Čeněk, 2009, s. 137. ISBN 978-80-7380-214-1.

začaly objevovat až ve druhé polovině dvacátého století současně s nástupem počítačových systémů, kdy se biometrické rozpoznávání člověka stalo automatizovaným.

Rozvoj technologie a počítačových systémů umožnil, že dnešní FR systémy dokáží nejen rozeznat, zda se na dvou rozdílných snímcích nachází tatáž osoba, ale dokáží také identifikovat konkrétní osobu (za předpokladu, že je její fotografie obsažena v referenční databázi systému). Může tak činit nejen na základě statických fotografií, ale také během dynamického monitorování veřejném prostoru. Biometrika však nefunguje na principu porovnávání fyzických obrázků, nýbrž na porovnávání matematických kódů. Dnešní FR systémy totiž užívají algoritmy na bázi AI, díky čemuž je biometrická identifikace mnohem rychlejší, přesnější a zcela automatizovaná. Zatímco lidský mozek potřebuje na rozpoznání jedné tváře 20 milisekund, speciálně naprogramované softwary dokáží analyzovat přes 15 miliónů tváří za minutu.[11]

FR systém však není jediný, který staví na biometrii. Mezi takovéto systémy můžeme zmínit například biometrický systém na rozpoznání otisků prstů, kdy otisky prstů jednotlivce jsou porovnávány s databází obsahující zaznamenané otisky prstů osob. Díky tomu, že otisk prstů jednotlivce je zcela originální a neshoduje se s otiskem prstu někoho jiného, jsou otisky prstů jednou ze základních metod forenzní analýzy. Mezi další druh systémů patří systémy rozpoznávající styl chůze využívající skutečnost, že každý jedinec klade jednu nohu před druhou jiným způsobem, což se projevuje na rozlišnosti chůze, kterou je možné analyzovat. Se stále se zlepšující moderní technologií se očekává, že tato metoda bude v budoucnu více a více populárnější. Zvláštním druhem biometrického systému silně navazujícím na FR systémy jsou systémy rozpoznávající náladu člověka. Ty skrze kamery nebo senzory zachycují obličejové rysy jako jsou výrazy očí, úsměvy nebo vrásky. Tyto vizuální informace jsou systémem následně zpracovány s cílem identifikovat charakteristické znaky spojené s určitými emocemi jako je například radost, smutek, hněv nebo překvapení. Výsledkem je pak odhadnutý emocionální stav člověka.

Biometrika s sebou v kriminalistice přináší spoustu výhod i nevýhod. Jak již bylo zmíněno výše, biometrické metody jsou vysoce přesné a spolehlivé. Stálost biometrických údajů je taktéž důležitá, jelikož biometrické údaje jako je tvář, otisk prstů nebo DNA se nemění s věkem, což umožňuje jejich dlouhodobé a opakované použití při identifikaci. Navíc konkrétně v případě FR systémů by systém neměl být ovlivněn například špatným osvětlením či výrazem, přičemž systém bere v úvahu proměnné jako je věk, líčidla či potenciální

[11] RAK, Roman, MATYÁŠ, Václav, ŘÍHA, Zdeněk. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada Publishing, 2008, s. 364. ISBN 978-80-247-2365-5.

plastické operace. Další výhodou je rychlost, kterou moderní biometrické systémy poskytují, a tudíž mohou kriminalistům ušetřit hodiny práce. Díky pokrokům v technologii je možné rychle identifikovat a verifikovat jednotlivce, což umožnuje rychlejší postup během vyšetřování. Biometrická identifikace s sebou přináší i nevýhody. Za zmínku stojí finanční náročnost, možnost zneužití či obava o soukromí osob.

1.4. Biometrické údaje

Mimo samotnou biometrii je třeba upřesnit, co to jsou biometrické údaje, které jsou biometrickými systémy zpracovávány. Jejich definici však česká právní úprava neobsahuje, proto je třeba nahlédnout do úpravy evropské. Dle čl. 4 nařízení GDPR jsou biometrickými údaji *„osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.“* Biometrické údaje jsou tedy takové údaje, které vedou k identifikaci osoby.[12] Čím se pak rozumí samotné technické zpracování, je definováno jakožto *„jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění seřazení či zkombinování, omezení, výmaz nebo zničení.“*[13]

Tato definice je však lehce problematická. V praxi tato definice znamená, že každý biometrický údaj je považován za osobní údaj. Může tak být sporné, zda biometrické šablony jsou biometrickými údaji či nikoli, jelikož jejich reverzibilita do biometrických vzorků je problematická. To bylo vyřešeno až díky vědcům, kteří konstatovali, že biometrické šablony jsou reverzibilní a nemohou tak představovat anonymní data.[14] S rozvojem technické vyspělosti tak hrozí, že podobných definičních problémů bude přibývat, proto bude zřejmě potřeba definici upřesnit.

V zásadě je možné rozlišovat mezi 2 kategoriemi biometrických údajů. První kategorií jsou údaje založené na fyziologických rysech, kterým je typicky obličej, oční duhovka, oční sítnice, otisk prstu či DNA. Jedná se o rysy velice stabilní, u kterých dochází ke změně pouze

[12] MATEJKA, Ján, KRAUSOVÁ, Alžběta, GÜTTLER, Vojen. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie*, roč. 9., č. 18, s. 91–129. DOI 10.5817/RPT2018-1-5.
[13] Čl.4 odst. 2 nařízení GDPR.
[14] MATEJKA, Ján, MATOCHOVÁ, Soňa, PROKEŠ Josef. Analysis of Biometric Data Under the General Data Protection Regulation. *Acta Informatica Pragensia*. 2019, roč. 8, č. 2. DOI: 10.18267/j.aip.126.

ve výjimečných situacích. Mohou tak být snadno zachyceny pomocí speciálních senzorů nebo kamer a jejich uchování v referenčních databází není z důvodu neměnnosti složité. Druhou kategorií jsou rysy behaviorální, do kterých řadíme znaky jako je způsob chůze, podpisu, způsob psaní či mluvení. Tyto znaky jsou dynamické povahy, jsou získávány opakovaným sledováním jednotlivce a s odstupem času může dojít k jejich změně. V případě vedení databází těchto znaků by mělo docházet k pravidelné aktualizaci, což může být v praxi velmi problematické. Z tohoto důvodu analýza těchto znaků nemusí být toliko spolehlivá jako v případě fyziologických rysů.

1.5. Technické aspekty FR systémů

Technologie biometrického rozpoznávání obličejů je poměrně komplexní a složitá, avšak pro pochopení jejího využít je zapotřebí alespoň zjednodušeně vysvětlit, jak funguje. Tato technologie je tvořena algoritmy vytvářející digitální záznamy (tzv. databázi), které obsahují obličejové snímky v podobě šablon a dále pak algoritmy porovnávající zachycené snímky se záznamy z databází. V případě monitorování veřejných prostor je tento systém napojen na kamerové zařízení. Středobodem FR systémů je tak software fungující na bázi AI, který využívá složité algoritmy za účelem identifikace či verifikace osob zachycených na záznamu, přičemž je porovnává s databází systému.

Obličejová biometrie využívá různé přístupy k identifikaci jednotlivců na základě charakteristik obličeje, k čemuž je využívána široká paleta technik. Mezi nejčastěji využívané techniky patří strojové učení s metodou hlubokého učení tzv. deep learning. Tato metoda vychází z toho, že každá struktura umělých neurálních sítí se skládá z vrstev obsahující jednotky, které transformují vstupní data na informace, jež jsou využity pro prediktivní úlohy následující vrstvou.[15] Každá vrstva obsahuje jednotky, které přeměňují vstupní data na informace, které jsou následně využity další vrstvou k plnění konkrétních prediktivních úkolů.[16] Tato metoda umožňuje počítači učit se prostřednictvím svého vlastního zpracování dat. Díky tomuto samostatnému učení představují systémy založené na architektuře neuronových sítí „black box“, čili „černou skříňku“. To znamená, že v současné době není možné detailně prozkoumat, jakým způsobem systém vyhodnotil určitý obrázek a proč dospěl k danému konkrétnímu výsledku namísto jiného.

[15] Hluboké učení vs. strojové učení - Azure Machine Learning. In: *Microsoft*. [online]. 19. 1. 2024 [cit. 01.07.2024]. Dostupné z: https://learn.microsoft.com/cs-cz/azure/machine-learning/concept-deep-learning-vs-machine-learning?view=azureml-api-2.

[16] Ibid.

V rámci metody hlubokého učení jsou využívány speciální architektury, v případě FR systémů je to architektura konvolučních neuronových sítí. Tato architektura je charakteristická uspořádáním vrstev ve 3 rozměrech, kterými jsou šířka, výška a hloubka. *„Konečný výstup se pak zmenší na jeden vektor skóre pravděpodobnosti uspořádaného podle rozměru hloubky.“*[17]

Před samotným spuštěním systému v praxi však probíhá nejprve testování na databázích obsahující obličejové snímky. Na těchto datech se algoritmus dokáže sám učit, jak data správně vyhodnocovat, což je kontrolováno programátory těchto systémů, kteří mohou před užitím systému v praxi provést potřebné úpravy.

1.6. Fungování FR systémů

K určení identity jednotlivce je zapotřebí několik na sebe navazujících operací. Je třeba však mít na paměti, že pokud šablona jednotlivce není v databázi, nelze jednotlivce během následujících operací identifikovat. Tato šablona vzniká extrahováním požadovaných rysů z databází fotografií obyvatel, přičemž těmito rysy může být například tvar a pozice nosu, lícních kostí, ústa, oči, ale také vzdálenost mezi těmito rysy.[18] Tyto rysy jsou na základě matematických operací následně převedeny do matematické reprezentace, která se nazývá šablona. Samotná šablona pak reprezentuje zakódovaný číselný obraz obličeje jednotlivce, který je zařazen do databáze.

Mezi prvotní operace patří operace rozpoznávání obličeje tzv. detekce. Tato fáze nevede k identifikaci konkrétní osoby, nýbrž pouze rozeznává obličej od jiných předmětů v obraze. Je však potřeba, aby záznam zachycující podobu jednotlivce měl určitou minimální kvalitu, se kterou může systém následně pracovat. Výběr samotného kamerového zařízení je tak velice podstatný, jelikož ovlivňuje přesnost a spolehlivost systému. Pro snímaní obličejů osob na veřejných místech je tak zapotřebí kvalitní kamerové zařízení, které může mít podobu standardní 2D kamery nebo pokročilé 3D kamery. Klasické 2D kamerové systémy však již nebývají příliš využívány, a to zejména pro způsobující deformaci obličeje, lehkou oklamatelnost, potřebu dobrého osvětlení a nízkou přesnost. V případě 3D kamerových zařízení je sice problematická vyšší prvotní cena, avšak jedná se o přesný a spolehlivý nástroj, který lze doplnit o další metody, jako jsou například termo snímky obličeje. Nic však v teoretické rovině nebrání tomu, aby byl obraz zachycen na zařízeních jako je běžná kamera, fotoaparát či smartphone a následně analyzován FR systémem.

---

[17] Ibid.

[18] SALEEM, Sharzeel, SHINEY, J., SHAN, B. P., MISHRA. V.K. Face recognition using facial features. *Materials Today: Proceedings*,Volume 80, Part 3, 2023, s.1. ISSN 2214-7853.

Během následující operace, tzv. kategorizace, dochází ke zařazení jednotlivce do konkrétní skupiny osob, a to dle charakteristikách rysů konkrétní skupiny. Kategorizace tak umožňuje jednotlivce zařadit do určité kategorie dle věku, pohlaví, rasy… Během těchto dvou fází, tedy detekce a kategorizace, nedochází ke zpracovávat biometrické údajů, a tudíž není možné na základě těchto dvou fází určit totožnost jednotlivce.

Určit totožnost osoby je možné až během následujíce operace, kterou je buďto operace verifikace či identifikace. Verifikace a identifikace osob představují zcela rozdílné operace, proto je zapotřebí mezi nimi rozlišovat. U verifikace (známé též pod pojmem autentizace) dochází k porovnávání šablony 1:1 s šablonou druhou.[19] Verifikace tak představuje proces, při kterém dochází k ověřování, zda je jedinec skutečně tím, za koho se vydává, a dochází tak k zodpovězení otázky, zda je daná osoba opravdu tou, za kterou se vydává. Verifikace tak bývá v praxi často využívána například při povolení vstupu do zabezpečených či chráněných objektů. Identifikace je naopak proces, při kterém je potřeba zjistit totožnost neznámého jedince, a tudíž dochází k porovnávání fotografie, respektive šablony jednotlivce 1:N s mnoha jinými šablonami.[20] Během procesu identifikace tak dochází k ztotožnění konkrétní osoby.

1.7. Zpětná a reálná identifikace

V současné době existují 2 druhy FR systémů, a to systémy fungující *„v reálném čase*“ a systémy „*zpětné*“. V případě FR systémů fungující v reálném čase dochází k identifikaci osoby téměř okamžitě. V tomto případě jsou kamerové systémy vybaveny systémem na zpracování biometrických údajů. Skrze živé monitorování veřejných prostor jsou pak generovány snímky osob, které jsou po zpracování následně porovnávány s šablonami z databází systému. Dokáží tak rozpoznat identitu jednotlivce téměř v reálném čase.

Jinak je tomu u zpětného FR systému, u kterého dochází k cílené identifikaci až s odstupem času. V takovémto případě je potřeba zdrojový obraz zachycující obličej vložit do systému k detenci biometrických údajů, přičemž až s odstupem času jsou obličejové prvky porovnávány s šablonami z databází FR systémů. Ve většině případů však touto funkcí disponují také systémy fungující v reálném čase. Díky ukládání kamerových záznamů v těchto systémem je možné v případě potřeby zpětně osobu identifikovat a není tak zapotřebí kamerový záznam do systému vkládat.

[19] Types of Biometrics: Face - Key Considerations In: *biometrics institute* [online] [cit. 03.10.2024]. Dostupné z: https://www.biometricsinstitute.org/types-of-biometrics-face-key-considerations/.

[20] KUHLMANN, Simone. Government Use of Facial Recognition Technologies under European Law. In: ZALNIERIUTE, Monika a Rita MATULIONYTE, eds. *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge: Cambridge University Press, 2024. s. 660. DOI: 10.1017/9781009321211.012.

2. Současné využití FR systémů

2.1. Využití v České republice

V České republice je využití FR systémů relativně nové, avšak jejich potenciál pro budoucí užití je značný. Již v současné době dochází k využívání FR systémů, jedním z významných příkladů je jejich použití na Letišti Václava Havla v Praze, kde systém umožňuje v reálném čase identifikovat cestující pohybující se na území letiště, čímž napomáhá s pátráním po hledaných osobách. Mimo to Policie využívá FR systém zejména za účelem zpětné identifikace pachatelů trestných činů. Objevují se však i další snahy o implementaci FR systémů, včetně snah Ministerstva vnitra o nasazení FR systémů na dalších mezinárodních letištích či na veřejných místech Praze, avšak k těmto nasazením do současné chvíle nedošlo. Okruh možného užití FR systémů mimo Policii se rozšiřuje, o čemž svědčí například snahy o využití k identifikaci nežádoucích osob na fotbalových stadionech.

2.1.1. Zpětné užívání Policií

Díky nevládní organizaci Iuridicum Remedium bylo zjištěno, že Policie využívá zpětného systému biometrické identifikace na dálku k identifikaci pachatelů závažných trestných činů a identifikaci mrtvých, a to již od 22. srpna 2022, kdy byl zahájen zkušební provoz.[21] Tato informace byla dne 20. července 2023 potvrzena na webu Policie, přičemž došlo k upřesnění, že Policie využívá ke zpětné identifikaci na dálku informační systém Digitální podoba osob od společnosti Autocont.[22] Policie je však kritizována za tajné využívání FR systému bez zákonného podkladu. Policie však tvrdí, že o užívání FR systému byl informován Výbor pro lidská práva a moderní technologie při Úřadu vlády České republiky, tedy k žádnému zatajování informací nemohlo docházet.[23] S touto informací však nesouhlasí již zmiňována organizace Iuridicum Remedium, která tvrdí, že k žádnému informování nikdy ze strany Policie nedošlo.

Zákonně provozovat tento systém je dle slov Policie možné na základě interního pokynu policejního prezidenta, tak ustanovení § 66a zákona č. 273/2008 Sb., o Policii České

[21] TROJÁNEK, Hynek. Policie již téměř rok využívá analytický nástroj na rozpoznávání tváří. Podrobnosti jeho fungování tají In: *Digitální svobody* [online]. 2023 [cit. 03.10.2024]. 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/.

[22] Aktualizace: Vyjádření k provozování informačního systému Digitálních podob osob - Policie České republiky [online]. [cit. 03.07.2024]. Dostupné z: https://www.policie.cz/clanek/vyjadreni-k-provozovani-informacniho-systemu-digitalnich-podob-osob.aspx.

[23] Ibid.

republiky.[24] Při zpětném porovnávání dochází k porovnání fotografií s referenční databází systému, která se skládá z fotografií zdrojových databází. Těmito zdrojovými databázemi jsou dle § 66a zákona o Policii České republiky fotografie uvedené v *a) informačním systému evidence občanských průkazů; b) informačním systému evidence cestovních dokladů; c) informačním systému evidence diplomatických a služebních pasů; d) registru řidičů; e) centrálním registru řidičů; f) informačním systému cizinců*. K červenci 2023 se v této referenční databázi nacházelo na 19 666 787 fotografií osob.[25]

Systém by měl mít schopnost v krátkém časovém úseku, konkrétně do 15 sekund, vyhledat a poskytnout identifikátory fotografií osob, které vykazují nejvyšší míru shody se zadanou referenční fotografií.[26] Každá taková fotografie by měla být navíc spojena s unikátním identifikátorem, který by umožňoval přístup k dalším osobním údajům těchto jednotlivců. Tento proces by měl zahrnovat důkladnou analýzu shody, kde algoritmy AI porovnávají různé rysy obličeje a další biometrické údaje, aby se zajistilo, že výsledky jsou co nejpřesnější. Do informačního systému má přístup „*73 osob z Policejního prezidia, Národní centrály proti organizovanému zločinu a Národní centrály proti terorismu, extremismu a kybernetické kriminalitě, z toho je 37 operačních důstojníků, 7 technických pracovníků a ostatní příslušníci kriminální policie.*“[27]

Dle Policie bylo od spuštění systému, tj. 22. srpna 2022, vyřízeno přes 100 žádostí na užití FR systému, avšak úspěšnost systému se pohybovala okolo 40 % - 45 %, a to zejména z důvodu špatné kvality vstupních fotografií, nikoli chybovosti systému jako takového.[28] Na základě žádosti o informace mi bylo sděleno, že ke dni 19.3.2024 bylo Policií vyřízeno přes 200 žádostí. Jaká je však falešná pozitiva či negativita tohoto systému mi však sděleno nebylo, s odůvodněním, že *“DPO po porovnání se zdrojovou fotografií neznámé osoby nabízí kandidáty na případné ztotožnění, o kterém rozhoduje k tomu určený pracovník na základě vizuálního posouzení podobnosti se zdrojovou fotografií. Jedná se pouze o podpůrný nástroj k identifikaci neznámých osob, přičemž bez dalšího nelze výsledek ztotožnění považovat*

[24] Ibid.

[25] MACH, Václav. Český Minority Report: Využití umělé inteligence Policií České republiky [online]. *Iuridicum Remedium (IuRe)*, 2023. s. 41. Dostupné z: https://digitalnisvobody.cz/wp-content/uploads/2024/01/cesky_minority_report_iure_23.pdf.

[26] Ibid., s. 41.

[27] Ibid., s. 42.

[28] Aktualizace: Vyjádření k provozování informačního systému Digitálních podob osob - Policie České republiky [online]. [cit. 03.07.2024]. Dostupné z: https://www.policie.cz/clanek/vyjadreni-k-provozovani-informacniho-systemu-digitalnich-podob-osob.aspx.

za jednoznačnou identifikaci neznámé osoby. Systém tedy nepracuje s pozitivitou/negativitou rozpoznání.“[29]

2.1.2. Letiště Václava Havla

Na letišti Václava Havla se nachází jediný oficiálně užívaný FR systém fungující v reálném čase, jehož součástí je na 145 kamer.[30] Systém byl vytvořen specificky v souladu s usnesením vlády České republiky č. 47/2015, o zvýšení bezpečnosti na mezinárodním letišti Václava Havla v Praze, které bylo přijato dne 19. ledna 2015, přičemž samotný systém je provozován od 15. června 2018 až do dnešního dne. Až do konce roku 2022 bylo systémem ztotožněno na 234 osob.[31] Pověřen výkonem činnosti je ředitelství služby cizinecké policie, přičemž do systému mají přístup bezpečnostní sbory působí na Letišti Václava Havla.[32]

Systém srovnává biometrický obraz tváří jednotlivců, kteří byli zachyceni kamerovým systémem s databází zájmových osob vedenou Policií, která získává data z informačního systému PATROS, sloužící k identifikaci hledaných a pohřešovaných osob.[33] Systém umožňuje provádět identifikaci jak v online režimu, tak i prozkoumávat tváře jednotlivců zachycených kamerovým systémem až 30 dní nazpět, přičemž následně dochází ke smazání pořízených záznamů. Dle informací mi poskytnutých Policií bylo od roku 2018 až do současnosti (tj. 19.3.2024) registrováno 171 pozitivních hitů, z toho však bylo 24 698 hitů vyřízeno jako falešných.[34]

K identifikaci hledaných a pohřešovaných osob je dle informací mi poskytnutých Policií využívána Technologie NEC NeoFace Watch verze 3. Podrobné informace o provozních podmínkách FR systému na letišti však nejsou veřejně dostupné. Provozovatel systému, kterým je Ředitelství služby cizinecké policie, se domnívá, že interní předpisy policie je nutné ze strategických důvodů udržovat v tajnosti, proto k podrobnostem

[29] Částečné poskytnutí informací ze dne 19.3.2024 vydané Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednacím PPR-12351/ČJ-2024-990810.

[30] Ministerstvo vnitra rozšíří zabezpečení Letiště Václava Havla o 145 kamer s automatickým rozpoznáváním obličejů - Ministerstvo vnitra České republiky. In: *MVCR* [online]. [cit. 01.10.2024]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-rozsiri-zabezpeceni-letiste-vaclava-havla-o-145-kamer-s-automatickym-rozpoznavanim-obliceju.aspx.

[31] MACH, Václav. Český Minority Report: Využití umělé inteligence Policií České republiky [online]. *Iuridicum Remedium (IuRe),* 2023. s. 35. Dostupné z: https://digitalnisvobody.cz/wp-content/uploads/2024/01/cesky_minority_report_iure_23.pdf.

[32] Systém detekce obličejů - Policie České republiky. In: *Policie* [online]. 2020. [cit. 01.07.2024]. Dostupné z: https://www.policie.cz/clanek/zverejnene-informace-2020-system-detekce-obliceju.aspx.

[33] Ibid.

[34] Částečné poskytnutí informací na základě žádost o informace ze dne 19.3.2024 vydané Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednacím PPR-12351/ČJ-2024-990810.

provozování systémů nemá veřejnost přístup.[35] Je tomu tak i v případě smlouvy mezi Ministerstvem vnitra a dodavateli zabezpečovacího systému, která obsahuje ustanovení o mlčenlivosti a stanovuje, že všechny informace a údaje získané během plnění zakázky, včetně předmětu plnění uvedené v příloze smlouvy, jsou považovány za důvěrné, a proto není možné tyto informace sdělit veřejnosti. [36] Tato praxe však dle mého názoru vzbuzuje obavy o potenciální zneužití pravomocí a nedostatek odpovědnosti ze strany Policie, zejména v kontextu ochrany osobních údajů a základních práv a svobod jednotlivců. I přes to je však užívání FR systému na Letišti Václava Havla mnohými považováno za legální a legitimní.[37]

2.1.3. Pokusy o další implementaci

Po nasazení biometrického systému na Letišti Václava Havla, Ministerstvo vnitra plánovalo nasadit biometrické systémy také na zbylých mezinárodních letištích v České republice, tedy v Ostravě, Brně, Karlových Varech a Pardubicích. Navzdory těmto plánům se však nasazení FR systémů na dalších letištích neuskutečnilo, přestože Ministerstvo vnitra mělo plán uskutečnit instalaci systémů do konce roku 2020.[38] Podobně tomu mělo být i na Pražském hradě,[39] v pražském metru či městském kamerovém systému hlavního města Prahy.[40] Tento neúspěch v realizaci mohl být způsoben několika faktory, včetně složitého procesu schvalování této technologie. Jedním z klíčových důvodů, proč k instalaci zřejmě nedošlo, mohl být požadavek provedení posouzení vlivů na ochranu osobních údajů, které je podle platné legislativy zapotřebí provést před každým zavedením systémů, které by mohlo mít významný dopad na soukromí jednotlivců.

Snahy o oficiální implementaci biometrických systémů však pokračují i mimo účel identifikace pachatelů trestných činů. Za zmínku stojí žádost o využití FR systémů za účelem zamezení vstupu nežádoucím osobám na fotbalových stadionech. Úřad pro ochranu osobních údajů se ve svém stanovisku vyjádřil k této problematice vyjádřil a argumentoval

---

[35] MACH, Václav. Český Minority Report: Využití umělé inteligence Policií České republiky [online]. *Iuridicum Remedium (IuRe),* 2023. s. 35 Dostupné z: https://digitalnisvobody.cz/wp-content/uploads/2024/01/cesky_minority_report_iure_23.pdf.

[36] Ibid.

[37] CIDLINA, Václav, PROKŮPEK, Jan, Legalita zavedení technologie rozpoznávání obličeje, In: *Bulletin Advokacie*, roč. 7-8/2020. s. 43.

[38] Ministerstvo vnitra pokračuje ve zvyšování bezpečnosti na mezinárodních letištích - Ministerstvo vnitra České republiky. In: *MVCR* [online]. [cit. 03.07.2024]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-pokracuje-ve-zvysovani-bezpecnosti-na-mezinarodnich-letistich.aspx.

[39] Události, komentáře In: *Česká televize* [online]. 17. dubna 2023 [cit. 03.07.2024]. Dostupné z: https://www.ceskatelevize.cz/porady/1096898594-udalosti-komentare/223411000370417/.

[40] Pražští policisté „otevírají diskusi“ o technologii na rozpoznávání obličejů. Hřib je proti. In: *Česká televize* [online]. [cit. 03.07.2024]. Dostupné z: https://ct24.ceskatelevize.cz/clanek/regiony/prazsti-policiste-oteviraji-diskusi-o-technologii-na-rozpoznavani-obliceju-hrib-je-proti-56924.

podmínkami čl. 9 GDPR o zpracování zvláštních kategorií osobních údajů: *„tento článek vyžaduje pro zpracování biometrických údajů i v případě významného veřejného zájmu výslovné zákonné zmocnění, které musí být přiměřené sledovanému cíli, musí dodržovat podstatu práva na ochranu údajů a poskytovat vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.*[41] Dle názoru Úřadu pro ochranu osobních údajů v době podání žádanosti zákonná úprava v roce 2019 takovéto zmocnění neobsahovala. Nic se nezměnilo ani s návrhy nových opatření v roce 2020. Přestože tyto návrhy požadované zmocnění obsahovaly, Úřad pro ochranu osobních údajů žádost opětovně nepodpořil. Hlavními důvody bylo nedostatečné zdůvodnění nezbytnosti užití zpracování biometrických údajů ve srovnání s jinými možnostmi eliminace rizik násilí na stadionech či chybějící posouzení rizik na ochranu osobních údajů ze zpracování biometrických údajů ve velkém rozsahu.[42]

2.2. Využití ve světě

FR systém je technologií, která je na celém světě využívána stále častěji. Jedním z možná nejkontroverznějších systémů na rozpoznávání obličejů je Clearview AI, původem americký systém, jehož databáze je tvořena z více než 20 miliard obrázků nashromážděných z internetu a sociálních sítí jako je Facebook, platforma X, Instagram a další. V případě shody systém uživateli poskytne krom shodného obrázku také internetové odkazy, kde se tyto obrázky objevily. Tento systém je používán OČTŘ napříč celým světem, ovšem výjimkou není ani užívání systému soukromými organizacemi. Dle uniklých informaci z roku 2020 tento systém používalo více než 2200 OČTŘ, vládních agentur a společností ze 27 zemí světa.[43]

Tento systém však byl z evropského trhu stáhnut v momentě, kdy několik evropských zemích zjistilo (společně s dalšími zeměmi jako je například Austrálie či Kanada), že společnost Clearview AI shromažďovala údaje občanů bez jejich souhlasu, čímž společnost porušovala zákony o ochraně osobních údajů. Úřady pro ochranu osobních údajů ve Francii,

[41] Úřad pro ochranu osobních údajů. Stanovisko. In: *UOOU*. [online]. 16. 8. 2019 [cit. 03.07.2024]. Dostupné z: https://uoou.gov.cz/uoou-k-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech.

[42] Ibid.; MACH, Václav. Český Minority Report: Využití umělé inteligence Policií České republiky [online]. *Iuridicum Remedium (IuRe)*, 2023. s. 39 Dostupné z: https://digitalnisvobody.cz/wp-content/uploads/2024/01/cesky_minority_report_iure_23.pdf.

[43] MCDONALD, Ryan Mac, Caroline Haskins, Logan. Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA. In: *BuzzFeed News* [online]. 28. 2. 2020 [cit. 03.07.2024]. Dostupné z: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

Velké Británii, Itálii či Řecku tak udělily pokuty společnosti Clearview AI. [44] Mimo to bylo společnosti Clearview AI nařízeno, aby fotografie občanů z databáze vymazala, což zapříčinilo její odchod z trhu EU.

V současné době policejní orgány jednotlivých evropských zemí používají vlastní systémy s národní databázemi k identifikaci osob. Příkladem může být INPOL „Informationssystem der Polizei“ v Německu, francouzský systém TAJ „Traitement des antécédents judiciaires”, systém křížového vyhledávání a analýzy VeRA v Bavorsku či systém KATSU ve Finsku. Na nadnárodní úrovni pak světová mezivládní organizace Interpol od roku 2016 využívá společnost IDEMIA k vytvoření vlastního systému „INTERPOL face recognition systém“, tzv. IFRS. Tento systém obsahující fotografie z více než 170 zemí světa napomohl k dopadení tisíců pachatelů trestných činů. Díky spokojenosti s IFRS INTERPOL v roce 2019 prodloužil Interpol dohodu se společností IDEMIA o modernizaci IFRS na MBIS (multibiometrický identifikační systém). Tento systém o nejnovější verzi zvané MBIS 5 využívající nejmodernější algoritmy a technologie je užíván dodnes.[45]

Využívání FR systémů nemusí ovšem sloužit pouze k identifikaci pachatelů trestných činů. Zatímco v zemích Evropské unie jsou tyto systémy užívány OČTŘ především k identifikaci pachatelů trestných činů, existují země, které jsou známy svým rozšířenějším a invazivnějším používáním této technologie. V zemích, které porušují základní lidská práva a svobody jsou tyto technologie vedle zajišťování veřejné bezpečnosti často zneužívány k invazivnímu sledování a kontrole občanů. Na následujících příkladech bych ráda ukázala, že FR systémy mohou v nesprávných rukou představovat velmi mocný nástroj, který může být mimořádně efektivní, ale zároveň ignorovat, v některých případech až porušovat, základní lidská práva a svobody. Tento nástroj tak může být velice snadno zneužitelný, proto je zapotřebí stanovit právní meze a limity užití této technologie.

2.2.1. Spojené arabské emiráty

Spojené arabské emiráty mají jednu z největších koncentrací bezpečnostních kamer na světě. Z dostupných zdrojů je známo, že policejní kamerový systém dubajské metropole je od roku

[44] HILL, Kashmir. Clearview AI Successfully Appeals $9 Million Fine in the U.K. In: *The New York Times* [online]. 2023 [cit. 03.07.2024]. Dostupné z: https://www.nytimes.com/2023/10/18/technology/clearview-ai-privacy-fine-britain.html.

[45] ZULHUSNI, Muhammad. How does the INTERPOL BioHub capture most wanted criminals? In: *Tech Wire Asia* [online]. 6. 12. 2023 [cit. 03.07.2024]. Dostupné z: https://techwireasia.com/2023/12/how-does-the-interpol-biometric-tool-capture-the-most-wanted/.

2016 napojen na FR systém.[46] Tento systém dokáže nejen identifikovat osobu na základě obličejových rysů, ale také například uší či chůze. Jen v roce 2022 biometrické systémy pomohly dubajské policii vyřešit na 3200 případů.[47] Mimo užívání FR systémů na mezinárodním letišti jsou od roku 2020 kamery oficiálně také napojeny na FR systém ve veřejné dopravě.

Od roku 2023 jsou ve Spojených arabských emirátech nasazeny drony s názvem „EagleEye Intelligent Patrol" (se 360 stupňovými kamerami napojenými na FR systém), ale také systémem poznávající značky aut, který dokáže mimo jiné rozpoznat rychlost automobilu, nezapnuté pásy či člověka držícího telefon během jízdy.[48] Tyto drony fungují v reálném čase, tudíž v případě potřeby zasílají potřebné informace dubajské policii, která dokáže okamžitě zasáhnout. Spojené arabské emiráty patří beze sporu mezi světovou špičku ve využívání nejmodernějších sledovacích technologií. Díky těmto technologiím patří Dubaj mezi nejbezpečnější města na světě, ale i přesto jsou zde i stinné stránky doprovázející užívání této technologie. Dodnes zůstává nejasné, jak přesně jsou využívány všechny záběry, které jsou shromažďovány. Bylo však zjištěno, že moderní technologie jsou ve Spojených arabských emirátech užívány k všudypřítomnému sledování veřejných prostor, internetovým aktivitám, a dokonce i telefonů a počítačů, především pak zařízení vlastnící aktivisté či nepohodlné osoby.[49] Dochází tak k porušování práva na soukromí, svobodu projevu, sdružování a dalších práv a svobod.[50]

2.2.2. Čína

Čínská policie vytvořila jeden z nejdokonalejších sledovacích systémů na světě čítající milióny kamer spolu s výkonným softwarem pro rozpoznávání obličejů a naprogramovala jej tak, aby tento systém identifikoval občany v dané lokalitě. Dle mluvčího komunistické strany

[46]Dubai Police to use biometrics to prevent crime. In: *Gulf News*. [online]. 20. 2. 2017 [cit. 03.07.2024]. Dostupné z: https://gulfnews.com/uae/dubai-police-to-use-biometrics-to-prevent-crime-1.1981638; Dubai Police develop next-gen video surveillance biometrics, solve 3,000 crimes In: *Arabian Business* [online] 15. 3. 2023 [cit. 03.07.2024]. Dostupné z: https://www.arabianbusiness.com/industries/technology/dubai-police-develop-next-gen-video-surveillance-biometrics-solve-3000-crimes.

[47] Dubai Police to introduce advanced body scanners to accurately identify suspects. In: *Zawya.* [online]. [cit. 03.07.2024]. Dostupné z: https://www.zawya.com/en/legal/crime-and-security/dubai-police-to-introduce-advanced-body-scanners-to-accurately-identify-suspects-q1qbg9lk.

[48] World's first AI EagleEye Intelligent Patrol by Zenith makes a groundbreaking debut at Intersec Dubai. In: *Gulf News.* [online]. 20.1.2023 [cit. 03.10.2024]. Dostupné z: https://gulfnews.com/business/corporate-news/worlds-first-ai-eagleeye-intelligent-patrol-by-zenith-makes-a-groundbreaking-debut-at-intersec-dubai-1.1674220000046.

[49] Stop governments spying on activists. In: *Amnesty International* [online]. 6. 10. 2020 [cit. 03.07.2024]. Dostupné z: https://www.amnesty.org/en/latest/campaigns/2020/10/stopspying/.

[50] Human Rights Watch. United Arab Emirates: Events of 2022. In: *World Report 2023* [online]. 2023 [cit. 03.07.2024]. Dostupné z: https://www.hrw.org/world-report/2023/country-chapters/united-arab-emirates.

na síti X byl systém v roce 2018 schopen naskenovat až 1,4 miliard obličejů lidí v jedné sekundě.[51] Jen ve městě Taiyuan bylo dle záznamů z roku 2019 provozováno v průměru na 1000 obyvatel 119.57 kamer.[52] Přestože tyto systémy mají v Číně primárně sloužit k zajištění větší bezpečnostni a napomáhat policii dopadnout pachatele trestných činů, systém je velice často zneužíván ke sledování disidentů, etnických menšin či migrujících pracovníků.

Čínská vláda je soustavně kritizována za využívání FR systém k porušování práv přibližně 11 miliónů ujgurských muslimů.[53] Vláda se tak pomocí sítě kamer a FR systému snaží tuto minoritu vystopovat a uchovává záznamy o jejich dennodenních aktivitách a pohybech. Tato technologie umožňuje vládě ujgurskou minoritu nejprve vystopovat a následně jsou příslušníci této menšiny násilně přesídleni do detenčních center nacházející se v západních regionech Číny. Zde je v současné době protiprávně drženo na několik miliónů ujgurských muslimů.[54] Čínská vláda je ovšem kritizována také za testování pokročilejší verze FR systému, konkrétně systému, který dokáže odhalit stavy emocí. Tento systém je testován na Ujgurech v provincii Xinjiang, přičemž dokáže nejen detekovat konkrétní emoci jednotlivce, ale je také schopen vytvořit koláčový graf ze souhrnu detekovaných emocí jednotlivce.[55]

Mimo to do roku 2023 čínská vláda implementovala ve 43 čínských modelových městech zkušební program tzv. sociálního kreditního systému.[56] Tyto systémy, nejen na základě rozpoznávání obličejů, detekují jednotlivce a následně tyto jednotlivce hodnotí na podkladě svého chování tzv. skórem. Kredit jednotlivce je tak zvyšován či snižován dle například dodržování legislativy, spáchání přestupků či trestných činů, ekonomického a

---

[51] DAVIES, Dave. Facial Recognition And Beyond: Journalist Ventures Inside China's „Surveillance State". *NPR* [online]. 2021 [cit. 03.07.2024]. Dostupné z: https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta.

[52] The Top 10 Most Surveilled Cities in the World. In: *US News* [online]. 2020 [cit. 26.09.2024]. Dostupné z: https://www.usnews.com/news/cities/articles/2020-08-14/the-top-10-most-surveilled-cities-in-the-world.

[53]MITSILEGAS, Valsamis. *Surveillance and privacy in the digital age: European, transatlantic and global perspectives*. Oxford, UK ; New York, NY: Hart Publishing, an imprint at Bloomsbury Publishing, 2021, s. 206. ISBN 9781509925179.

[54] China's camps to erase Muslim beliefs. In: *Amnesty Internationa*l [online]. 15.3.2024 [cit. 03.10.2024]. Dostupné z: https://www.amnesty.org.uk/chinas-uighur-muslims-truth-behind-headlines.

[55] BROWN, Tristan G., STATMAN, Alexander, SUI, Celine. Public Debate on Facial Recognition Technologies in China. *MIT Case Studies in Social and Ethical Responsibilities of Computing*. MIT Schwarzman College of Computing, 2021, č. Summer 2021. DOI: 10.21428/2c646de5.37712c5c.

[56] KNIGHT, Adam. Technologies of Risk and Discipline in China's Social Credit System. In: CREEMERS, R. J. E. H., TREVASKES, S. *Law and the Party in China: Ideology and Organisation*. Cambridge: Cambridge University Press. 2020. s. 237-263. Dostupné z: https://www.cambridge.org/core/books/abs/law-and-the-party-in-china/technologies-of-risk-and-discipline-in-chinas-social-credit-system/9C07910C3EF48B555D3D481BDB6A0A9E.

sociálního chování ba dokonce i způsobu chování na internetu a využívání digitálních technologií. Výše tohoto skóre pak ovlivňuje dostupnost služeb, cestování či přístup ke vzdělání a pracovním pozicím.

2.2.3. Rusko

I přes chybějící legislativu omezující využívaní FR systémů je užívání této technologie v Rusku velice rozšířené, a to zejména od roku 2017, kdy Moskva oznámila zahájení užívání FR systémů. Díky rozsáhlému kamerovému systému čítající přes 160 000 kamer, přičemž více než 3000 z nich je napojeno na FR systém, hrál FR systém roli ve více než 2000 soudních řízeních.[57] V posledních letech moskevské úřady využívají tuto technologii k identifikaci a stíhání nejen pachatelů trestných činů, ale také stíhání zejména pokojných demonstrantů, či k identifikaci a následnému zadržování odvedenců, kteří se snaží vyhnout mobilizaci do války na Ukrajině.[58] Díky výsledkům této technologie moskevské oddělení informačních technologií plánuje rozšířit kapacitu moskevského systému do dalších regionů.

[57] How facial recognition is helping Putin curb dissent. *Reuters* [online]. 2023 [cit. 03.07.2024]. Dostupné z: https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/.

[58] Russia Uses Facial Recognition to Hunt Down Draft Evaders In: *Human Rights Watch* [online]. 2022 [cit. 03.10.2024]. Dostupné z: https://www.hrw.org/news/2022/10/26/russia-uses-facial-recognition-hunt-down-draft-evaders.

3. Využití FR systémů k hledání osob

FR systémy se ve světě stále častěji využívají v souvislosti s monitorováním veřejných prostor. Kamerové systémy, zejména pak kamerové systémy uzavřeného okruhu známé pod pojmem CCTV kamery, jsou přímo napojeny na FR systémy, což umožňuje nepřetržité sledování a analýzu záznamů z bezpečnostních kamer umístěných na veřejných místech, jako jsou náměstí, parky, dopravní uzly a nákupní centra. Tato technologie umožňuje vyhledat a lokalizovat osoby, které nejsou jen podezřelé z trestné činnosti, ale také osoby hledané nebo považované za bezpečnostní hrozbu. Při užití FR systému tento systém sdělí informaci o rozpoznání hledané osoby operátorovi, který vyhodnotí výsledek a rozhodne se, jak s danou informací naloží a zda například informaci o lokalizaci sdělí příslušnému strážníkovi.

Současná technická vyspělost a pokrytí kamerovými systémy v České republice (na které by bylo možné FR technologii napojit) sice nelze v současné chvíli zcela připodobňovat například ke kamerovému pokrytí v Číně, avšak trend zvyšování počtu kamer je na vzestupu. V případě rostoucího trendu umisťování kamer ve veřejném prostoru v České republice by tak mohlo býti v budoucnu možné, aby člověk pohybující se mimo domov byl pod neustálým dohledem kamerových systémů. Policie v současné chvíli provozuje informační systém Digitální podoba osob ke zpětné identifikaci jednotlivců neznámé totožnosti, přičemž nejčastěji se jedná o případy mrtvých osob nebo neznámých pachatelů závažných trestných činů. Je ale otázkou, zda-li má takovýto systém (případně jakýkoli jiný FR systém tohoto typu) zákonný podklad ke svému provozu.

3.1. Zákonná úprava

3.1.1. Relevantní právní normy

Aby mohl být FR systém využíván ke hledání osob, je zapotřebí relevantní právní úprava poskytující pro jeho užívání zákonný podklad. Dle zásady enumerativnosti veřejnoprávních pretenzí, která vyplývá přímo z čl. 2 odst. 2 Listiny a čl. 2 odst. 3 Ústavy, lze státní moc uplatňovat orgány veřejné moci jen v případech, mezích a způsoby, které stanoví zákon. Smyslem této zásady je zamezit, aby nedocházelo k libovůli ze strany orgánů veřejné moci.

Takovéto zákonné zmocnění, které by konkrétně umožňovalo užívání FR systémů, však v zákoně nenajdeme. Je proto zapotřebí hledat v ustanoveních zákona č. 273/2008 Sb., zákona o Policii České republiky, které sice neobsahují ani zmínku o užívání FR technologie, ale obsahují alespoň ustanovení potenciálně vztahující se k užívání FR systémů. Mimo jiné pak tento zákon zřizuje samotnou Policii. Dle §6 tohoto zákona je Policie je státním útvarem podřízeným Ministerstvu vnitra, který je tvořen policejním prezidiem České republiky, útvary

policie s celostátní působností krajskými ředitelství policie a útvary zřízené v rámci krajského ředitelství. Současně je také jednotným ozbrojeným bezpečnostním sborem, který má celostátní působnost. Mimo to je Policie policejním orgánem, který patří společně se soudem a státním zástupcem mezi OČTŘ dle §12 TRŘ.

Do věcné působnosti Policie patří pátrání po osobách jako součást plnění úkonů Policie, a to dle §68 odst. 1 zákona o Policii České republiky, dle kterého může Policie zahájit takovéto pátrání pro hledané nebo pohřešované osoby. Pro účely této práce se však budeme zaměřovat pouze na hledané osoby. V případě hledaných osob, po kterých probíhá pátrání dle §68 zákona o Policii České republiky, se jedná zejména o osoby podezřelé ze spáchání trestného činu, obviněné, osoby odsouzené a další. V praxi je pak pátrání rozlišováno na administrativní a výkonné. Administrativní pátrání představuje vytváření a aktualizování informačních systémů, které pak mohou být Policií užity během samotného pátrání. V případě výkonného pátrání pak může Policie využít osobního pátrání, které je vykonáváno policisty při výkonu služebních povinností, přičemž se jedná o nejčastější a nejběžnější způsob výkonného pátrání. Mimo to lze také využít pátracích akcí, kterými se rozumí *„jednorázové, časově a prostorově omezené nasazení většího počtu sil a prostředků směřující k vypátrání objektu pátrání.“*[59] Ke své práci Policie využívá různé pátrací prostředky a pomůcky, operativně pátrací prostředky, uveřejnění informací v médií, kriminalisticko-technické prostředky a jiné.

Při pátrání po osobách za využití FR systému je užívána také referenční databáze digitálních fotografií fyzických osob, ze kterých FR systém čerpá. Zákonnou oporu k požadování a následnému využití státem již nashromážděných údajů v databázích můžeme hledat v §66a odst. 1 zákona o Policii České republiky, dle kterého *„policie může od správce evidence nebo zpracovatele získávat a dále zpracovávat digitální fotografie a agendové identifikátory fyzických osob vedené v informačním systému evidence občanských průkazů, cestovních dokladů, diplomatických a služebních pasů, registru řidičů, centrálním registru řidičů, nebo informačním systému cizinců.“*[60] *„Tyto osobní údaje pak Policie může využívat pouze pro identifikaci konkrétní osoby při plnění účelů uvedených v § 79 odst. 1.“* [61] Přestože toto ustanovení přímo neupravuje užití ani zpracování osobních údajů FR systémy, může být toto ustanovení zákonným podkladem pro užívání FR systémů.

[59] Čl.12 písm. e) odst.1 závazného pokynu policejního prezidenta č. 135/2010.
[60] §66a odst. 1 zákona č. 273/2008 Sb. o Policii České republiky.
[61] §66a odst. 3 zákona č. 273/2008 Sb. o Policii České republiky.

Povolení k provozu databází digitálních fotografií fyzických osob není však to jediné, co je v souvislosti s užíváním FR systémem potřeba. Je zapotřebí zajistit zákonný podklad ke zpracovávání osobních dat z kamerových záznamů. Takovéto zákonné zmocnění lze nalézt v §60 odst. 1 zákona o Policii České republiky, dle kterého Policie *„zpracovává informace včetně osobních údajů v rozsahu nezbytném pro plnění svých úkolů“*. Tyto údaje je však možné zpracovávat pouze 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.“* [62] Co je však zákonem o Policii České republiky považováno za osobní údaje, které lze v databázích shromažďovat, tento zákon neupravuje. Proto je třeba nahlédnout do zákona č. 110/2019 Sb. o zpracování osobních údajů, přesněji §24 odst. 1 tohoto zákona, dle kterého se ustanovení hlavy III zákona o zpracování osobních údajů použije také při zpracování osobních údajů Policií ČR za účelem odhalování trestné činnosti, stíhání trestných činů apod. §24 odst. 2 tohoto zákona pak říká, že pro účely hlavy III se použije čl. 4 bod 1 nařízení GDPR, které již osobní údaje definuje. Dle tohoto nařízení jsou osobními údaji *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě.“*[63] Jak již bylo zmíněno výše, biometrické údaje jsou vždy údaji osobními. Je zapotřebí však připomenout, že nařízení GDPR se krom výjimek neuplatní v případech automatizovaného ani neautomatizovaného zpracování osobních údajů, které jsou zpracovávány *„za účelem prevence, vyšetřování, odhalování či stíhání trestných činů.“*[64] Ohledně uchovávání osobních údajů v databázi může Policie osobní údaje v evidenci uchovávat pro již výše zmiňované účely stanovené v §79 odst. 1 tohoto zákona po neomezeně dlouhou dobu.[65]

Policie při své činnosti musí také pořizovat spoustu druhů záznamů, mezi které patří automatizované záznamy o zpracování osobních údajů. [66] Jedná se o tzv. logy, které požadují pořizování záznamů *„alespoň o operacích shromáždění, vložení, pozměnění, kombinování, nahlédnutí, předání, sdělení a výmazu osobních údajů,“* přičemž tyto záznamy je možné *„užít pouze pro účely trestního řízení, ověření zákonnosti zpracování osobních údajů, zajištění neporušenosti zabezpečení osobních údajů a zajištění plnění úkolů.“* [67] Logy tak uchovávají záznamy o všech manipulacích s osobními údaji, včetně informací o manipulující osobě.

[62] §79 odst.1 zákona č. 273/2008 Sb. o Policii České republiky.
[63] Čl. 4 bod 1 nařízení GDPR.
[64] Čl. 2 odst. 2 písm. d) nařízení GDPR.
[65] §87 odst.1 zákona č. 273/2008 Sb. o Policii České republiky.
[66] §36 zákona č. 110/2019 Sb. o zpracování osobních údajů.
[67] §16 odst. 1 písm. b) zákona č. 110/2019 Sb. o zpracování osobních údajů.

„Takové opatření má vysoký preventivní účinek proti zneužití údajů z informačního systému, neboť každý, kdo s ním oprávněně pracuje, si musí být vědom, že je možno zpětně ověřit, kdo, kdy a jakým způsobem s informačním systémem pracoval a zda se tak dělo oprávněně.“[68] Tyto záznamy pak mohou být uchovávány až po dobu 3 let. [69] Pokud by byl tedy kamerový záznam zpracován FR systémem, toto zpracování musí být zaznamenáno alespoň formou automatizovaně pořizovaných záznamů.

V případě, kdy Policie osobní údaje zpracovává pro účely uvedené v § 79 odst. 1 zákona o Policii České republiky bez vědomí fyzických osob, musí fyzické osoby zpětně informovat o tomto zpracování. [70] Musí tak učinit ale až v situaci *„kdy není ohroženo plnění úkolů policie při předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů…“*[71] Z této informační povinnosti však existují 2 výjimky, a to pokud by sdělení těchto informací vyžadovalo neúměrné úsilí, jako například nemožnost vyhledat bydliště fyzické osoby, nebo pokud by byly tyto záznamy bez zbytečného odkladu vymazány.[72]

V případě, kdy jsou FR systémy napojeny na bezpečnostní kamery monitorující veřejný prostor, je třeba hledat také zmocnění pro provozování kamerových systémů. To je možné nalézt v §62 zákona o Policii České republiky, na základě kterého je Policie oprávněna *„pořizovat zvukové, obrazové nebo jiné záznamy osob a věcí nacházejících se na místech veřejně přístupných.“* V případě, že kamerové systémy ukládají kamerové záznamy, jedná se o automatické kamerové systémy, které systematicky zpracovávají osobní údaje. Na základě samotné existence těchto záznamů neexistuje informační povinnost vůči osobám zachycených na těchto kamerových záznamech. Je ovšem nutné, aby Policie zveřejnila informace o zřízení těchto systémů vhodným způsobem. Za běžných okolností mohou být kamerové záznamy uchovávány nejdéle po dobu 30 dní, avšak výjimku tvoří záznamy pro kriminalistické účely. Tyto kamerové záznamy pak mohou být pro účely stanovené v §79 zákona o Policii České republiky uchovávány déle.

---

[68] Rozsudek Nejvyššího správního soudu ze dne 27.4.2017, č.j. 1 As 134/2016-28. In: *Beck-online* [online]. Nejvyšší správní soud [cit. 3.7.2024]. Dostupné z: https://app-beck-online-cz.ezproxy.is.cuni.cz/bo/document-view.seam?documentId=njuwenjrgu2tqnk7nzzxg&refSource=toc.

[69] §36 zákon č. 110/2019 Sb. o zpracování osobních údajů; §87 odst.2 zákona č. 273/2008 Sb. o Policii České republiky.

[70] §88 zákona č. 273/2008 Sb. o Policii České republiky.

[71] §88 zákona č. 273/2008 Sb. o Policii České republiky.

[72] VANGELI, Benedikt. *Zákon o Policii České republiky. Komentář. 2. vydání*. Praha: C. H. Beck, 2014, s. 351. ISBN 978-80-7400-543-5.

3.1.2. Interpretace právních norem

Právní norma, i přes svou neměnnost a abstraktnost, musí reflektovat dynamiku společnosti. Její abstraktní povaha neumožňuje předvídat všechny možné situace, a proto v jednotlivých případech vyžaduje právní norma interpretaci, aby bylo možné subsumovat konkrétní situace pod její ustanovení. Využívání FR systémů za účelem hledání osob tak vyvolává otázky týkající se jejjch užívání v rámci existujících právních předpisů, v tomto případě zákona o Policii České republiky. Konkrétně pak, zda-li právní úprava umožňuje užívání FR systémů za účelem hledání osob.

Jazykový výklad je základním krokem při interpretaci,[73] kdy jsou jednotlivá ustanovení vykládána na základě gramatického znění. V tomto případě však tento druh výkladu není příliš užitečný, jelikož z právní normy přímo nevyplývá zákaz či povolení užití FR systému. Na základě jazykové interpretace tak není možné vyvodit jasný závěr. Tento druh výkladu však není esenciální, jelikož *„jazykový výklad představuje pouze prvotní přiblížení se k aplikované právní normě. Je pouze východiskem pro objasnění a ujasnění si jejího smyslu a účelu (k čemuž slouží i řada dalších postupů, jako logický a systematický výklad, výklad e ratione legis atd.). Mechanická aplikace abstrahující, resp. neuvědomující si, a to buď úmyslně nebo v důsledku nevzdělanosti, smysl a účel právní normy, činí z práva nástroj odcizení a absurdity.“*[74] Ani jiné základní metody interpretace práva dle mého názoru nevedou k jasné odpovědi, proto je zapotřebí ustanovení zákona o Policii České republiky podrobit zvláštním metodám interpretace, jako je například historický nebo teleologický výklad.

Při historickém výkladu je nutné zkoumat účel normy za pomocí okolností, za kterých byla právní norma přijata, stejně tak jako je zapotřebí zkoumat vůli zákonodárce, [75] například za pomocí důvodové zprávy. Tato metoda interpretace však nepůsobí osamoceně, ale je třeba na ni nahlížet v kontextu zbylých interpretačních metod. Zákon o Policii České republiky nabyl účinnosti v roce 2009, kdy technologie rozpoznávání obličeje ještě nebyla rozvinuta v rozsahu, jaký známe dnes. V roce 2009 mohly být zamýšlené postupy Policií spíše založeny na tradičních formách identifikace jako je například práce s fotografiemi a záznamy z bezpečnostních kamer, které nebyly schopny automatické analýzy biometrických dat. I když tehdy zákonodárce pravděpodobně nepředpokládal užívání FR systémů, v roce 2019 došlo

[73] WINTR, Jan. *Metody a zásady interpretace práva.* Praha: Auditorium, 2013. s. 45. ISBN 978-80- 87284-36-0.
[74] Nález Ústavního soudu České republiky ze dne 29. 7. 2013, sp. zn. I. ÚS 671/13. In: *Nalus* [online]. Ústavní soud [cit. 26.9.2024]. Dostupné z https://nalus.usoud.cz/Search/GetText.aspx?sz=1-671-13_1.
[75] MELZER, Filip. *Metodologie nalézání práva: úvod do právní argumentace.* Praha: C.H. Beck, 2010. s. 120. ISBN 978-80-7400-149-9.

k novele zákona o Policii České republiky, na základě které došlo k přidání §66a, který Policii umožňuje přístup k fotografiím z civilních evidencí. Tento nový právní rámec je zásadní pro fungování FR systémů. Účel této novely je patrný také z důvodové zprávy, dle které *„navrhovaná změna přináší policii možnost softwarového vyhledávání a rozpoznávaní obličejů, která v případě potřeby dokáže významným způsobem zkrátit čas k odhalení pachatele, případně zabránit dalším hrozícím útokům.“* [76] Policie tak prostřednictvím tohoto ustanovení získala oprávnění k požadování a následnému využití státem již nashromážděných údajů, což umožňuje provoz referenční databáze digitálních fotografií, konkrétně pak databází informačního systému Digitální podoba osob. Zatímco tak dle mého názoru není možné předpokládat, že zákon o Policii České republiky před novelou předpokládal využití takto pokročilých technologií, po přijetí novely zakotvující §66a dle mého názoru takovýto úmysl dovodit lze.

Teleologický výklad se pak zaměřuje na vlastní účel a smysl právní normy,[77] který se neurčuje podle původní představy zákonodárce při jejím přijetí, nýbrž podle toho, jaký by tento účel měl být z pohledu ideálního zákonodárce, pokud by bral v úvahu dnešní společenské okolnosti. *„Teleologické výkladové metody jako interpretační přístup nelze pominout z ústavněprávního hlediska a je způsobilý v kontextu racionální argumentace představovat významný korektiv při zjišťování obsahu právní normy.“*[78] Účelem upraveným v zákoně o Policii České republiky je mimo jiné ochrana veřejného pořádku, zajištění bezpečnosti osob, majetku a předcházení trestných činů. S ohledem na účely této právní úpravy a relevantní paragrafy zmíněné výše může FR systém významně přispět k dosažení těchto účelů, zejména pokud jde o efektivitu a rychlost dosažení cílů.

Výklad norem zákona o Policii České republiky z pohledu teleologického výkladu ve spojení s historickou interpretací práva tedy nasvědčuje tomu, že provozování FR systému má zákonný podklad.

3.2. Zásah do práva na soukromí

Zákonný podklad pro užívání FR systému však nestačí. V případě, kdy je veřejnou mocí zasahováno do základních práv a svobod z důvodu prevence a ochrany před trestnou činností,

---

[76] Důvodová zpráva k zákonu č. 111/2019 Sb., změna některých zákonů v souvislosti s přijetím zákona o zpracování osobních údajů [k § 66a zákona č. 273/2008 Sb.] [Systém Beck-online]. [cit. 03.10.2024]. Dostupné z: https://app-beck-online-cz.ezproxy.is.cuni.cz/bo/chapterview-document.seam?documentId=oz5f6mrqge4v6mjrgfpwi6q&rowIndex=0.

[77] WINTR, Jan. *Metody a zásady interpretace práva.* Praha: Auditorium, 2013. s. 123. ISBN 978-80-87284-36-0.

[78] Nález Ústavního soudu České republiky ze dne 6. 2. 2009, sp. zn. II.ÚS 3201/08. In: *Nalus* [online]. Ústavní soud [cit.26.9.2024]. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=2-3201-08.

lze takovýto zásah umožnit jen skrze imperativní zákonnou úpravu (tj. úpravu, obsahující principy právního státu a naplňující test proporcionality).[79] Takovýto zákonný podklad pro přípustnost omezení základních práv a svobod vychází z čl. 4 odst. 2 Listiny, dle kterého „*meze základních práv a svobod mohou být za podmínek stanovených Listinou základních práv a svobod upraveny pouze zákonem*." V případě, kdy Listina nestanovuje omezení práv v konkrétních článcích, je takovéto omezení možno uskutečnit pouze výhradou zákona. Zákonodárce má tak větší míru uvážení pro stanovení konkrétních mezí, avšak je nucen brát zřetel, že omezení musí platit stejně pro všechny případy a zároveň je nucen šetřit jejich podstaty a smyslu.[80] Tento limit minimalizace zásahu do základních práv a svobod je pak součástí testu proporcionality.

V případě užívání FR systému dochází k intenzivnímu zásahu do práva na soukromí. Koncept práva na soukromí prochází s plynutím času silným vývojem. Primární úzké pojetí soukromí lze ilustrovat na rozhodnutí Ústavního soudu, podle kterého: *„Soukromý život obecně chrání možnost jednotlivce žít svůj život bez nepřiměřených zásahů a narušení. V základech tohoto práva je koncept svobody ve smyslu „být nechán na pokoji", tedy existence nějaké soukromé zóny, do které by neměl nikdo vstupovat či zasahovat. Tuto zónu lze chápat jak prostorově, tak i co se týče rozhodování o vlastní osobě. Funkcí práva na respekt k soukromému životu je zajistit prostor pro svobodu člověka."*[81]

Postupem času se pojetí soukromí rozvinulo, aby nabídlo doplňkovou, širší ochranu osobní svobody jednotlivce, což umožňuje jeho seberealizaci v rámci sociálních, včetně rodinných a společenských vztahů. Právo na soukromí tak má multidimenzionální povahu, což může být s postupem času a s měnícím se pojetí tohoto práva lehce problematické. Oproti čl. 8 Úmluvy, který zakotvuje právo na soukromý život a všechny dimenze práva na soukromí pokrývá, Listina jednotlivé aspekty deklaruje na různých místech. Těmito aspekty je „*právo na soukromí v prostorové dimenzi (tj. ochrana obydlí zakotvená v čl. 12), právo na rodinný život (čl. 10 odst. 2), právo na ochrana komunikace (tj. listovní tajemství ve smyslu čl. 13) a právo na informační sebeurčení (právo na ochranu osobních údajů dle čl. 10 odst. 2)."* [82] Mezi další aspekty bývá také řazena ochrana osobnostních práv (čl. 10 odst. 1)

[79] Nález Ústavního soudu České republiky ze dne 22.3.2011, sp. zn Pl. ÚS 24/10. In: *Nalus* [online]. Ústavní soud [cit. 3.7.2024]. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-24-10_1.

[80] Čl. 4 odst. 3 a 4 Listiny.

[81] Nález Ústavního soudu ze dne 15.12.2015, sp. zn. I. ÚS 1587/15. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024]. Dostupné z: https://www.usoud.cz/fileadmin/user_upload/Tiskova_mluvci/Publikovane_nalezy/.

[82] Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024]. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-24-10_1.

a nedotknutelnost osoby (ve smyslu čl.7 odst. 1 Listiny). [83] Analýza záznamů za pomocí FR systému však zasahuje zejména do aspektu práva na informační sebeurčení zaručeného na základě čl. 10 odst. 3 Listiny, dle které má *každá právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě*. Právem na ochranu osobních údajů jakožto aspektem práva na soukromí se tak budu v následujících odstavcích zabývat.

V případě, kdy jsou osobní údaje FR systémem zpracovávány a vzhledem k povaze, rozsahu, okolnostem nebo účelu hrozí vysoké riziko neoprávněného zásahu do práv a svobod subjektů údajů, je zapotřebí provést posouzení vlivu takového zpracování.[84] V roce 2023 Policie zpracovala posouzení vlivů na ochranu osobních údajů pro informační systém Digitální podoba osob, avšak je třeba upozornit, že toto zpracování proběhlo až poté, co Policie začala Informační systém Digitální podoba osob provozovat.

Právo na ochranu osobních údajů je právem, které v sobě zahrnuje *„právo jednotlivce rozhodnout podle vlastního uvážení, zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům.“*[85] Rozlišování, zda se jednotlivec nachází v soukromém či veřejném prostoru však z pohledu práva na soukromí není významné. Pokud dochází k provádění jednání na veřejném místě, *„neznamená to, že se osoba vzdává svého práva na soukromí.“*[86]

Užívání FR systému společně s kamerovými systémy na veřejných místech vede k tomu, že každý, kdo se pohybuje na těchto veřejných místech, může být Policií za pomocí FR systému nepřetržitě sledován a monitorován, aniž by o tom věděl nebo dal souhlas. Je zřejmé, že při pohybu na veřejném prostranství může každý rozumně předpokládat, že je ostatními lidmi pozorován. Jinak je tomu v případě, kdy je záznam zachycující pohyb osob či kontakt s lidmi ukládán. *„Soukromý život tak může být dotčen, pokud budou data systematicky či nepřetržitě zaznamenávána. Zásahem do soukromého života je poté, spíše než samotné monitorování až přechovávání či použití záznamu tohoto monitorování*.“[87] Dle Ústavního

[83] KOKEŠ, Marian. Článek 10 In: HUSSEINI, F., BARTOŇ, M., KOKEŠ, M., KOPA, M. a kol. *Listina základních práv a svobod. Komentář. 1. vydání*. [Systém Beck-online]. Praha: C. H. Beck, 2021. ISBN 978-80-7400-812-2. Dostupné také z: https://app-beck-online-cz.ezproxy.is.cuni.cz/bo/document-view.seam?documentId=nnptembsgfpwk232ge4texzrfzrwymjq.

[84] §37 zákona č. 110/2019 Sb. o zpracování osobních údajů.

[85] Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024]. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-24-10_1.

[86] WAGNEROVÁ, Eliška. Právo na soukromí: Kde má být svoboda, tam musí být soukromí. In ŠIMÍČEK, Vojtěch, ed. *Právo na soukromí*. Brno: Muni Press, 2011.s. 51. ISBN978-80-210-5449-3.

[87] KRATOCHVÍL, Jan. Článek 8 In: KMEC, J., KOSAŘ, D., KRATOCHVÍL, J., BOBEK, M. *Evropská úmluva o lidských právech. Komentář. 1. vydání.* [Systém Beck-online]. Praha: C. H. Beck, 2012. s. 863 – 962. ISBN:

soudu „*monitorování veřejného místa kamerou a následné pořízení trvalého záznamu spadá pod ochranu poskytovanou čl. 10 Listiny a čl. 8 odst. 1 Úmluvy. Obecně je pro účely hodnocení, zda došlo k nedovolenému zásahu do soukromí ze strany orgánů veřejné moci, nutno zkoumat, zda byla zaznamenána soukromá záležitost či veřejná událost a zda byl získaný materiál určen pro omezené použití či měl být dostupný široké veřejnosti.*“[88] Provozování kamerových systémů a monitorování veřejného prostranství je pouze část problematiky, která s užíváním FR systémů souvisí.

Podstatnějším zásahem do práva soukromí a ochranu osobních údajů je zpracování biometrických údajů bez vědomí osob, které jsou kamerami zachyceny a za pomocí FR lokalizovány či sledovány. Mimo to v případě nedostatečného zabezpečení FR systémů hrozí zneužití této technologie, kdy mohou být osobní údaje zpracovávány mimo schválené účely, popřípadě se k osobním údajům může dostat osoba, která by k FR systému neměla mít přístup. Problematické se pak z pohledu práva na ochranu osobních údajů jeví také uchovávání fotografií osob, respektive jejich biometrických údajů v referenčních databází po neomezeně dlouhou dobu bez návaznosti na předchozí trestněprávní minulost osob (k této problematice blíže v kapitole č. 6).

3.2.1. Test proporcionality

Právo na soukromí není právem absolutním. Oproti Listině však čl. 8 odst. 2 Úmluvy stanovuje požadavky pro dovolené zásahy do tohoto práva. Je zapotřebí, aby byl zásah v souladu s právním řádem a zároveň, nezbytný v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti…V případě požadavku užívání FR systémů v souladu s právní úpravou bylo ESPL judikováno, že *„osobní data jsou shromažďována a využívána v souladu se zákonem, jen pokud existuje přehledná právní úprava této činnosti a pokud se mohou dotčené osoby účinně domoci, aby soudy přezkoumaly, zda nejsou tato data shromažďována nad míru, která je v demokratické společnosti nezbytná, a zda jsou využívána jen k legitimním účelům.*“[89] V rámci kritéria nezbytnosti v demokratické společnosti je tato nezbytnost úzce spojena s principem proporcionality, což znamená, že *„sledovaný veřejný zájem musí být dostatečně závažný, aby převážil zájem jednotlivce na nezasahování do jeho*

978-80-7400-365-3. Dostupné také z: https://app-beck-online-cz.ezproxy.is.cuni.cz/bo/document-view.seam?documentId=nnptembrgjpwk5tlgyxgg3by.

[88] Nález Ústavního soudu ze dne 8.2.2010, sp. zn. IV.ÚS 2425/09. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024]. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=4-2425-09_1.

[89] Rozhodnutí ESLP ze dne 4. 5. 2000, ve věci Rotaru proti Rumunsku. č. 28341/95.

práv pod čl. 8 odst. 1.“ [90] Samotné zásahy do práva na soukromí jsou pak ESPL posuzovány na základě 5 stupňového testu.

V případě Listiny se jedná o právo relativní, které je možno omezit za účelem ochrany jiného základního práva či veřejného zájmu, který může být reprezentován ústavně chráněnou hodnotou nebo principem. [91] Takováto kolize pak bude posuzována soudem na základě testu proporcionality. Obecně platí, že pokud jde o zásahy do práva na soukromí, je nezbytné, aby byly z právní úpravy zjevné důvody, účel a meze základního práva, [92] což vyplývá z čl. 4 odst. 2 Listiny. K posuzování legality těchto zásahů do práva na informační sebeurčení slouží test proporcionality prováděný Ústavním soudem, který jsem se taktéž rozhodla v této práci provést. Tento test se však ve své podstatě toliko neliší od 5 stupňového testu prováděného ESLP.

Test proporcionality je test s dlouholetou tradicí užívaný Ústavním soudem k posuzování zásahu do ústavně zaručených práv. Jeho první užití lze spatřovat v rozhodnutí Ústavního soudu ze dne 12. října 1994, sp. zn. Pl. ÚS 4/94. Tento test má 3 stupně, kterými jsou vhodnost, potřebnost a proporcionalita v užším slova smyslu. Na rozdíl od 5 stupňového testu ESLP, který je používán pro práva obsažené v Úmluvě, Ústavní soud ČR se zabývá především právy, která jsou zakotvena v Listině. Právo na soukromí, respektive právo na ochranu osobních údajů, je zaručeno jak v Úmluvě, tak v Listině, přičemž oba testy, jak ten užívaný ESLP, tak Ústavním soudem, si jsou v konečném závěru velice podobné. Vedle testu proporcionality je Ústavním soudem užíván také tzv. test racionality, který je užíván pro zjištění vhodnosti zásahu do hospodářských, sociálních a kulturních práv, avšak právo na ochranu osobních údajů mezi tato práva nepatří.

V případě testu proporcionality dochází k poměřování 2 základních práv, popřípadě základního práva s veřejným zájmem. *„Veřejný zájem je třeba chápat jako takový zájem, který by bylo možno označit za obecný či obecně prospěšný zájem.“*[93] FR systémy užívané za účelem hledání osob (pachatelů trestných činů), mohou zpracovávat osobní údaje za účely stanovenými v §79 zákona o Policii České republiky, konkrétně se jedná o *„předcházení,*

[90] KRATOCHVÍL, Jan, Článek 8 In: Kmec, J., Kosař, D., Kratochvíl, J., Bobek, M. *Evropská úmluva o lidských právech. Komentář. 1. vydání*. Praha: C. H. Beck, 2012. s. 863 – 962. ISBN: 978-80-7400-365-3. Dostupné také z: https://app-beck-online-cz.ezproxy.is.cuni.cz/bo/document-view.seam?documentId=nnptembrgjpwk5tlgyxgg3by.

[91] Nález Ústavního soudu ze dne 18. 12. 2006, sp. zn. I. ÚS 321/06. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024]. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=1-321-06.

[92] WAGNEROVÁ, Eliška. Článek 10. In WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK a Ivo POSPÍŠIL. *Listina základních práv a svobod - Komentář*. Wolters Kluwer, 2012, s. 287. ISBN: 978-80-7357-750-6.

[93] Nález Ústavního soudu ze dne 28. 3. 1996, sp. zn. I. ÚS 198/95. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024]. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=1-198-95.

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.“ Zpracování osobních údajů tak vede k naplňování veřejného zájmu, kterým je veřejná bezpečnost. Sám Ústavní soud pak judikoval, že „*stíhání trestných činů a spravedlivé potrestání jejich pachatelů je ústavně aprobovatelným veřejným zájmem.“*[94] V testu proporcionality tak budeme porovnávat právo na ochranu osobních údajů s veřejnou bezpečností.

a) Kritérium vhodnosti

V případě prvního kritéria vhodnosti je třeba posuzovat, zda je prostředek omezující základní lidská práva a svobody schopen dosáhnout stanoveného cíle. Při hledání odpovědi na tuto otázku se primárně zkoumají faktické, nikoliv právní otázky. Pro určení, zda je určitý prostředek vhodný k dosažení cíle však nezáleží na tom, zda bylo cíle skutečně dosaženo, ale spíše na tom, zda by bylo možné dosáhnout sledovaného cíle vybraným prostředkem za normálních okolností.

Dle mého názoru není pochyb, že FR technologie napomáhá k identifikaci hledaných osob. V případě informačního systému Digitální podoby osob, u kterého se úspěšnost pohybuje dle slov Policie mezi 40-45 %, [95] se dle mého názoru jedná o nástroj efektivní. Tato na první pohled poměrně vysoká chybovost je dle slov Policie způsobena nízkou kvalitou vstupních fotografií, nejedná se tedy o neschopnost systému jako takového.

Problematická je však dle mého názoru konkrétně chybovost FR systému u osob jiné než bílé pleti, která je způsobena samotným algoritmem systému. Chybovost informačního systému Digitální podoba osob není známa, proto pro účely této práce budu vycházet ze závěrů studií zkoumající jiné FR systémy. Studie z roku 2018, která byla provedena společností Gender Shades ukázala, že existují podstatné rozdíly v přesnosti systémů rozpoznávající obličeje u rozdílných demografických skupin. Tato studie prokázala, že tři jimi vybrané a zkoumané algoritmy dobře nezvládaly rozpoznání tváří žen tmavé pleti, přičemž největší chybové odchylky při rozpoznávání obličejů byly zjištěny právě v případě těchto žen, u kterých byly tyto odchylky o 34% výrazně vyšší než u mužů bílé pleti. V případě mužů bílé

[94] Nález Ústavního soudu ze dne ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024]. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-24-10_1.

[95] Vyjádření k provozování informačního systému Digitálních podob osob In: Policie [online]. 20. července 2023. [cit. 2.10.2024]. Dostupné z: https://www.policie.cz/clanek/vyjadreni-k-provozovani-informacniho-systemu-digitalnich-podob-osob.aspx.

pleti pak chybovost činila pouhé 1 %. [96] Výrazně vyšší chybovost FR systémů u žen tmavé pleti byla pak potvrzena i v případě jiných studií, jako je například studie provedena Národním institutem pro standardy a technologie v USA, která svou studii provedla na 189 algoritmech.[97] Z těchto výzkumů lze tedy dovodit, že v případě identifikace osob jiné, než bílé pleti existuje riziko vysoké míry nepřesnosti algoritmů FR systémů. Opak je ale pravdou. Tato chybovost FR systémů je způsobena tím, že ve většině případů je algoritmus systému v největší míře testován na fotografiích osob bílé pleti. Této chybovosti je tak možné velice snadno předejít, pokud budou algoritmy FR systémů trénovaný intenzivněji na skupinách, u kterých k chybovosti dochází.[98] Je navíc prokázáno, že díky současným moderním technologiím analýza dat umožňuje vědcům vylepšit algoritmus v případě zjištění vyšší míry falešné pozitivity pro určité demografické skupiny. [99] Z tohoto důvodu se domnívám, že FR systém může být vhodným nástrojem pro hledaní osob.

b) Kritérium potřebnosti

V rámci zkoumání kritéria potřebnosti je nutné posoudit, zda by stanoveného cíle nebylo možné dosáhnout jinými prostředky, které by toliko nezasahovaly do ústavně zaručeného práva, popřípadě by představovaly alespoň méně intenzivní zásah, respektive nejlépe by se o zásah do základního práva nejednalo vůbec.[100] V případě účelu nalezení hledané osoby může FR systém velice zjednodušit a urychlit práci kriminalistů oproti klasickému pátrání ve smyslu §68 odst. 1 zákona o Policii České republiky, které Policie provádí jako součást plnění svých povinností. K samotnému vyhlášení pátrání není třeba souhlas státního zástupce či soudce, naopak je vyhlašováno Policií na základě vlastního rozhodnutí, popřípadě na základě žádosti jiných osob.

Obrovskou výhodou FR systémů oproti klasickému výkonnému pátrání během služby strážníků je, že FR systém dokáže analyzovat záznam během velice krátkého času, proto

[96] BUOLAMWINI, Joy, GEBRU, a Timnit. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* PMLR, 2018 [cit. 04.07.2024]. Dostupné z: https://proceedings.mlr.press/v81/buolamwini18a.html.

[97] GROTHER, Patrick, NGAN, Mei, HANAOKA, Kayee. Face recognition vendor test part 3: demographic effects. Gaithersburg, *MD: National Institute of Standards and Technology*, 2019, s. 7. DOI: 10.6028/NIST.IR.8280.

[98] SMITH, Marcus, MANN, a Monique. Facial Recognition Technology and Potential for Bias and Discrimination. In: *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge University Press, 2024. DOI: 10.1017/9781009321211.008.

[99] LUNTER, Jan. Beating the bias in facial recognition technology. *Biometric Technology Today*. Elsevier, 2020, roč. 2020, č. 9. DOI: 10.1016/S0969-4765(20)30122-3.

[100] GERLOCH, Aleš, TRYZNA, Jan. WINTR, Jan eds. *Metodologie interpretace práva a právní jistota*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2012. s. 263. ISBN978-80-7380-388-9.

v případě nebezpečných osob může mít tato technologie obrovskou zásluhu na prevenci další trestné činnosti díky rychlé identifikaci hledané osoby. Není tedy pochyb, že samotný nástroj FR technologie je silně potřebným prostředkem k hledání pachatelů trestných činů. Dle mého názoru tak v současnosti neexistuje efektivnější nástroj pro identifikaci a lokalizaci osob na rozsáhlém území, ovšem za předpokladu dostatečného kamerového pokrytí území.

S otázkou, zda by nebylo možné stanoveného cíle dosáhnout jinými prostředky, souvisí již zmiňovaná chybovost FR systému u demografických skupin, kterou je zapotřebí vzít do úvahu. Přestože je možné algoritmus vyvinout takovým způsobem, aby byla falešná pozitivita či negativita co možná nejnižší, určitou míru chybovosti není možné zcela vyloučit. Tato chybovost by však měla být korigována obsluhující osobou, která se rozhoduje, jak s informací vygenerovanou FR systémem naloží. FR systém slouží pouze jako podpůrný nástroj k hledání osob. Je třeba brát v úvahu, že i samotní policisté se dopouštění chyb v případě identifikace a pátrání po osobách. K nápravě těchto chyb slouží identifikace konkrétní osoby na místě. Velkou výhodou FR systémů oproti klasickému výkonnému pátrání je, že je velice těžké až nemožné umělou inteligenci oklamat výrazným líčením nebo změnou účesu, zatímco člověka ano. Dále je nutné zohlednit situaci, kdy policista patří k jiné rase, než je hledaná osoba, což vede k tzv. "efektu jiné rasy." Tento efekt spočívá v tom, že lidé rozpoznávají příslušníky své vlastní rasy lépe a přesněji než tváře jiných ras.[101] Z těchto informací tak jasně vyplývá, že ani samotný policista v terénu nemusí být zárukou nechybovosti. FR systém je tak dle mého názoru potřebný prostředek k efektivnímu a rychlému hledání osob.

c) Kritérium proporcionality v užším smyslu

Posledním krokem je proporcionalita v užším smyslu. V rámci tohoto kroku je zjišťováno, zda je prostředek, kterým se snažíme dosáhnout daného cíle, proporcionální, jinými slovy přiměřený tomuto cíli. Během této části testu dochází k individuálnímu posouzení vzájemně se proti sobě stavících základních práv či základního práva s veřejným zájmem. *„Opatření omezující základní lidská práva a svobody nesmějí, jde-li o kolizi základního práva či svobody s veřejným zájmem, svými negativními důsledky přesahovat pozitiva, která představuje veřejný zájem na těchto opatřeních.“*[102]

[101] PHILLIPS, P. Jonathon, An Other-Race Effect for Face Recognition Algorithms. *ACM Transactions on Applied Perception,* 2011. s.2. Dostupné z: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906254.

[102] Nález Ústavního soudu ze dne 13. 8. 2002, sp. zn. Pl.ÚS 3/02. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024]. Dostupné z:https://nalus.usoud.cz/Search/GetText.aspx?sz=pl-3-02.

Ochrana osobních údajů je klíčová pro zachování soukromí jednotlivců, zamezení neoprávněnému sledování a zneužití osobních údajů, zatímco hledání pachatelů trestných činů je nezbytné pro udržení veřejného pořádku a bezpečnosti, ochranu občanů před trestnou činností a následné rychlé zajištění spravedlnosti. V tomto případě je užití FR systémů omezeno na přesně vymezený účel, tedy hledání osob, proto se domnívám, že se jedná o proporcionální nástroj v užším smyslu. Je ovšem zapotřebí, aby užívání takovéhoto systému, který má potenciál silně zasáhnout do práva na soukromí, bylo spojeno s bezpečnostními omezeními. Je proto nutné stanovit bližší podmínky užívání těchto systémů, zejména kontrolních mechanismů, aby nebylo možné zneužít osobní údaje osob.

Policie se vyjádřila k podrobnostem provozování informačního systému Digitální podoba osob. Dle slov Policie *„Policie užívá kontrolní mechanismy, užívané standardně i v jiných informačních systémech, které obsahují citlivé informace,“* [103] přičemž k systému mají přístup pouze určení a vyškolení policisté z Policejního prezidia. [104] Problematické ovšem dle mého názoru je, že konkrétní fungování systémů, omezení a práce s ním není známa. Jeho úprava vychází z interního pokynu prezidenta, ale jeho podstatné části nebyly v celkové délce zveřejněny, tudíž není možné říci, zda jsou kontrolní mechanismy informačního systému Digitální podoba osob dostatečné. Pokud by tedy interní pokyn prezidenta obsahoval dostatečné záruky před zneužitím tohoto nástroje, mohl by být i informační systém Digitální podoba osob považován za proporcionální nástroj.

[103] Částečné poskytnutí informací ze dne 19.3.2024 vydané Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednacím PPR-12351/ČJ-2024-990810.

[104] Aktualizace: Vyjádření k provozování informačního systému Digitálních podob osob - Policie České republiky [online]. [cit. 03.07.2024]. Dostupné z: https://www.policie.cz/clanek/vyjadreni-k-provozovani-informacniho-systemu-digitalnich-podob-osob.aspx.

4. Využití FR systémů k vyhledání důkazů a jejich zajištění

FR systémy mohou v rukou Policie sloužit jakožto nástroj k vyhledávání a zajišťování důkazů, přesněji tedy konkrétních bezpečnostních kamerových záznamů, prokazující relevantní skutečnosti v případě spáchání trestného činu konkrétní osobou. Tyto skutečnosti je systém schopen detekovat jak v reálném čase, tak zpětně, a to díky efektivní analýze rozsáhlých objemů záznamů z bezpečnostních kamer. Je však otázkou, zda může být FR systém použit jako nástroj k vyhledávání a zajišťování důkazů během vyšetřování a zda důkazy získané prostřednictvím této technologie lze využít v trestním řízení.

4.1. Dokazování a relevantní pojmy

Dle §89 odst. 2 TRŘ „*za důkaz může sloužit vše, co může přispět k objasnění věci, zejména výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání.“* Užití pojmu důkaz však může být v tomto kontextu zavádějící. Trestní řád vznikl v době, kdy mezi důkazem a důkazním prostředkem právní teorie nečinila rozdíl, avšak v současné době k rozlišování těchto dvou pojmů dochází, proto je zapotřebí tyto pojmy taktéž rozlišovat. Dnešním pohledem je za důkaz považován přímý poznatek získaný OČTŘ prostřednictvím důkazního prostředku v procesu dokazování. [105] Vždy je však zapotřebí, aby důkaz splňoval základní podmínky, tedy způsobilost k prokázání či vyvrácení tvrzené skutečnosti a dále pak vztah k prokazované skutečnosti.

Naproti tomu důkazní prostředek je nástroj, prostřednictvím kterého jsou důkazy získávány. Konkrétně se jedná o postup orgánu činného v trestním řízení sloužící k získání informací o skutečnostech, které mají být zjištěny za účelem poznání skutkové okolnosti. [106] Je to tedy prostředek sloužící k poznání předmětu důkazu, tj. skutečnosti, která má být zjištěna. TRŘ uvádí pouze demonstrativní výčet možných důkazních prostředků, nikoli taxativní. Jsou jimi například výpověď obviněného, výpověď svědka, věcné a listinné důkazy, znalecké posudky, ohledání, další zvláštní způsoby dokazování. Někdy jsou pak mezi důkazní prostředky zařazovány také operativně pátrací prostředky, ale převládá názor, že takovéto zařazení není správné.[107]

Předmětem samotného trestního řízení je skutek. To znamená, že dokazování probíhá pouze pro vybraný skutek, pro který bylo zahájeno trestní řízení. TRŘ pak v §89 odst. 1

[105] JELÍNEK, Jiří a kol. *Trestní právo procesní 6. vydání*. Leges. 2022. str. 400. ISBN 978-80-7502-550-0.
[106] ŠÁMAL, Pavel. a kol. *Trestní řád I. 7. vydání.* Praha: C. H. Beck, 2013, s. 1333. ISBN: 978-80-7400-465-0.
[107] DRAŠTÍK, Antonín, FENYK, Jaroslav a kol. *Trestní řád. Komentář. II. Díl* [Systém ASPI]. Praha: Wolters Kluwer ČR, 2017, §89, bod. 17. ISBN978-80-7552-601-4. Dostupné z: https://www.aspi.cz/products/lawText/13/61/1/2.

demonstrativně uvádí skutečnosti, které jsou důležité pro trestní řízení, a jsou tak zapotřebí pro daný skutek dokazovat (tj. jsou předmětem dokazování):

a) zda se stal skutek, v němž je spatřován trestný čin,

b) zda tento skutek spáchal obviněný, případně z jakých pohnutek,

c) podstatné okolnosti mající vliv na posouzení povahy a závažnosti činu,

d) podstatné okolnosti k posouzení osobních, rodinných, majetkových a jiných poměrů obviněného,

e) podstatné okolnosti umožňující stanovení následku, výše škody způsobené trestným činem a bezdůvodného obohacení,

f) okolnosti, které vedly k trestné činnosti nebo umožnily její spáchání.[108]

Osoby a orgány, které se podílejí na procesu získávání důkazů, nazýváme subjekty dokazování. Tyto subjekty mají v procesu dokazování různé role a pravomoci upravené TRŘ. Jedná se o OČTŘ, strany trestního řízení a ve specifických případech ostatní osoby, jako je například znalec.

Dokazování v rámci trestního práva procesního představuje specifický a zákonem stanovený postup, který je upraven TRŘ. Cílem tohoto postupuje je získat a poznat relevantní skutečnosti, které jsou klíčové pro rozhodování ve věci. Samotný proces dokazování zahrnuje několik fází. První je vyhledání důkazů, jejichž cílem je identifikovat relevantní skutečnosti, které mohou mít vliv na objasnění skutku. Další důležitou součástí dokazování je procesní zajištění důkazů, což zahrnuje kroky k tomu, aby důkazy nebyly poškozeny, ztraceny nebo pozměněny, a mohly být v průběhu celého řízení spolehlivě využity. Poté následuje provedení důkazů, tedy jejich formální předložení a prezentace v rámci procesu tak, aby mohly být správně hodnoceny a přezkoumávány soudem. V současné době provádění důkazů probíhá zejména v hlavním líčení před soudem. Nakonec OČTŘ přistupují k hodnocení důkazů. Každý důkaz je posuzován jak samostatně, tak ve vzájemné souvislosti s ostatními důkazy, a to proto, aby byl zajištěn co nejpřesnější obraz o skutkovém stavu věci. Cílem je dosáhnout jistoty, zda je obviněný skutečně vinen či nevinen a zajistit spravedlivé rozhodnutí, které je podloženo relevantními a důkladně prověřenými důkazy. Během celého procesu dokazování pak probíhá prověrka důkazů, tedy zjišťování *„kvality pramene důkazu, jeho úplnost, spolehlivost a věrohodnost.“*[109]

[108] §89 odst. 1 TRŘ.

[109] FRYŠTÁK, Marek. *Znalecké dokazování v trestním řízení - 2. vydání*. Wolters Kluwer, 2021. s. 3. ISBN 978-80-7676-063-9.

Relevantní z pohledu této práce, přesněji využívání FR systémů, je však především vyhledávání a zajišťování důkazů. Jak již bylo zmíněno výše, vyhledávání důkazů je proces získávání informací, zda existuje určitý pramen důkazu, který by mohl být použit jako podklady pro rozhodnutí o vině či nevině a objasnit tak všechny základní skutečnosti důležité pro posouzení případu. Vyhledávání důkazů v trestním řízení je založena na zásadě vyhledávací, která je zakotvena v §2 odst. 5 TRŘ. Na základě této zásady mají OČTŘ povinnost z vlastní iniciativy aktivně vyhledávat a zjišťovat všechny skutečnosti, které mohou mít význam pro dané řízení, bez ohledu na to, zda se jedná o skutečnosti ve prospěch nebo v neprospěch obviněného, aby byla zajištěna rovnováha stran a spravedlivé posouzení případu. Policie jakožto OČTŘ tak pečlivě zkoumá všechny okolnosti případu, a to nejen na základě podnětů stran, ale i na základě vlastního zjištění a vlastního úsudku. Povinnost aktivně vyhledávat skutečnosti tak existuje nezávisle na návrzích stran.[110]

Vyhledávání důkazů probíhá v přípravném řízení, kdy sepsáním záznamu o zahájení úkonů v trestním řízení či provedením neodkladného nebo neopakovatelného úkonu je zahájeno trestní řízení, konkrétně fáze prověřování. Během prověřování Policie *„objasňuje a prověřuje skutečnosti důvodně nasvědčujících tomu, že byl spáchán trestný čin.“* [111] Policie tak opatřuje podklady pro své rozhodnutí a zároveň je vhodným způsobem procesně zachycuje a zajišťuje za účelem, aby mohly být v průběhu trestního řízení využity.

V případě, že skutečnosti důvodně nasvědčujících tomu, že byl spáchán trestný čin, Policie zahájí trestní stíhání dle §160 odst. 1 TRŘ, a to pro konkrétní skutek a konkrétní osobu. Zahájením trestního stíhání dochází k přechodu z fáze prověřování do fáze vyšetřování. V této fázi trestního řízení Policie jakožto vyšetřovací orgán *„vyhledává a za stanovených podmínek i provádí důkazy bez ohledu na to, zda svědčí ve prospěch či neprospěch obviněného.“*[112] Vyšetřování pak končí buďto návrhem na podání obžaloby, návrhem na jiné rozhodnutí či jiným způsobem.

4.2. Zákonná úprava

Právní úpravu užívání FR systému za účelem vyhledávání a zajišťování důkazů v TRŘ nenajdeme. Provozování FR systémů a referenčních databází se řídí zákonem o Policii České republiky, který je podkladem pro užívání tohoto systému (viz výše).

[110] NOVOTNÝ, Jiří. Dokazování v trestním řízení. *Forenzní vědy, právo, kriminalistika*. 2024, roč. 9, č. 1. DOI: 10.37355/fvpk-2024/1-01.
[111] §158 odst. 3 TRŘ
[112] §164 odst. 3 TRŘ.

Ne však všechny kriminalistické metody (případně pak kriminalistické prostředky, které využívají kriminalistické metody), které mohou sloužit k vyhledávání důkazů, jsou TRŘ upraveny. Dle judikatury *„žádný úkon, který může přispět k objasnění věci, nelze apriorně vyloučit z okruhu přípustných důkazních prostředků jen proto, že jde o úkon určitého druhu. Má-li úkon obecné náležitosti úkonu podle trestního řádu, lze ho jako důkaz použít, i když trestní řád nemá zvláštní úpravu postupu při tomto úkonu.“*[113] Nelze tak dovodit, že nedostatečná či žádná úprava konkrétního úkonu vedoucího k objasnění věci vede k její nezákonnosti. To by bylo v rozporu s §89 odst. 2 TRŘ, který jelikož uvádí pouze demonstrativní výčet možných důkazních prostředků, nemůže stanovit všechny možné postupy a metody vyhledávání a zajišťování takovýchto důkazních prostředků.

I přesto je zapotřebí, aby úkony Policie s využitím různých kriminalistických metod (respektive kriminalistických prostředků jako je například FR systém) splňovaly jistá kritéria. Je zapotřebí, aby takto TRŘ neupravené kriminalistické metody splňovaly všechny tyto požadavky:

- *„Metoda a způsob její aplikace v kriminalistické praxi nesmí porušovat základní lidská práva a svobody, demokratické a právní principy státní činnosti.*
- *Metoda a způsob její aplikace v kriminalistické praxi nesmí porušovat základní limity a zásady trestního řízení.*
- *Konkrétní metoda a její aplikace musí spolehlivě vést k poznání a prokázání určitých skutečností.“*[114]
- *„Při provádění skutečností jsou dodržovány trestním řádem výslovně stanovené záruky zajištění zákonnosti provádění podobných, v trestním řádu výslovně uvedených úkonů.“*[115]
- *„Konkrétní metoda musí být experimentálně prověřená a teoreticky podložená tak, aby se její výsledky daly označit za průkazné a validní.*
- *Nejedná se o metody právními normami výslovně zakázané a odpovídají požadavkům profesionální etiky.“*[116]

[113] Usnesení Vrchního soudu ze dne 1.07.2016, čj. VSOL 5 To 46/2016. In: *Salvia* [online]. Nejvyšší soud [cit. 26.9.2024]. Dostupné z: https://kraken.slv.cz/VSOL5To46/2016.

[114] PORADA Viktor, POLÁK Peter, a kol. *Kriminalistika*. Plzeň: Aleš Čeněk, 2015. s. 31, 32. ISBN 978-80-7380558-6.

[115] PJEŠČAK, Ján. a kol. *Kriminalistika*. Bratislava: Obzor, 1981. s. 41. ISBN: 65-056-81.

[116] PORADA Viktor, POLÁK Peter, a kol. *Kriminalistika*. Plzeň: Aleš Čeněk, 2015. s. 31,32. ISBN 978-80-7380558-6.

4.2.1. Porušování základních lidských práv a svobod

Užíváním FR systému za účelem vyhledávání a zajišťování důkazů taktéž dochází k zásahu do práva na soukromí (k právu na soukromí viz výše). Použití FR systému pro vyhledání a zajištění důkazů znamená zásah do soukromí osob, které jsou sledovány na základě kamerových záznamů, aniž by o tom věděly. Zásah spočívá v uchovávání a zpracovávání biometrických údajů, což reprezentuje výrazný zásah do soukromí osob. K objasnění, zdali tento nástroj opravdu zasahuje do práv zaručených Listinou v co nejmenší možné míře, provedeme test proporcionality.

a) Kritérium vhodnosti

V případě prvního kritéria testu proporcionality, posuzující kritérium vhodnosti, je třeba zkoumat, zda prostředek omezující základní lidské práva a svobody (konkrétně tedy právo na soukromí) může vést k naplnění legitimního cíle – tedy objasnění trestné činnosti. Užití FR systému za účelem vyhledání důkazů má za cíl objasnit konkrétní trestnou činnost a identifikovat osoby zapojené do kriminálních aktivit. FR systém je nástroj, který je schopen identifikovat osoby na základě jejich obličejových rysů a vyhledat tak důležité důkazní prostředky, které mohou napomoci při objasnění trestného činu. Proto je tento prostředek vhodný k objasnění trestné činnosti, tedy k dosažení legitimního cíle.

b) Kritérium potřebnosti

Při zkoumání kritéria potřebnosti je třeba posoudit, zda lze stanoveného cíle dosáhnout i jinými prostředky, které by méně popřípadě vůbec nezasahovaly do práva na ochranu soukromí. Alternativní metody vyhledání a zajištění důkazů mohou zahrnovat tradiční metody jako jsou například výslechy svědků, analýza stop z místa činu, fyzické přehrávání videozáznamů policisty či použití jiných kriminalistických metod. Nicméně FR systém může být jedinečný v tom, že umožňuje rychlou a personálně nenáročnou identifikaci osob na základě kamerových záznamů, což může být zásadní při objasňování některých druhů trestné činnosti. FR systém tak může být v mnoha případech nejefektivnějším nástrojem. O co více, mohou nastat situace, kdy alternativní metody vyhledávání nejsou vůbec schopny napomoci k vyhledání konkrétních důkazům, přičemž v těchto situacích může být FR systém jediným vhodným prostředkem. Pokud jiné metody vyhledání a zajištění důkazů nejsou dostatečně efektivní nebo dostupné, je použití FR systému považováno za potřebné. Potřebnost užití tohoto nástroje tak musí být dle mého názoru vždy zdůvodněna potřebností, a to v každém individuálním případě.

c) Kritérium proporcionality v užším smyslu

Pokud je FR systém využit pouze pro vyhledání a zajištění důkazů, má čistě procesní cíl, tedy zjistit konkrétní skutečnosti potřebné pro trestní řízení. Použití FR systému pro vyhledání a zajištění důkazů představuje zásah do soukromí osob, který spočívá zejména v uchovávání a zpracovávání biometrických údajů. Na druhé straně je však zájem na objasnění závažné trestné činnosti, který je vysoký. Efektivní a rychlé objasnění trestného činu je v zájmu společnosti a spravedlnosti, zejména pak pokud jde o závažné zločiny, které mohou být za pomoci FR systémů objasněny. Zásah do soukromí by tak měl být úměrný závažnosti trestné činnosti. Domnívám se proto, že při vyšetřování závažných trestných činů, jako je například terorismus či vražda, se jeví použití FR systému více opodstatněné než při méně závažných přestupcích. Současná právní úprava však užití FR systémů nikterak neomezuje, proto není možné úměrnost závažnosti trestné činnosti dle současné legislativy zkoumat. Stejně tak nejsou stanoveny přesná pravidla a postupy související s prací a fungováním tohoto systému.

Závěrem je tak možné dle mého názoru říci, že FR systém v podobě, jak jej známe dnes, tedy bez jakéhokoli omezení jeho užití, nemůže projít testem proporcionality. Je tomu tak zejména proto, že současná právní úprava nezkoumá potřebnost užití FR systému v konkrétních případech, možnost zneužití ani úměrnost závažnosti trestné činnosti. V případě, že by právní úprava podrobněji upravovala podmínky užití tohoto nástroje, mohlo by se jednat o nejen velice efektivní nástroj, ale také nástroj splňující podmínky proporcionality zásahu do ústavně zaručených práv. Návrhům těchto podmínek se pak věnuji v kapitole č. 4.3.

4.2.2. Porušení zásad

Užívání FR systému musí vycházet z obecných zásad trestního řízení. Jednou ze zásad, která může být v rozporu s užíváním FR systému, je zásada zdrženlivosti podle §2 odst. 4 TRŘ. Na základě této zásady je zapotřebí šetření práv a svobod zaručených Listinou a mezinárodními smlouvami o lidských právech, tzn. OČTŘ jsou povinny co nejméně zasahovat do základních práv a svobod. Tato zásada *„vyžaduje, aby takovýto postup byl odůvodněný, a to s ohledem na povahu a závažnost činu, dále osobu, vůči níž úkon směřuje, jakož i závažnost zásahu do jejích práv.*“[117] Jak bylo zmíněno výše, česká právní úprava

[117] MULÁK, Jiří. Základní zásady trestního řízení – jejich výjimečnost a výjimky z nich. *AUC IURIDICA*. 2023, roč. 69, č. 3, s. 40. DOI: 10.14712/23366478.2023.25.

neupravuje omezení užívání FR systému, proto se domnívám, že současné užití by bylo v rozporu se zásadou zdrženlivosti.

4.2.3. Podobnost s jiným úkonem

Domnívám se, že v případě užití FR systému za účelem vyhledávání a zajišťování důkazů nejsou zajištěny záruky zákonnosti provádění podobných, v TRŘ výslovně uvedených úkonů. Dle mého názoru je možné užití FR systému připodobnit ke sledování osob a věcí ve smyslu § 158d odst. 2 TRŘ, zejména pak za předpokladu dostatečného pokrytí území České republiky kamerovými systémy. Sledování osob patří mezi operativně pátrací prostředky, které patří do okruhu kriminalistických metod, které jsou převážně záležitostí praktického uplatnění. Konkrétně se jedná o systém specifických kriminalistických postupů a metod, jejichž cílem je získání skutečností důležitých pro trestní řízení.

Jak na základě sledování ve smyslu § 158d odst. 2 TRŘ, tak v případě užití FR systému, je možné zajistit skutečnosti, na základě kterých je možné určit polohu osoby, co dělá a s kým se stýká. Oproti sledování osob dle §158d odst. 2 TRŘ FR systém umožňuje zajištění těchto skutečností i zpětně. Jedinou limitací systému je délka uchovávání kamerových záznamů před tím, než dojde k jejich smazáni. V případě FR systému je „sledování osoby“ významně jednodušší, rychlejší, a ne toliko personálně náročné. Jelikož je však FR systém omezen pouze na veřejné prostory, takovéto sledování nemusí být vždy nejvhodnější a nejefektivnější metodou.

Svou podstatou lze FR systém užít obdobně jakožto operativně pátrací prostředek sledování osob a věcí, přestože se mezi operativně pátrací prostředky dle TRŘ neřadí. V současné chvíli právní úprava žádné zákonné požadavky k užití FR systému nestanovuje. Je tak zapotřebí, aby pro užívání FR systémů byly splněny minimálně stejné zákonné požadavky, jako v případě sledování osob a věcí dle §158d odst. 2 TRŘ. Tímto požadavkem je tedy minimálně omezení pro úmyslné trestné činy na základě písemné žádosti, kterou je třeba odůvodnit.

4.2.4. Poznání relevantních skutečností

FR systémy dokáží rychle porovnávat obličejové rysy jednotlivců s databázemi známých pachatelů nebo podezřelých. To umožňuje bezpečnostním složkám přesně a efektivně identifikovat osoby na záznamech, což zvyšuje šance na rychlé a cílené vyšetřování. FR systém tak napomáhá k vyhledání a následnému poznání relevantních skutečností pro trestní řízení.

4.2.5. Prověřenost metody

FR systémy jsou založeny na technologiích AI, které mají vědecký základ. Jejich efektivita a přesnost jsou závislé na kvalitě algoritmů, datových sadách a technických parametrech v případě každého jednotlivého FR systému. FR lze tedy charakterizovat jakožto systémy založené na vědeckých, matematických a informačních technologií.

V případě užití FR systému za účelem vyhledávání a zajišťování důkazů je možné vždy ověřit, zda vyhledaný kamerový záznam je skutečně relevantní k trestnímu řízení. Je důležité však zmínit, že prvotním hodnotícím subjektem práce FR systému je vždy policista pracující s FR systémem. Samotný proces vyhledávání kamerových záznamů je pouze alternativou k práci policistů, kteří mohou fyzicky procházet kamerové záznamy a relevantní záznamy z nich vybírat. Prověření, zda se jedná o relevantní záznam je pak možné ověřit například i na základě výpovědi obviněného, svědků či expertízami videozáznamu. S problematikou prověření pak také úzce souvisí přesnost a spolehlivost této technologie. Případu falešné pozitivity a negativity u osob jiných než bílé pleti jsem se však věnovala v kapitole 3.2.1., přičemž závěry týkající se chybovosti v této kapitole lze uplatnit i nyní. Lze tedy shrnout, že této chybovosti je možné předejít či snížit na minimum.

4.2.6. Právem nezakázaná metoda

FR technologie není v TRŘ výslovně zakázána. Používání této technologie, která napomáhá při vyhledávání a zajišťování důkazů, tak není TRŘ vyloučeno. Díky tomu mají OČTŘ možnost v trestním řízení přistupovat k moderním technologiím a využívat je.

4.3. Úvahy mezí de lege ferenda

V současné chvíli mi nejsou známá pravidla, která by užívání FR systémů omezovala či by stanovovala jasné podmínky užívání tohoto systému. Jaké by tato meze pro užívání FR systému mohly být, zejména aby došlo k splnění podmínek testu proporcionality, se proto pokusím nastínit níže.

4.3.1. Specifikace trestné činnosti

Jak již bylo zmíněno výše, FR systémy lze užít jak v reálném čase (v čem se významně podobají sledování osob dle §158d TRŘ), tak zpětně. Dle mého názoru dochází v obou případech k obdobnému zásahu do práva na soukromí osob. Tento rozdíl v čase, kdy dochází k identifikaci osoby za účelem vyhledávání důkazů, neovlivňuje míru zásahu do soukromí, jelikož je využívána podobná technologie a stejná databáze, což vede k obdobným dopadům na právo na soukromí osob. Navíc, v obou případech dochází k identifikaci osob bez jejich vědomí. V případě sledování osoby a věcí dle §159 odst. 2 TRŘ lze k tomuto sledování

přistoupit pouze u úmyslných trestných činů. [118] Proto se domnívám, že FR systém je možné užít minimálně obdobně, tedy za účelem objasňování úmyslných trestných činů.

Z tohoto důvodu tak zastávám názor, že není možné užívat FR systém bez návaznost na konkrétní trestnou činnost. Prevence kriminality je legitimním zájmem, který může ospravedlňovat zásah do práva na soukromí.[119] To však neznamená, že každý prostředek napomáhající prevenci kriminality je možné užít preventivně bez návaznosti na trestnou činnost. To vyplývá také z rozhodnutí ESLP, který se vyjádřil k otázce konkrétního užívání FR systémů v případě Glukhin vs Rusko.[120] Stěžovat, pan Glukhin, účastník pokojné demonstrace, byl pomocí systému na rozpoznání obličeje identifikován jako účastník této pokojné demonstrace, byla lokalizována jeho poloha, načež byl následně stíhán za přestupek. Přestože tento zásah do soukromí splňoval legitimní cíl, tedy prevence kriminality, a byl v souladu s ruskou právní úpravou, ESLP nakonec došel k závěru, že zpracování biometrických osobních údajů žadatele v rámci správního řízení, jednak za účelem jeho identifikace na fotografiích a videích zveřejněných na internetu a jednak k jeho nalezení a zatčení při cestování moskevským metrem, nelze považovat za potřebné v demokratické společnosti, a je tak v rozporu s článkem 8 Úmluvy. V případě užití argumentace *ad maiori ad minus* lze tedy říci, že pokud užití FR systémů za účelem identifikace pachatele přestupků nenaplňuje kritérium potřebnosti, pak není možné tvrdit, že by užití této technologie bez návaznosti na konkrétní trestnou činnost, tedy za účelem preventivního užití, naplňovalo požadavky potřebnosti.

4.3.2. Užití v jiné trestní věci

V souvislosti s užitím FR systémů může nastat situace, že dojde k odhalení jiné trestné činnosti, než ke které byl FR systém užit. Je proto zásadní určit, zda je možné vyhledaný důkazní prostředek za pomocí FR systému užít i v jiné trestné věci. Obecně platí, že pokud se během trestního řízení objeví důkazy o spáchání jiných trestných činů, než pro které bylo řízení původně zahájeno, tyto důkazy vztahující se k jinému činu (jenž nebyly předmětem trestního řízení), nejsou procesně účinné.[121] Z tohoto pravidla však existují výjimky.

---

[118] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. §158d In: ŠÁMAL, Pavel a kol.: *Trestní řád I. 7. vydání*. [Systém Beck-online]. Praha: C. H. Beck, 2013, s. 2001 - 2012. ISBN 978-80-7400-465-0. Dostupné z: https://app-beck-online-cz.ezproxy.is.cuni.cz/bo/document-view.seam?documentId=nnptembrgnpwk5tlge3c443cl4ytsnrrl4ytimk7obtdqoi#.

[119] Čl. 8 odst. 2 Úmluvy o ochraně lidských práv a základních svobod.

[120] Rozhodnutí ESLP ze dne 4. 7. 2023, ve věci Glukhin proti Rusku, č. 11519/20.

[121] JELÍNEK, Jiří a kol. *Trestní právo procesní 7. aktualizované a doplněné vydán*í. Leges. 2023. s. 416. ISBN 978-80-7502-687-3.

V případě již zmiňovaného sledování osob a věcí za pořizování zvukových, obrazových nebo jiných záznamů, lze *„připojený protokol použít jako důkaz jen tehdy, je-li i v této věci vedeno řízení o úmyslném trestném činu nebo souhlasí-li s tím osoba, do jejíž práv a svobod bylo sledováním zasahováno záznamu ze sledování v jiné trestní věci užít.“* [122] U prostorových odposlechů spadajících pod sledování osob a věcí dle §158d odst. 3 TRŘ je užití v jiné trestné věci složitější, jelikož TRŘ použitelnost těchto záznamů neupravuje. Nejvyšší soud však rozhodl, že záznamy dle §158 odst.3 TRŘ lze obdobně užít jako v případě záznamů pořízených dle §158 odst. 2 TRŘ *„s ohledem na zásadu proporcionality a s respektem k právu na nedotknutelnost osoby a jejího soukromí. Přitom je nutno zejména přihlédnout k intenzitě zásahu do práv uvedených v § 158d odst. 3 TRŘ. a k závažnosti trestného činu, o němž se vede řízení v jiné trestní věci."* [123]

I přes to, že prostorové odposlechy a FR systémy nelze zcela připodobňovat, rozhodnutí Nejvyššího soudu považuji za inspirativní argumentační základnu pro použití vyhledaných důkazů za pomocí FR systémů v jiné trestné věci. Mimo to je dle mého názoru zapotřebí, aby byl výstup z FR systému v prvním případě získán zákonným, plně transparentním způsobem.

4.3.3. Povolení soudce či státního zástupce

Je otázkou, zda by užití FR systémů mělo býti podmíněno povolením soudce či státního zástupce. Podmínění užití prostředků, které zasahují do základních práv a svobod, povolením, představuje v trestním řízení běžnou praxi. Například u zajištění údajů o uskutečněném telekomunikačním provozu dle §88a TRŘ nařizuje vydání těchto údajů předseda senátu, zatímco v přípravném řízení tak činí soudce, a to na návrh státního zástupce. V případě již zmiňovaného sledování osob a věci je zapotřebí povolení státního zástupce, ve specifických případech pak soudce dle §158d odst. 2 TRŘ. U obecného sledování osoby není potřeba povolení, a to za podmínky, že během takovéhoto sledování nebyly pořízeny žádné záznamy a zároveň nebylo *„sledováním zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků.“*[124] V případech, kdy během sledování dochází k pořizování zvukových, obrazových a jiných záznamů, je ovšem zapotřebí písemné povolení státního zástupce, přičemž tento způsob sledování lze svou podstatou více připodobnit k fungování FR

[122] §158d odst. 10 TRŘ.
[123] Usnesení Nejvyššího soudu ze dne 01.09.2020, čj. 7 Tdo 865/2020. In: *Sbírka Nejvyšší soud* [online]. Nejvyšší soud [cit. 4.7.2024]. Dostupné z: https://sbirka.nsoud.cz/sbirka/5700/.
[124] §158d odst. 1 TRŘ.

systémů napojených na kamerové systémy ukládající kamerový záznam. Ve specifických případech dle §158d odst. 3 TRŘ je pak zapotřebí pro zahájení sledování osoby povolení soudce.

Domnívám se, že užití FR systému by mělo minimálně podléhat povolení ze strany státního zástupce či soudce, aby byla zajištěna opodstatněnost užití tohoto systému. Pokud by Policie mohla užívat FR systém bez dostatečného zdůvodnění, užití FR systému by mohlo vést k nepřiměřenému zásahu do soukromí jednotlivců, kteří nejsou podezřelí z trestné činnosti. Hrozilo by tak mimo jiné riziko zneužití této technologie. Obrana proti takovému zneužití by pak byla téměř nemožná. Dle ESLP „*esenciální předpoklady spravedlivého procesu vyžadují, aby byl jednotlivec vybaven dostatečnými garancemi a zárukami proti možnému zneužití pravomoci ze strany veřejné moci.*“[125] Omezení používání FR systémů pouze na trestní řízení zajišťuje, že technologie bude použita pouze v případech, kde je skutečně potřebná a oprávněná, což minimalizuje zásahy do soukromí nevinných osob.

Zdali by se jednalo o povolení soudce či státního zástupce není dle mého názoru důležité, jelikož oba zaručují dostatek nestrannosti a ochranu před zneužitím této technologie. Navíc samotné povolení, konkrétně pak příkaz představující rozhodnutí svého druhu,[126] je zapotřebí řádně a dostatečně zdůvodnit které z důvodu zásahu do práv a svobod, což zajišťuje nejen ochranu práv a svobod jednotlivců, ale může sloužit jako prevence k zneužití této technologie.

4.3.4. Informační povinnost a přezkum

Užití FR systému vyvolává otázku, zda by měla existovat informační povinnost vůči osobě, jejichž osobní údaje byly v souvislosti s FR systémem zpracovány. Významnou roli v této problematice hraje již výše zmiňované ustanovení §88 zákona o Policii České republiky, kdy v případě zpracovávání osobních bez vědomí fyzických osob za účelem *„předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů,“* je zapotřebí dotčené osoby zpětně informovat. Mimo například nemožnost vyhledat bydliště této osoby tak nemusí činit ano v případě, pokud byly záznamy o zpracování bez zbytečného odkladu vymazány. V ostatních případech je informační povinnost zachována.

Informování dotčené osoby je zakotveno například u poskytování údajů o uskutečněném telekomunikačním provozu dle §88a odst. 2 TRŘ, nebo také odposlechů a

[125] WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK a Ivo POSPÍŠIL. *Listina základních práv a svobod - Komentář*. Wolters Kluwer, 2012, s. 129. ISBN: 978-80-7357-750-6.
[126] STŘÍŽ, Igor et al. *Trestní zákoník a trestní řád 2. díl*. Praha: Linde Praha, 2010, s. 304. ISBN978-80-7201-803-1.

záznamů telekomunikačního provozu za podmínek §88 odst. 9 TRŘ s výjimkou *„řízení o zločinu, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, spáchaném organizovanou skupinou, v řízení o trestném činu spáchaném ve prospěch organizované zločinecké skupiny, v řízení o trestném činu účasti na organizované zločinecké skupině, v řízení o trestném činu účasti na teroristické skupině nebo pokud se na spáchání trestného činu podílelo více osob a ve vztahu alespoň k jedné z nich nebylo trestní řízení doposud pravomocně skončeno, nebo pokud je proti osobě, jíž má být informace sdělena, vedeno trestní řízení, anebo pokud by poskytnutím takové informace mohl být zmařen účel trestního řízení, včetně řízení uvedeného v odstavci 6, nebo by mohlo dojít k ohrožení bezpečnosti státu, života, zdraví, práv a svobod osob.*“ §88 odst. 9 TRŘ (podobně také §88a odst.3 TRŘ) tak vylučuje z informační povinnosti nejzávaznější trestné činy a situace, kdy by mohlo dojít k zmaření účelu trestního stíhání či ohrožení chráněných zájmů. Dle ESLP omezení informační povinnost není v rozporu s čl. 8 Úmluvy, jelikož *„aktivita nebo nebezpečí, k jejichž potření sledovací opatření směřují, může přetrvávat léta či dokonce desetiletí poté, co bylo od těchto opatření upuštěno. Následné upozornění každé osoby dotčené opatřením by mohlo kompromitovat dlouhodobý cíl, kterým bylo původně nařízení sledování odůvodněno. Navíc takové upozornění by hrozilo přispět k odhalení pracovních metod zpravodajských služeb, pole jejich působnosti a případně i totožnosti jejich agentů.”*[127]

Informační povinnost není stanovena u všech prostředků zasahující do základních lidských práv a svobod. U sledování osob a věcí dle § 158d TRŘ tato povinnost taktéž chybí. Absence informační povinnosti však při sledování osob a věcí nezůstává nepovšimnuta a je kritizována například Stálou komisí, která tento požadavek zdůraznila ve svém usnesení v roce 2017.[128]

Domnívám se, že informační povinnost v souvislosti s užitím FR systémů by měla býti zakotvena. Informační povinnost při zásahu do základních práv a svobod je důležitým krokem k ochraně těchto práv. V případě práva na informační sebeurčení pak mají jednotlivci právo vědět, jak jsou jejich osobní údaje zpracovávány a využívány. To s sebou přináší mimo jiné možnost lépe reagovat na neoprávněné použití FR systémů, vznášet námitky proti zpracování osobních údajů, což pomáhá předcházení potenciálního zneužití technologie. Je třeba mít na paměti, že v případě užití FR systému však nedochází k zpracování osobních údajů pouze

[127] Rozsudek ESLP ze dne 6. září 1978, ve věci Klass a ostatní proti Německu, č. 5029/71.

[128] Stálá kontrolní komise pro kontrolu použití odposlechů a záznamů telekomunikačního provozu, sledování osob a věcí a rušení elektronických komunikací, Usnesení č. 25 ze dne 23. února 2017, dostupné z: https://www.psp.cz/sqw/text/text2.sqw?idd=102715.

dotčené osoby, avšak ke zpracování osobních údajů i necílených osob. V případě těchto osob by však nebylo možné vyhledat bydliště těchto fyzické osoby, a pokud ano, takovéto hledání by bylo v rozporu s hospodárností a efektivností trestního řízení. V případě osoby, na kterou byl FR systém cíleně užit se však domnívám, že pro Policii není problematické takovouto osobu až na výjimky informovat, a tudíž se klaním spíše k variantě informační povinnosti.

V některých případech je dokonce umožněn speciální přezkumu zákonnosti příkazu u Nejvyššího soudu, jako je tomu například u odposlechu a záznamů o telekomunikačním provozu. Naproti tomu, v případě sledování osob a věcí dle §158d odst. 2 a 3 TRŘ takováto možnost přezkumu příkazu chybí. Přestože dle Ústavního soudu *„efektivní soudní kontrola provádění jakýchkoliv operativně pátracích prostředků, s přesahem do oblasti základních práv a svobod, je naprosto nezbytnou podmínkou spravedlivého procesu v trestním řízení,*“ [129] do dnešního dne neexistuje forma přezkumu příkazů k zahájení sledování osob a věcí dle §158d odst. 2 TRŘ. Tento nedostatek je často kritizován odbornou veřejností a rovněž i já se domnívám, že absence tohoto přezkumu, stejně jako absence povinnosti notifikovat osobu, vůči níž byl FR systém užit, představuje porušení práva na soukromí a spravedlivý proces. Proto zastávám názor, že zavedení přezkumu příkazů k užití FR systému by bylo vhodnou formou kontroly zákonnosti jeho používání.

4.4. Ne/účinnost vyhledaných důkazů a ovoce z otráveného stromu

Při hodnocení důkazů v trestním řízení se postupuje podle několika kritérií, přičemž nejdůležitější jsou tři základní aspekty: závažnost, zákonnost a pravdivost důkazu. Nejdříve je zapotřebí v každém jednotlivém případě posoudit závažnost důkazu, tedy jak zásadní je důkaz pro samotné řízení a jeho potenciální vliv na výsledek. OČTŘ musí pečlivě zvážit, zda předložený důkaz poskytuje podstatné informace o trestném činu, o vině nebo nevině obžalovaného, nebo o okolnostech, které jsou klíčové pro objasnění případu. Pokud se důkaz jeví jako málo závažný nebo irelevantní, OČTŘ může rozhodnout o jeho vyloučení z dalšího projednávání. Tento krok tak chrání trestní řízení před zahlcením nepotřebnými nebo irelevantními důkazy, čímž napomáhá efektivnímu vedení řízení.

Další klíčovou fází hodnocení je otázka zákonnosti důkazu. Zákonnost se týká toho, zda byl důkaz získán v souladu s právním řádem, především pak s procesními pravidly a zásadami trestního řízení.[130] *A contrario* nezákonný důkaz je tedy takový, u kterého

[129] Nález Ústavního soudu ze dne 23. 5. 2007, sp. zn. II.ÚS 615/06. In: *Nalus* [online]. Ústavní soud [cit. 26.9.2024]. Dostupné z:https://nalus.usoud.cz/Search/GetText.aspx?sz=pl-3-02.

[130] JELÍNEK, Jiří, ed. *Dokazování v trestním řízení v kontextu práva na spravedlivý proces*. Praha: Leges, 2018, s. 263. ISBN: 978-80-7502-287-5.

především opatřování a provádění daného důkazu nebylo prováděno v souladu s právními předpisy.[131] Příkladem může být § 89 odst. 3 TRŘ, který uvádí zákaz získávání důkazu nezákonným donucením nebo hrozbou takového donucení. Z pohledu trestního řízení je posuzována zákonnost ve všech fází dokazování. Problematické je však posuzování zákonnosti ve fázi vyhledávání důkazů, protože ne vždy má soud přehled o tom, jakým způsobem byl konkrétní důkaz vyhledán, a to zejména v případě vyhledávání důkazů před zahájením trestního řízení. Pokud je důkaz vyhledán neprocesním úkonem, k posuzování zákonnosti nedochází,[132] nýbrž je zapotřebí zkoumat jeho přípustnost. Od zahájení prověřování je však zahájeno trestního řízení, přičemž státní zástupce začíná dohlížet na dodržování zákonnosti během přípravného řízení, proto je možné ověřit zákonnost vyhledávání důkazů již od zahájení prověřování.

V případě využití FR systému za účelem vyhledání důkazů je možné posuzovat nezákonnost důkazu, která je zapříčiněna chybným, nezákonným postupem OČTŘ. Tato nezákonnost musí souviset s porušením právních předpisů při vyhledávání důkazů, přičemž je zapotřebí, aby se jednalo o takovou vadu, která představuje podstatnou vadu řízení. TRŘ neobsahuje výčet podstatných vad řízení, proto k zjištění takovýchto vad je zapotřebí užít výklad. *„Je nutné nepoužitelnost důkazů dovozovat výkladem v každém konkrétním případě zvlášť, a to především s ohledem na charakter vady řízení, vliv na konkrétní důkaz a význam tohoto důkazu pro řízení.“*[133]

U nezákonných důkazů lze rozlišovat absolutní neúčinnost, kdy je důkaz zcela vyloučen pro účely dokazování v trestním řízení a relativní neúčinnost, která může připustit účinnost důkaz za určitých podmínek. V případě absolutní neúčinnosti se jedná o takovou podstatnou vadu, kterou nelze zhojit. Takovýmto příkladem může být získání důkazů výše zmíněným nezákonným donucením nebo hrozbou takového donucení. Naproti tomu v případě relativní neúčinnosti důkazů jde taktéž o podstatnou vadu řízení, ale takovouto vadu lze dostatečně zhojit. Jedná se například o důkazy získané při úkonu, k němuž je vyžadován souhlas státního zástupce či soudce, přičemž takto získané důkazy mohou být dodatečně legitimizovány, pokud tento souhlas bude dodatečně udělen zpětně.

[131] ZAORALOVÁ, Petra. *Procesní použitelnost důkazů v trestním řízení a její meze*. Praha: Leges, 2018, s. 38–39. ISBN 978-80-7502-310-0.
[132] NETT, Alexandr. *K problematice neúčinných důkazů v trestním řízení*. Brno: Vydavatelství MU, 1995. s. 6. ISBN 80-210-1163-7.
[133] Nález Ústavního soudu ze dne 8. 2. 2010, sp. zn. IV.ÚS 2425/09. In: *Nalus* [online]. Ústavní soud [cit. 26.9.2024]. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=4-2425-09_1.

Zákonnost vyhledaných důkazů za pomocí FR systému tak závisí na podmínkách, které je nejprve pro užití tohoto systému stanovit. Až následně bude možné hodnotit zákonnost takto vyhledaných důkazů. Pokud bychom však vycházeli z úvah mezí *de lege ferenda* a k užití FR systému by bylo zapotřebí povolení soudce či státního zástupce, jednalo by se s největší pravděpodobností o relativní neúčinnost takto vyhledaného důkazu, kterou by bylo možné dodatečně zhojit. Pokud by však tento systém bylo možné užít například pouze v souvislosti s úmyslnou trestnou činností, avšak FR systém by byl užit v souvislosti s nedbalostním trestným činem, případně bez jakékoli souvislosti s trestnou činností, jednalo by se dle mého názoru o podstatnou vadu, kterou není možné dodatečně zhojit, a tudíž by takto získaný důkaz představoval absolutně neúčinný důkaz.

Posledním, avšak neméně důležitým krokem při hodnocení důkazů je jeho věrohodnost, která se vztahuje k jeho faktické správnosti a schopnosti objektivně popsat skutečnosti.

S problematikou neúčinnosti důkazů blízce souvisí otázka získaných důkazů na základě důkazů neúčinných, ke které se silně váže doktrína „ovoce z otráveného stromu“. Jedná se o koncept, který vychází z americké doktríny zvané „fruits of the poisonous tree doctrine“, která se zabývá otázkami účinnosti důkazů v trestním řízení, přesněji otázkou, zdali je možné v trestním řízení použít důkaz odvozený z nezákonného důkazu. Odvozený důkaz v této doktríně představuje ovoce, přičemž primární důkaz otrávený strom. Podstatou vzniku této doktríny je specifické americké prostředí, které v trestním právu uplatňuje adversální model. Tento model pramení z charakteristické nedůvěry společnosti vůči státu, což se projevuje například rozdělením důkazního břemene vůči stranám řízení, které předkládají důkazy vůči soudu (nezávislému třetímu), který o řízení rozhoduje. Důkazní pravidla jsou pak nastavena velice rigidně, a to zejména z důvodu ochrany jednotlivce před zneužitím pravomocí státem.

Na základě této doktríny pak důkazy, které byly získány na podkladě důkazu získaného nezákonným způsobem (tudíž neúčinného) budou také neúčinnými. V této doktríně však bylo vytvořeno několik výjimek za účel zmírnění dopadů. Jednou z nich je pravidlo, že pokud byl úkon proveden v dobré víře a ex post dojde k zjištění, že se jedná o nezákonný důkaz, takovýto důkaz pak může být proveden v souladu se zákonem. Další takovou výjimkou je například pravidlo, že důkaz, který by policie objevila legálně i bez ohledu na nezákonné jednání, bude v řízení před soudem účinný.

České trestní právo procesní americký koncept nepřevzalo. Proti fungování této doktríny je v českém prostředí spousta výhrad a na akademické sféře se vedou debaty o různé

aplikace této doktríny. K této otázce se již několikrát vyjádřil například Ústavní soud, který konstatoval, že *„výskyt nezákonného důkazu nevede k nepoužitelnosti všech ostatních (jiných) důkazů. Ani tak rigorózní důkazní teorie, jako je např. doktrína ovoce z otráveného stromu, jejíž aplikovatelnost je sama o sobě sporná, nezastává názor, že výskyt nezákonného důkazu způsobuje nepoužitelnost všech důkazů opatřených v daném řízení. Nepoužitelnost se týká toliko těch důkazů, jež jsou od nezákonného důkazu kauzálně odvozeny."*[134] Významným posunem pak byl nález Ústavního soudu sp. zn. I. ÚS 1677/13, ve kterém se Ústavní soud zabýval doktrínou „plodů z otráveného stromu" v kontextu rozdílných trestněprávních modelů. Šlo o případ, kdy byla provedena nezákonná rekognice podle fotografií bez přítomnosti soudce. I když soudy uznaly nepoužitelnost této rekognice, odsoudily stěžovatele na základě následných výpovědí poškozeného, který se odkazoval na fotku z nezákonné rekognice. Ústavní soud potvrdil svůj zdrženlivý přístup k doktríně, ale částečně vyhověl stěžovateli, když vyloučil ty pasáže výpovědi, které byly přímo spojeny s nepoužitelnou rekognicí, protože takové důkazy porušily právo na spravedlivý proces.

Každý případ se tak posuzuje individuálně, s ohledem na kauzální souvislost mezi důkazy a závažnost vad, které mohou vést k vyloučení důkazu. Na základě zásady volného hodnocení důkazů je pak soud povinen posuzovat důkazy jak jednotlivě, tak v kontextu jejich vzájemných souvislostí. Je tedy možné, že na základě nezákonně vyhledaného důkazu za pomocí FR systému bude možné použit jiný důkaz, odvozený od takto vyhledaného kamerového záznamu.

[134] Nález Ústavního soudu ze dne 8. 3. 2012, sp. zn. III. ÚS 2260/10. In: *Salvia* [online]. Ústavní soud [cit. 26.9.2024]. Dostupné z: https://kraken.slv.cz/III.US2260/10.

5. Rekognice

Technologie rozpoznávání obličeje je významným nástrojem během vyšetřování trestných činů, který umožňuje policistům rychle a efektivně analyzovat obrazový materiál z mnoha zdrojů získaných během vyšetřování. Může se jednat například o bezpečnostní kamery, které jsou instalovány v dopravních prostředcích, budovách, jiných veřejných místech či soukromé záběry osob. V případech, kdy má Policie k dispozici pouze fotografii či kamerový záznam osoby pachatele, ale není známa identita takovéhoto pachatele, se může jednat o velice složitou situaci. K dispozici má Policie několik tradičních metod, jak identifikovat osoby na základě fotografií. Jednou z těchto metod je oslovení veřejnost prostřednictvím různých kanálů, jako jsou tiskové zprávy, televizní stanice, noviny nebo sociální sítě. Cílem této metody je oslovit co nejširší okruh lidí, kteří mohou mít informace o totožnosti osoby na snímku nebo potenciální svědky, kteří by mohli osobu na fotografii rozpoznat. Jinou možností je pátrání po svědcích, kteří mohou rozpoznat osobu na fotografii nebo mají další informace. Jiným krokem, který může Policie podniknout, je fyzické srovnání fotografie s dostupnými databázemi, zda snímek odpovídá někomu v těchto databázích. Všechny z těchto či jiných metod mohou být velmi časově náročné a málo efektivní. Může tak dojít ke zdržení v přípravném řízení, což může ohrozit bezpečnost a ztížit nalezení pachatele.

V případě užití FR systémů se však identifikace osoby jeví jako rychlejší a efektivnější způsob, jak identifikovat pachatele trestné činnosti, a to zejména z důvodu automatizovaného porovnání fotografie s databázemi osobních údajů, což snižuje potřebu manuálního vyhledávání. Díky FR systému je možné rychle vyhledat a porovnat rysy obličeje na snímku s miliony záznamy v databázích, což nejen zkracuje dobu potřebnou k nalezení shody, ale také zvyšuje celkovou efektivitu vyšetřování.

Již v současné době užívá Policie informační systém Digitální podoba osob za účelem identifikace neznámých pachatelů závažných trestných činů. Tento systém tak například *„napomohl objasnění zvlášť závažného zločinu znásilnění dle § 185/1 alinea 2, 2a),3a) TZ a přečinu výroby a jiného nakládání s dětskou pornografií, kdy v tomto konkrétním případě přispěl k rozkrytí celé organizované skupiny. Dalším příkladem je několik ztotožnění pachatelů trestného činu loupeže dle § 173 TZ.“*[135]

Je však otázkou, jaký význam v trestním řízení má výstup FR systému, který identifikuje osobu na záznamu. V tomto případě se nejedná o vyhledání záznamů za pomocí

[135] Aktualizace: Vyjádření k provozování informačního systému Digitálních podob osob - Policie České republiky [online]. [cit. 03.07.2024]. Dostupné z: https://www.policie.cz/clanek/vyjadreni-k-provozovani-informacniho-systemu-digitalnich-podob-osob.aspx.

FR systému jako tomu bylo v kapitole č. 4, ale jedná se o případ, kdy FR systém ztotožní osobu, která se na konkrétním záznamu nachází. V této kapitole se tak budu zaobírat otázkou, jak konkrétně a zda-li vůbec je možné takovýto výstup v trestním řízení užít jakožto důkaz.

5.1. Zákonná úprava

Na základě § 89 odst. 2 TRŘ *„za důkaz může sloužit vše, co může přispět k objasnění věci.“*
V případě výstupu FR systému se jedná o takový důkaz, který je získán za pomocí kriminalistické metody (realizována prostřednictvím kriminalistického prostředku), který není TRŘ v současné chvíli upraven. Jak již bylo představeno výše, na takovéto metody jsou stanoveny přísné požadavky:

- *„Metoda a způsob její aplikace v kriminalistické praxi nesmí porušovat základní lidská práva a svobody, demokratické a právní principy státní činnosti.*
- *Metoda a způsob její aplikace v kriminalistické praxi nesmí porušovat základní limity a zásady trestního řízení.*
- *Konkrétní metoda a její aplikace musí spolehlivě vést k poznání a prokázání určitých skutečností.“*[136]
- *„Při provádění skutečností jsou dodržovány trestním řádem výslovně stanovené záruky zajištění zákonnosti provádění podobných, v trestním řádu výslovně uvedených úkonů.“*[137]
- *„Konkrétní metoda musí být experimentálně prověřená a teoreticky podložená tak, aby se její výsledky daly označit za průkazné a validní.*
- *Nejedná se o metody právními normami výslovně zakázané a odpovídají požadavkům profesionální etiky.“*[138]

5.1.1. Porušování základních lidských práv a svobod

Použití FR systému za účelem rekognice osoby zachycené na kamerovém záznamu představuje dle mého názoru velmi omezený a specifický zásah do lidských práv, konkrétně pak práva na soukromí osob. Užití FR systému se zaměřuje pouze na identifikaci konkrétní osoby již zaznamenané v určité situaci na konkrétním záznamu, z tohoto důvodu se tedy domnívám, že provádět test proporcionality není zapotřebí. To však neznamená, že by užití

[136] PORADA, Viktor, POLÁK, Petr, a kol. *Kriminalistika*. Plzeň: Aleš Čeněk, 2015. s. 31,32. ISBN 978-80-7380558-6.
[137] PJEŠČAK, Ján. a kol. *Kriminalistika*. Bratislava: Obzor, 1981. s. 41. ISBN: 65-056-81.
[138] PORADA, Viktor, POLÁK, Petr, a kol. *Kriminalistika*. Plzeň: Aleš Čeněk, 2015. s. 31,32. ISBN 978-80-7380558-6.

technologie nemělo být transparentní a nepodléhat přísným pravidlům a kontrolám. OČTŘ by měly mít jasně definované postupy a protokoly pro použití této technologie, včetně záznamů o každém použití, což nejenže minimalizuje riziko zneužití, ale také zajišťuje odpovědnost OČTŘ. Pokud budou takovéto záruky existovat, bude se jednat o nástroj splňující test proporcionality.

5.1.2. Porušení zásad

Domnívám se, že hodnocení výstupů učiněných FR systémem je problematické vůči zásadě práva na obhajobu obviněného upravené v § 2 odst. 13 TRŘ. Jako součást materiálního práva na obhajobu má obžalovaný právo se v hlavním líčení vyjádřit ke každému důkazu podle §38 odst. 2 Listiny a § 214 TRŘ, což umožňuje obžalovanému ovlivnit hodnocení důkazů soudem. Mimo to má právo předkládat důkazy, které jeho tvrzení potvrzují a vyvracejí naopak tvrzení obžaloby. *„Toto ústavně zaručené základní právo vyjádřit se ke všem prováděným důkazům (čl. 38 odst. 2 al. 1 Listiny, § 214 tr. ř.) přirozeně obsahuje v sobě předpoklad, že jde o důkazy, s nimiž se jak obžalovaný sám, tak i jeho obhájce měli možnost seznámit natolik, aby jim byly zcela srozumitelné, a aby k nim - ze svého hlediska - mohli zaujmout stanovisko.“*[139] Fungování FR systému je poměrně složité, ale i přesto by dle mého názoru měl mít obžalovaný právo rozumět výstupům systému a vyjadřovat se k možné chybovosti FR systému v konkrétním případě, k podrobnostem trénování systémů, základnímu naprogramování algoritmu a dalším aspektům. To může být v důsledku „black-box“ problému značně problematické. Důkazy založené na strojovém učení jsou velice špatně vysvětlitelné, protože ani samotní odborníci či znalci nedokáží zjistit a zdůvodnit, jakým způsobem stroj dospěl k určitému závěru.[140] Aby mohl v případě potřeby znalec odborně zhodnotit výstup FR systému, jsou dle mého názoru zapotřebí hluboké znalosti o fungování systému rozpoznávání obličejů, včetně znalostí o použitých tréninkových databází, statistických metod pro vývoj algoritmů či výpočtu pravděpodobnosti shod. Jelikož však FR systémy fungují na bázi AI a algoritmech strojového učení, díky čemuž se systém dokáže sám učit a zlepšovat, bylo by i pro samotného znalce těžké zdůvodnit, jak FR systém dospěl ke svému výstupu.

Je tak otázkou, zda by k naplnění záruky práva na materiální obhajobu stačilo například poskytnout data o samotném algoritmu, zdrojový kód, podrobnosti testování FR systému, statistickou chybovost a informaci o kvalitě kamerového záznamu. Domnívám se, že

[139] Nález Ústavního soudu České republiky ze dne30. 11. 1995, sp. zn. II.ÚS 62/95 [online]. Ústavní soud [cit. 9.7.2024]. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=3-62-95.

[140] NUTTER, Patrick W. Machine Learning Evidence: Admissibility and Weight. [online]. In: JOURNAL OF CONSTITUTIONAL LAW, 2019, roč. 21, č. 3. Dostupné z: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1691&context=jcl947Ibid., s. 947.

minimálně tyto informace jsou zapotřebí, aby mohl obžalovaný alespoň v hrubých rysech porozumět fungování konkrétního systému a vyjadřovat se tak k výstupům FR systému v trestním řízení.

5.1.3. Poznání relevantních skutečností

Využití FR systémů vede k poznání relevantních skutečností, konkrétně tedy k ztotožnění osoby zachycené na kamerovém záznamu. FR systém porovnává biometrické rysy obličeje s existujícími záznamy v databázích, čímž může dojít k určení totožnosti osoby, která je na záznamu zachycena. Úspěšnost ztotožnění osoby však závisí na kvalitě záznamu. Pokud je obraz rozmazaný, nedostatečně osvětlený nebo je snímaný nekvalitní kamerou, může dojít k chybné identifikaci nebo k úplnému selhání systému při rozpoznávání. Proto je přesnost a efektivita těchto systémů výrazně ovlivněna technickými podmínkami při pořizování záznamu.

5.1.4. Podobnost s jiným úkonem

Dle mého názoru využití FR systému za účelem ztotožnění osoby zachycené na fotografii je v jádru velmi podobné lidské rekognici podle fotografie dle §104b odst. 4 TRŘ. Rekognice dle fotografie je manuální proces, při kterém osoba porovnává fotografii s minimálně dalšími třemi fotografiemi osob. Úspěšnost tohoto procesu závisí na lidské schopnosti identifikovat unikátní rysy obličeje, jako jsou oči, nos, ústa, vlasy…Tento proces je však založen na subjektivním vnímání, což může vést k chybám, zejména pak pokud došlo k výrazným změnám podoby v případě porovnávané osoby.

Rekognice osoby podle fotografie a rozpoznávání osoby za pomocí FR systému sdílejí společný cíl, tedy identifikovat nebo ověřit identitu jedince na základě obličejových rysů, přestože oba způsoby ztotožňování využívají zcela rozdílných metod a principů. Rekognice jakožto zvláštní způsob dokazování nachází uplatnění v konkrétních individuálních případech, zatímco FR systém může být použit široké škále případů. V případě rekognice dle fotografie se jedná o subjektivní přístup, zatímco FR systém využívá sofistikované algoritmy, které umožňují analyzovat velké množství dat rychle s vysokou přesností, a to na základě biometrických charakteristik, jako jsou rozměry obličeje, vzdálenost mezi očima nebo tvar čelisti, což představuje objektivní přístup.

OČTŘ může k rekognici dle §104b TRŘ přistoupit bez předchozího souhlasu soudce či státního zástupce, přičemž protokol o rekognici je možné v řízení před soudem přečíst a užít jako důkaz, a to za podmínek § 207 odst. 2 nebo § 211 odst. 1, 2, 3, 4 TRŘ.

Domnívám se, že vzhledem k podobnosti mezi rekognicí a využitím FR systému, není pro aplikaci FR technologie zapotřebí povolení soudce či státního zástupce. Rekognice není vázána na specifickou trestnou činnost či podmínky, proto si myslím, že připuštění výstupů FR systému v trestním řízení dodržuje záruky zajištění zákonnosti rekognice osob dle fotografie. Pokud TRŘ připouští důkazy získané rekognicí dle § 104 TRŘ, pak dle mého názoru v zásadě neexistují překážky pro akceptaci výstupů FR systému jako důkazu. Je třeba si však uvědomit, že tak jako v případě fyzické rekognice nelze přesně popsat jednotlivé myšlenkové postupy, které vedly osobu k jejímu závěru, totéž platí i pro FR systém. Ani u něj není možné jednoznačně určit, jakým způsobem systém dospěl k výsledku, což opět podtrhuje důležitost transparentnosti a informovanosti o technických aspektech fungování FR technologie. Proto je dle mého názoru nezbytné, aby byl soud byl obeznámen alespoň o podrobnostech testování FR systému, statistikou chybovosti, kvalitou kamerového záznamu a dalšími relevantními informacemi. Bez těchto údajů by bylo problematické posoudit spolehlivost a relevanci důkazů získaných FR systémem. Samotný „black-box“ problém by však dle mého názoru neměl bránit možnosti užití důkazů získaných FR systémem v trestním řízení.

5.1.5. Prověřenost metody

Jak již bylo zmíněno v kapitolách výše, FR systém funguje na bázi algoritmů AI, zejména pak na algoritmech strojového učení a počítačového vidění. Přesnost systému pak souvisí s kvalitou vstupních dat a kontextu použití, přičemž finální výsledek je ovlivňován kvalitou analyzované fotografie. Všechny tyto faktory musí být brány do úvahy v případě hodnocení výstupu FR systému. Tyto výstupy je možné potvrdit i dalšími důkazními prostředky, jako jsou svědecké výpovědi či další forenzní metody, ovšem není možné zdůvodnit, jakým způsobem došel FR systém ke svému výstupu.

5.1.6. Právem nezakázaná metoda

Výstupy FR technologie ani samotná FR technologie nejsou TRŘ výslovně zakázány, a tudíž používání této technologií není *a priori* v rozporu s TRŘ. To je důležité z hlediska flexibility při zavádění nových technologií v oblasti vyšetřování trestných činů, neboť právní úprava často nedrží krok s technologickým vývojem.

5.2. Užití výstupu jako důkaz v hlavním líčení

Dle §89 odst. 2 TRŘ *„za důkaz může sloužit vše, co může přispět k objasnění věci.“* Aby však mohl výstup FR systému sloužit jako důkaz v řízení před soudem, je zapotřebí, aby mimo zákonné užití FR systému byly i samotné kamerové záznamy přípustným důkazním

prostředkem. Proto je nutné rozlišovat mezi kamerovými záznamy, které jsou pořízeny v rámci výkonu veřejné správy (například Policií) a mezi soukromými záznamy.

Ne vždy je možné soukromé záznamy v trestním řízení použít, a to zejména z důvodu nepřípustnosti a nezákonnosti. Právní teorie rozlišuje přípustnost důkazu (tzv. nepřípustnost v širším smyslu), která je posuzovaná na základě dvou kumulativních podmínek, a to přípustnosti pramene důkazu (tzv. nepřípustnost v užším smyslu) a zákonnosti důkazu.[141] Základem přípustnosti v širším smyslu je ustanovení §89 odst. 2 TŘ, přičemž s ohledem na toto ustanovení v obecné rovině nelze vyloučit záznam pořízený fyzickou osobou.

Při hodnocení přípustnosti důkazu (přípustnosti v širším smyslu) se užívá tzv. teorie konfliktu zájmů, vycházející z předpokladu, že *„v právní úpravě dokazování i její praktické aplikaci se zřetelně projevuje střet zájmu na účinném postupu OČTŘ a zájmu na dostatečné ochraně práv a svobod osob na trestním řízení zúčastněných.“* [142] V případě takového střetu zájmu dochází k poměřování zásahu do práv a svobod osob s postihnutím pachatele trestného činu, k čemuž slouží test proporcionality. Tento test je tak užíván v případě soukromých záznamů, kdy je záznamem zasaženo do práv a svobod jednotlivců. O přípustnosti takového důkazu rozhoduje vždy soud, který provádí test proporcionality v návaznosti na konkrétní okolnosti případu. Již samotné natáčení či fotografování, kdy dochází k zachycené podoby osoby, vede k zásahu do osobnostních práv, resp. práva na soukromí, proto bude docházet zejména k poměřování práva na soukromí a objasnění trestné činnosti.

V případě přípustnosti v užším smyslu se jedná o nepřípustnost vztahující se k pramenu důkazu.[143] Protože v TRŘ neexistuje vylučující klauzule jako tomu je v jiných trestních řádech, je třeba nahlédnout do judikatury a právní teorie. Nepřípustné důkazy v užším smyslu lze pro zjednodušení rozdělit do dvou skupin. Do první skupiny řadíme důkazy, které pochází z takových pramenů, u kterých není možné *„ověřit si výsledky určitých postupů dostupnými vědeckými metodami.“* [144] Takovýmto důkazem může být důkaz získaný užitím polygrafu, [145] či předpověď jasnovidce. V druhé skupině pak nalezneme důkazy, které

[141] FRYŠTÁK, Marek. *Dokazování v přípravném řízení*. Brno: Masarykova univerzita, 2015, s. 173. 978-80-210-7687-7.

[142] ZEMAN, P. Dokazování v českém trestním řízení po roce 1990 očima soudců a státních zástupců. *Trestněprávní revue*. roč. 2009, č. 6. ISSN 1213-5313.

[143] JELÍNEK, Jiří, ed. *Dokazování v trestním řízení v kontextu práva na spravedlivý proces*, s. 263. ISBN: 978-80-7502-287-5.

[144] ŠÁMAL, Pavel. Provádění dokazování v hlavním líčení a úprava absolutní a relativní neúčinnosti důkazů ve věcném záměru nového trestního řádu. *Trestněprávní revue.* roč. 2008, č. 12.

[145] Usnesení Nejvyššího soudu ze dne 25.03.1992, sp. zn. 6 To 12/92. In: *Sbírka Nejvyšší soud* [online]. Nejvyšší soud [cit. 26.9.2024]. Dostupné z: https://sbirka.nsoud.cz/sbirka/12287/

byly získány mimo procesní dokazování, úkony učiněnými před zahájením trestního stíhání (mimo neodkladné a neopakovatelné úkony) a jiné.[146]

V případě zákonnosti je třeba zkoumat, zda byl důkaz získán postupem v souladu s právními předpisy. V případě soukromých záznamů se bude jednat o nezákonný záznam, pokud *„skryté operativní prostředky* (tedy i záznamy*) použijí orgány státní moci způsobem, kterým obcházejí zákon, a vyhnou se tak přísnějším podmínkám v ustanoveních trestního řádu shora naznačených.“*[147] Je tomu tak z toho důvodu, že pravidla TRŘ upravující postup opatřování důkazů OČTŘ se na opatřování důkazů soukromými osobami neuplatní. Cílem je tedy zamezit situacím, kdy by OČTŘ *„požádal či vyzval soukromou osobu, aby důkaz obstarala, popř. jí k tomu poskytl potřebné technické prostředky či jinou součinnost.“*[148] V případě, kdy je protiprávně zasaženo do osobnostního práva jednotlivců, může se i přes to jednat o procesně použitelný důkaz. „*S ohledem na ustanovení § 89 odst. 2 trestního řádu nelze vyloučit možnost, aby byl k důkazu použit i zvukový záznam pořízený soukromou osobou bez souhlasu osob, jejichž hlas je takto zaznamenán,*[149] přičemž stejně by tomu mělo být i u obrazových záznamů. Bude zapotřebí pro každý takovýto individuální případ provést test proporcionality, u kterého bude *„uvažováno o legitimitě cíle, kterého má být prostřednictvím provedení tohoto důkazu dosaženo, na straně druhé musí být posouzena přiměřenost užitého postupu, a to vždy přísně individuálně.“*[150]

Rozlišovat však mezi nezákonností a přípustností v užším smyslu není v praxi podstatné, jelikož obě vedou k neúčinnosti důkazu. Je však zapotřebí rozlišováno mezi neúčinnost absolutní a relativní (k této neúčinnosti viz výše). Příkladem absolutní neúčinnosti důkazu mohou být již zmiňované záznamy obstarané na základě postupu OČTŘ, které obcházejí ustanovení TRŘ. Naopak tomu je u neúčinnosti relativní, kdy podstatnou vadu je možno zhojit.

---

[146] PÚRY, František. §89 In: ŠÁMAL, Pavel. a kol.: *Trestní řád I. 7. vydání.* [Systém Beck-online]. Praha: C. H. Beck, 2013, ISBN 978-80-7400-465-0. Dostupné také z: https://app-beck-online-cz.ezproxy.is.cuni.cz/bo/document-view.seam?documentId=nnptembrgnpwk5tlge3c443cl4ytsnrrl4ytimk7obtdqoi# s. 1308 – 1394.

[147] Usnesení Ústavního soudu ze dne 20. 10. 2011, sp. zn. II. ÚS 143/06. In: *Salvia* [online]. Ústavní soud [cit. 7.7.2024]. Dostupné z: https://kraken.slv.cz/II.US143/06.

[148] TIBITANZLOVÁ, Alena, ZAORÁLOVÁ, Petra. Použitelnost soukromých zvukových a obrazových záznamů jako důkazu v trestním řízení In: *Bulletin advokacie*. roč. 2023, č. 9.

[149] Rozsudek Nejvyššího správního soudu ze dne 19.10.2017, č.j. 4 Tdo 1055/2017.

[150] Rozsudek Nejvyššího správního soudu ze dne 18. 11. 2011, č.j. 2 As 45/2010-68. In: *Sbírka Nejvyšší soud* [online]. Nejvyšší správní soud [cit. 4.7.2024]. Dostupné z: https://sbirka.nssoud.cz/cz/ochrana-osobnich-udaju-pouzitelnost-kameroveho-zaznamu-porizeneho-soukromou-osobou.p2474.html.

V případě, kdy soukromá osoba provozuje kamerový systém, který systematicky ukládá kamerový záznam (na základě kterého lze identifikovat osobu) bez oznámení Úřadu pro ochranu osobních údajů, nejedná se za všech okolností o nezákonný důkaz. Provozování systému bez tohoto systému *„má pouze ten následek, že, má-li být jím pořízený záznam použit jako důkaz ve správním či soudním řízení, bude nutné provést má-li být jím pořízený záznam použit jako důkaz ve správním či soudním řízení, bude nutné provést celkové posouzení, zda docházelo ke zpracovávání osobních údajů v rozporu se zákonem, či nikoliv.“* [151] *„Přípustnost takového důkazu je však nezbytné vždy posuzovat i s přihlédnutím k právu na soukromí zakotvenému v čl. 8 Úmluvy o ochraně lidských práv a základních svobod a na nedotknutelnost osoby a jejího soukromí ve smyslu čl. 7 a čl. 10 odst. 2 Listiny základních práv a svobod*.“[152]

Jinak by tomu však bylo v případě, kdy by Policie (či jiný vykonavatel veřejné správy) provozovala kamerový systém bez oznámení příslušnému úřadu. V takovémto případě by existoval *„mezi pořizovatelem záznamu a dotčenou osobou (do jejíhož osobnostního práva bylo záznamem zasaženo) vztah vertikální, přičemž musí být takový postup zákonem výslovně předpokládán a musí být striktně splněny všechny podmínky zákonem vyžadované.“* [153] Pokud tedy Policie provozuje kamerové záznamy v rozporu se zákonnými předpisy, tyto záznamy není možné v trestním řízení použít jakožto důkazní prostředek, tedy ani pro analýzu těchto záznamů FR systémem.

[151] Ibid.

[152] Usnesení Nejvyššího soudu ze dne 3.06.2009, čj. 3 Tdo 593/2009 In: *Aspi* [online]. Nejvyšší soud [cit. 4.7.2024]. Dostupné z: https://www.aspi.cz/products/lawText/4/151842/1/2.

[153] Rozsudek Nejvyššího správního soudu ze dne 18. 11. 2011, č.j. 2 As 45/2010-68. In: *Sbírka Nejvyšší soud* [online]. Nejvyšší správní soud [cit. 4.7.2024]. Dostupné z: https://sbirka.nssoud.cz/cz/ochrana-osobnich-udaju-pouzitelnost-kameroveho-zaznamu-porizeneho-soukromou-osobou.p2474.html.

6. Problematika referenčních databází

Problematické při všech způsobech užívání FR systémů je vedení referenční databáze FR systémů. Již v současné době Policie provozuje informační systém Digitální podoba osob, jehož součástí je referenční databáze skládající se z fotografii zdrojových databází *„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.“* [154] Tento systém tak ve své referenční databázi obsahuje fotografie téměř všech občanů a dalších osob nacházejících se na území České republiky.

Je však problematické, že státem vytvořené a spravované biometrické databáze obsahující obličejové snímky osob bez konkrétního důvodu jsou v rozporu se základními právy.[155] Uchovávání fotografií osob v databázích po neomezenou dobu bez ohledu na závažnost trestného činu vyvolává značné obavy ohledně zásahu do základních práv a svobod osob, především ochrany soukromí a proporcionality zpracování osobních údajů, což bylo potvrzeno i ESLP. Je však třeba mít na paměti, že Policie k informacím z civilních registrů má přístup i mimo provozování FR systém, přičemž informace k těmto registrům potřebuje k naplňování úkonů, jako je například identifikace osob při běžným administrativních úkonech. Myslím si však, že je zásadní rozdíl mezi využitím fotografií z evidencí pro běžnou identifikaci osob, s nimiž Policie denně přichází do styku při administrativních činnostech, a přenesením a zpracování fotografií do samostatné referenční databáze po neomezeně dlouhou dobu. Skrze užití FR systému pak dochází ke zpracovávání biometrických údajů pro účely trestního řízení nebo pátrání po osobách.

Je zřejmé, že neomezené uchovávání fotografií, jejich zpracování do šablon a následné využití vede k dosažení legitimních cílů, které jsme si určili v návaznosti na konkrétní způsob využití FR systémů v předchozích kapitolách, tzn. veřejné bezpečnosti či objasnění trestné činnosti. Problematičtější je však z mého pohledu rozsah zásahu do základních práv a svobod. Neomezené ukládání a zpracování fotografií osob bez návaznosti na předchozí trestnou činnost způsobuje zásah do práv všech osob, jejichž fotografie se nacházejí v referenční databázi. Pokud však máme dospět k dosažení všech legitimních cílů stejně rychle a efektivně, domnívám se, že neexistuje jiný, stejně efektivní a rychlý prostředek, který by

[154] §66a zákona č. 273/2008 Sb. o Policii České republiky.

[155] KUHLMANN, Simone. Government Use of Facial Recognition Technologies under European Law. In: ZALNIERIUTE, Monika a Rita MATULIONYTE, eds. *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge: Cambridge University Press, 2024. s. 127-138 DOI: 10.1017/9781009321211.012.

zasahoval do práv osob v menším měřítku. Je tak zapotřebí zkoumat proporcionalitu v užším smyslu a poměřit zásah do práv osob se zajištěním veřejné bezpečnosti a objasnění trestné činnosti. Ke zkoumání proporcionality v užším smyslu se již několikrát vyjádřil ESLP ve své judikatuře.

K uchovávání fotografií v databázi se vyjádřil ESLP, kdy ve věci Gaughram proti Spojenému království rozhodl, že uchovávání biometrických údajů, konkrétně fotografie stěžovatele, na dobu neurčitou, představuje porušení práva na ochranu osobních údajů, a není tak proporcionální k ochraně veřejné bezpečnosti.[156] V tomto případě šlo o fotografii stěžovatele, která byla pořízena během jeho zatčení za řízení pod vlivem alkoholu. Soud namítal, že *„biometrické údaje a fotografie žadatele byly uchovávány bez ohledu na závažnost jeho činu a bez ohledu na pokračující potřebu uchovávat tyto údaje na dobu neurčitou.“*[157] Na základě argumentu *ad minori ad maius* lze dojít k závěru, že pokud není možné pro neomezenou dobu uchovávat v kriminalistické databázi fotografie osob odsouzené pro nezávažné trestné činy, nelze po neomezenou dobu uchovávat fotografie osob z civilních registrů v referenčních databází FR systémů bez souvislosti s trestným činem, jako je tomu například v případě informačního systému Digitální podoba osob.

Dalším podobným případem je pak rozhodnutí věci S. a Marper proti Spojenému království z roku 2008, kdy ESLP rozhodl, že neomezené uchovávání DNA profilů a otisků prstů osob, které nebyly odsouzeny za trestný čin, porušuje čl. 8 Úmluvy.[158] Soud konstatoval, že uchovávání osobních údajů (včetně biometrických) na neomezeně dlouhou dobu bez jakéhokoli rozlišení mezi osobami odsouzenými za závažné trestné činy a těmi, kteří byli jen zatčeni nebo obviněni, je nepřiměřené. Tento soud pak také zdůraznil, že uchovávání citlivých údajů musí být přiměřené a sloužit legitimnímu účelu, jako je prevence kriminality nebo ochrana veřejného pořádku. Pouhé potenciální využití dat v budoucnosti k těmto účelům však není dostatečným důvodem pro jejich neomezené uchovávání

K této otázce se ESLP vyjádřil i ve věci P.N. proti Německu, kdy potvrdil, že uchovávání fotografie, otisků prstů a dlaní v policejní databázi po dobu pěti let neporušuje právo podle čl. 8 Úmluvy, protože bylo provedeno individuální hodnocení rizika opětovného spáchání trestného činu a kontrola potřeby dalšího uchovávání údajů.[159]

[156] Rozhodnutí ESLP ze dne 13. 2. 2020, ve věci Gaughran proti Spojenému království. č. 45245/15.
[157] Ibid.
[158] Rozhodnutí ESLP ze dne 4. prosince 2008, ve věci S. a Marper proti Spojenému království. č. 30562/04 a 30566/04.
[159] Rozhodnutí ESLP ze dne 11.6.2020, ve věci P. N. proti Německu. č. 74440/17.

V případě neomezeného uchovávání fotografií v databázích FR systémů tak vidím závažný problém, neboť neomezené uchovávání fotografií považuji za nepřiměřené a v rozporu s výše zmiňovanou judikaturou, ze které konkrétně vyplývá, že uchovávání fotografií či jiných biometrických údajů v databázích osob po neomezeně dlouhou dobu je nepřiměřené. *A simili* lze říci, že vedení referenčních databází obsahující fotografie osob po neomezeně dlouhou dobu je stejně tak nepřiměřené. To však dle mého názoru neznamená, že je zapotřebí FR systém přestat užívat. Existují i jiné možnosti vedení databází, které by do práv osob zasahovaly v menším rozsahu a splňovaly by kritérium přiměřenosti.

Jednou z takových variant je, aby fotografie osob byly v databázi uchovávány po mezenou dobu za nastavení přísných pravidel pro uchovávání dat, které by omezily dobu jejich uložení pouze na období nezbytné pro konkrétní účely, například vyšetřování trestné činnosti či pátrání po konkrétní osobě. Po uplynutí doby, která byla zapotřebí k dosažení stanoveného účelu, by fotografie dotčených osob musely být automaticky smazány. Další alternativní variantou je pak vytvoření referenční databáze, která obsahuje fotografie pouze osob obviněných či odsouzených, jako je tomu například u databází otisků prstů nebo DNA. Na rozdíl od databáze otisků prstů nebo DNA však můžou OČTŘ využít již existující databáze fotografií osob z centrálních evidencí,[160] a tudíž není zapotřebí specificky fotografovat tyto osoby pro účely referenční databáze FR systémů. Domnívám se, že i fotografie obviněných a odsouzených osob by měly být v databázi pouze po omezenou dobu, a to v návaznosti na výše zmiňovanou judikaturu ESLP.

Závěrem lze tedy říci, že neomezené uchovávání fotografií v referenčních databází FR systémů je v rozporu s judikaturou ESLP. Existují však i jiné možnosti vedení databází, než které jsem v této práci představila, avšak v tomto ohledu záleží na zákonodárci, aby vybral nejvhodnější formu fungování referenčních databází FR systémů.

[160] SMITH, Marcus, MILLER, Seumas. *Biometric Identification, Law and Ethics.* Springer 2021. s. 23. ISBN 978-3-030-90256-8.

7. Evropská právní úprava

S rozvojem technologie v jednotlivých státech Evropské unie došlo k rozvoji využívání AI v různých oblastech. V reakci na tento rozvoj bylo zapotřebí, aby technologie využívající AI, mezi které patří taktéž FR systém, byly užívány způsobem respektující evropské prostředí. 13 března 2024 schválil Evropský parlament a následně 21. května Rada Evropské unie historicky světově první komplexní regulaci upravující užívání AI známé pod názvem Akt o AI. *„Cílem nového legislativního aktu je podpořit rozvoj a zavádění bezpečné a důvěryhodné umělé inteligence po celém jednotném trhu EU subjekty z veřejného i soukromého sektoru. Zároveň je jeho cílem zajistit dodržování základních práv občanů EU a stimulovat investice a inovace v oblasti umělé inteligence v Evropě.“*[161] Užívání AI v oblastech vojenství, obrany, či výzkumu je však i nadále ponecháno na jednotlivých státech.

Mimo například regulaci vývoje AI či její užívání na evropském trhu se Akt o AI zaměřuje také na minimalizaci rizik spojených s technologiemi AI, zejména v oblasti bezpečnosti, kam spadá taktéž užívání FR systémů. Akt o AI nabude účinnosti 24 měsíců od jeho vstupu v platnost, což je 20 dní od vyhlášení v Úředním věštníku Evropské unie. Některé části nařízení však nabydou účinností dříve. Ustanovení pro zakázané praktiky budou účinné 6 měsíců po vstoupení v platnost, obecná pravidla pak po 12 měsících, avšak legislativa uvedená v příloze I nařízení nabude účinnosti až po 36 měsících. Je však zapotřebí, aby v jednotlivých státech unie došlo ke změně právní úpravy, a to v souladu s Aktem o AI, jinak nebudou moci orgány vymáhající právo za pomocí FR systémů tuto technologii užít. Toto nařízení však nebrání jednotlivým státům unie přijmout přísnější úpravu, nebo dokonce i například FR systémy zcela zakázat. Mimo jiné s účinností od 21. února 2024 dala Evropská komise vzniknout Evropskému úřadu pro umělou inteligenci, který slouží jakožto poradní orgán a zároveň bude moci poskytovat doporučení a stanoviska týkající se implementace tohoto nařízení.

7.1. Kategorizace rizik

Akt o AI zavádí systém kategorizace AI dle posouzení rizik pro člověka, které rozřazují všechny aplikace AI do jedné ze 4 kategorií: nepřijatelné riziko, vysoké riziko, omezené riziko a minimální riziko. V případě kategorie zakázaných systémů upravené čl. 5, tj. kategorie pro nepřijatelně vysoká rizika, zahrnuje tato kategorie například technologie

[161] Akt o umělé inteligenci (AI): Rada s konečnou platností schválila celosvětově první pravidla pro AI. In: *Consilium* [online] [cit. 07.07.2024]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/

využívající techniky manipulující lidské chování, zneužívající zranitelnosti konkrétních skupin či zavádějící systém sociálního kreditu. Patří zde také technologie FR systémů užívaná v reálném čase na veřejných místech. Pro tuto technologie však existují výjimky, a to pokud je užívána pro jeden ze stanovených účelů, které si rozebereme níže.

Technologie zpětného rozpoznávání obličejů (dle nařízení „systémy biometrické identifikace na dálku“) na veřejných místech spadá do druhé kategorie, tedy kategorie vysoce rizikového systému dle čl. 6 nařízení. Výjimkou jsou však FR systémy, které se používají k ověření, zda daná fyzická osoba je skutečně tou, za koho se vydává. Do kategorie vysoce rizikového systému patří mimo technologie rozpoznávající obličeje také nástroje, které mohou významně ovlivnit bezpečnost, zdraví nebo základní práva jednotlivců, či další nástroje zmíněné v příloze III tohoto nařízení (pokud však nepředstavují *„nepředstavuje významné riziko újmy na zdraví, bezpečnosti nebo základních právech fyzických osob“).* Pokud systém spadá do této kategorie, musí splňovat přísné požadavky, které jsou upraveny v čl. 12 až 15 tohoto nařízení, mezi které patří například vypracování technické dokumentace a její následná aktualizace, transparentnost a dohled.

Kategorie omezeného rizika zahrnuje například aplikace AI jako jsou například chatboti nebo virtuální asistenti. V případě užití těchto systému musí být systémy transparentní, a tudíž informovat uživatele, že neinteragují s lidskou bytostí, nýbrž s AI. Systémy s minimálním rizikem pak zahrnují takové aplikace AI, které nemají významný dopad na práva a bezpečnost jednotlivců. Mezi takové systémy můžeme zařadit hry či filtry obrázků, přičemž na tuto kategorii systémů se nevztahuje žádná specifická regulace zavedená Aktem o AI.

7.2. Podmínky pro užívání technologie rozpoznávání obličejů

Užití FR systémů v reálném čase bude možné pouze pro specifické účely vymáhání práva. Mezi tyto účely dle čl. 6 nařízení patří například pátrání po specifickém okruhu osob jako jsou například únosy, identifikace pachatelů trestných činů, kterým hrozí za spáchání trestného činu trest odnětí svobody s horní hranicí v délce nejméně čtyři roky (popřípadě ochranné opatření zbavující osobu osobní svobody ve stejné délce) a jedná se přitom o pachatele jednoho z trestných činů dle seznamu v příloze II nařízení, za účelem prevence konkrétních a významných hrozeb pro veřejnou bezpečnost, teroristické útoky a jiné. K užití FR systémů na veřejných místech bude zapotřebí příslušné povolení justičního orgánu nebo nezávislého správního orgánu členského státu. V případě naléhavých situacích, kdy není možné o povolení zažádat před užitím systému, musí do 24 hodin od užití donucující orgán dodatečně zdůvodnit

svou potřebu užití FR systému a dodatečně o povolení požádat. V případě negativního vyřízení žádosti bude muset donucující orgán užití systému zastavit a v případě, že k užití systému již došlo, veškeré záznamy vymazat. Užití FR systémů na veřejných místech mimo donucovací orgány budou zakázány. V případě porušení tohoto zákazu hrozí poskytovatelům systémů AI vysoké pokuty, a to až 35 milionů eur nebo 7 % celosvětového obratu.

Donucovací orgány však FR systémy nemohou používat jen tak. Před zahájením jejich užívání je zapotřebí, aby *„příslušný donucovací orgán dokončil posouzení dopadů na základní práva, a nestanoví-li nařízení jinak, zaregistroval systém v databázi podle nařízení.“*[162] OČTŘ musí být transparentní ohledně používání technologie rozpoznávání obličejů. V případě užití FR systémů za účelem vymáhání práva je zapotřebí, aby provozovatel systému oznámit užití systému příslušnému úřadu pro dohled. Ten musí v jednotlivých státech buďto vzniknout, nebo jeho působnost převezme již existující jiný úřad v daném státě. Tyto úřady pak vytvářejí každoroční report, který zasílají Evropské komisi, která pak každoroční report publikuje.

V případě zpětného užití pak bude možné FR systémy použít za účelem pátrání po osobě podezřelé či již odsouzené za trestné činy dle čl. 26 nařízení. I v takovémto případě je zapotřebí získat povolení před užitím FR systému nebo nejpozději do 48 hodin od užití systému dodatečně o takovéto povolení požádat. Výjimkou je užití FR systému k *„identifikaci potenciálního podezřelého na základě objektivních a ověřitelných skutečností přímo souvisejících s trestným činem.“* [163] Je ovšem zapotřebí, aby nebyl „*systém AI pro následnou biometrickou identifikaci na dálku používán pro účely vymáhání práva necíleným způsobem, bez jakékoli souvislosti s určitým trestným činem, trestním řízením, skutečnou a aktuální nebo skutečnou a předvídatelnou hrozbou trestného činu nebo pátráním po konkrétní pohřešované osobě.“*[164] Jelikož se jedná o zpětné užití, které spadá do kategorie vysoce rizikových systémů, bude v souvislosti s užitím FR systémů zapotřebí, aby systémy splnily přísné požadavky, jako je například posouzení dopadů na lidská práva, uchovávání dokumentace, informační povinnost vůči orgánu dohledu a jiné.

Kamerový systém napojený na FR systémy na Letišti Václava Havla spadá jakožto systém fungující v reálném čase do kategorie zakázaných systémů, resp. systémů s nepřijatelným rizikem. V případě informačního systému Digitální podoby osob jakožto systému fungující zpětně, je tento systém řazen do kategorie systémů s vysokým rizikem.

[162] Bod 34 Akt o AI.
[163] Čl. 26 (10) Aktu o AI.
[164] Ibid.

To s sebou přináší úskalí pro fungování těchto systémů v blízké budoucnosti. Na tuto situaci tak již reagovalo Ministerstvo vnitra předložením novely, která má upravovat FR systémy užívané v reálném čase, čímž se snaží využít možnosti danou samotným nařízením, dle kterého lze podrobnosti fungování FR systémů upravit vnitrostátně.[165]

7.3. Hodnocení této úpravy

Je zcela zřejmé, že se stále větším a rychlejším vývojem AI byla revoluční právní úprava potřeba. Stále více státu Evropské unie užívá FR technologie za účelem identifikace pachatelů trestných činů, avšak ve většině států chyběla podrobná právní úprava. Rozdělení FR systémů do rozdílných kategoriích, a to dle povahy užití na reálné a zpětné je dle mého názoru zbytečné, a to z hlediska zásahu do základních práv. Rozdíl v užití technologie zpětně nebo v reálném čase se dle mého názoru jeví jako čistě technický rozdíl, který spočívá pouze ve dvou různých okamžicích procesu identifikace. Tento rozdíl v čase, kdy dochází k identifikaci osoby, neovlivňuje míru zásahu do soukromí a osobních práv, jelikož využívá stejné technologie a stejnou databázi, což vede k obdobným dopadům na soukromí.

Slabinou této právní úpravy pak může být udělení výjimky z důvodu národní bezpečnosti, kdy se Akt o AI neuplatní v případech vývoje a užití FR systémů za účelem národní bezpečnosti. Co spadá do účelu národní bezpečnosti záleží na interpretaci jednotlivých států unie, což může vést k obcházení tohoto nařízení. Navíc, takovéto užití pak umožňuje nedodržovat jakékoli technické nebo právní záruky, které jsou pro technologii tohoto typu potřeba.

Problémem tohoto nařízení může být také rozhodnutí ohledně orgánu povolující užití FR v jednotlivých případech. Členské státy na základě tohoto nařízení mohou samy rozhodovat, která entita bude povolovat konkrétní užití FR systémů. Může jí být jak soudní, tak nezávislý správní orgán. V případě soudního orgánu o jeho nezávislosti není pochyb, protože soudní orgány naplňují nejvyšší kritéria pro nezávislost orgánu. V případě nezávislého správního orgánu je však možné, že standardy nezávislosti budou nižší, a tedy může dojít k jeho ovlivňování.

[165] Bezpečnější cestování i lepší výměna informací In: *MVCR* [online] [cit. 04.10.2024]. Dostupné z: https://www.mvcr.cz/clanek/bezpecnejsi-cestovani-i-lepsi-vymena-informaci-resort-vnitra-pripravil-zmenu-zakona-o-policii-i-o-zpracovani-osobnich-udaju.aspx.

Závěr

V této diplomové práci jsem se zaměřila na analýzu problematiky využití FR systémů za účelem identifikace pachatelů trestných činů. Hlavním cílem této práce bylo odpovědět na výzkumnou otázku, zda-li je užívání systémů na rozpoznávání obličeje Policií České republiky v souladu s českým právním řádem.

Abych mohla odpovědět na výzkumnou otázku, na začátku této diplomové práce jsem práce se zaměřila na teoretické vymezení AI a FR systémů. Mimo to jsem se v této úvodní kapitole snažila vysvětlit, jak prakticky biometrické systémy, v čele s FR systémy, fungují. Toto vymezení bylo podstatné pro pochopení navazujících kapitol, které předpokládaly znalosti fungování FR systému. V následující kapitole jsem nastínila současné využívání FR systému v České republice, a to zejména pro demonstraci, že FR systémy nejsou pouze teoretickými systémy, ale mají v České republice uplatnění. Přestože je cílem této práce zdůvodnit, zdali je užití FR systému v souladu s českým právním řádem, v této kapitole jsem ve zkratce popsala, jak jsou FR systémy využívány i ve světe. Chtěla jsem tak demonstrovat, jak bez stanovení mezí a nerespektování lidských práv a svobod může dojít k nadměrnému zasahování do základních práv a svobod jako je tomu například v Číně, Spojených arabských emirátech a Rusku. Tyto dvě kapitoly byly spíše popisné, přičemž v následujících kapitolách bylo analyzováno užívání FR systémů dle české právní úpravy.

Ve třetí kapitole této práce jsem se zaměřila na analyzování využití FR systému za účelem hledání osob. Díky výkladu současné právní úpravy jsem došla k závěru, že použití FR technologií Policií ČR je možné na základě zákona o Policii, a to za účelem hledání osob. Problematické jsem však shledala užívání FR systému z důvodu zásahu do práva na soukromí, přičemž díky testu proporcionality jsem došla k závěru, že použití FR systémů může být proporcionální, pokud bude striktně dodržován legislativní rámce ochrany soukromí a osobních údajů společně se zavedením kontrolních mechanismů.

V případě další kapitoly zaměřené na užití FR systémů za účelem vyhledávání a zajištění důkazů jsem došla k závěru, že současná právní úprava neomezuje použití FR systémů v závislosti na závažnost trestných činů ani nestanovuje podmínky pro jeho užití, což vede k riziku nepřiměřeného zásahu do soukromí. Aby FR systémy prošly testem proporcionality, je třeba upravit právní rámec, který by přesně vymezil podmínky a omezení jejich využívání. Z tohoto důvodu jsem se věnovala úvahám *de lege ferenda* stanovující podmínky užívání FR systémů, aby jejich užití bylo v souladu s trestněprávní úpravou České republiky. Těmito podmínkami by mělo být užívání FR systému pro úmyslné trestné činy

za předpokladu povolení státního zástupce či soudce. Navíc informační povinnost a možnost přezkumu zákonnosti použití těchto systémů jsem shledala jako klíčovou pro ochranu základních práv a zajištění spravedlivého procesu.

V páté kapitole jsem se věnovala užití výstupu FR systému v řízení před soudem za účelem ztotožnění jednotlivce. Došla jsem k závěru, že je nezbytné zajistit, aby obžalovaný měl možnost rozumět a reagovat na výsledky této technologie, včetně chybovosti a podrobností fungování FR systémů. Mimo to je zapotřebí při užití výstupů FR systémů v řízení před soudem zohlednit ne/účinnost kamerových záznamů jakožto důkazního prostředku.

V šesté kapitole jsem se věnovala vedení referenční databáze, které vyvolává vážné obavy ohledně ochrany soukromí, a to zejména kvůli časově neomezenému uchovávání fotografií osob. Na základě judikatury jsem došla k závěru, že neomezené uchovávání bez ohledu na závažnost trestného činu je nepřiměřené. Je proto zapotřebí zavést jasná pravidla a pravidelná hodnocení pro uchovávání fotografií v databází FR systémů. V poslední kapitole jsem pak představila novou evropskou právní úpravu, tzv. Akt o AI, která zavádí nová pravidla pro užívání FR systémů.

Seznam použitých zdrojů

Knihy

DRAŠTÍK, Antonín, FENYK, Jaroslav a kol. *Trestní řád. Komentář. II. Díl* [Systém ASPI]. Praha: Wolters Kluwer ČR, 2017, §89, bod. 17. ISBN978-80-7552-601-4.

FRYŠTÁK, Marek. *Dokazování v přípravném řízení*. Brno: Masarykova univerzita, 2015, s. 173. 978-80-210-7687-7.

FRYŠTÁK, Marek. *Znalecké dokazování v trestním řízení - 2. vydání*. Wolters Kluwer, 2021. s. 3. ISBN 978-80-7676-063-9.

GERLOCH, Aleš, TRYZNA, Jan. WINTR, Jan eds. *Metodologie interpretace práva a právní jistota*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2012. s. 263. ISBN978-80-7380-388-9.

GŘIVNA, Tomáš a kol. *Vliv nových technologií na trestní právo*. Auditorium, 2022, s. 261. ISBN 978-80-87284-95-7.

RAK, Roman, MATYÁŠ, Václav, ŘÍHA, Zdeněk. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha : Grada Publishing, 2008, s. 115. ISBN 978-80-247-2365-5.;

JELÍNEK, Jiří a kol. *Trestní právo procesní 6. vydání*. Leges. 2022. str. 400. ISBN 978-80-7502-550-0.

JELÍNEK, Jiří a kol. *Trestní právo procesní 7. aktualizované a doplněné vydán*í. Leges. 2023. s. 416. ISBN 978-80-7502-687-3.

JELÍNEK, Jiří, ed. *Dokazování v trestním řízení v kontextu práva na spravedlivý proces*. Praha: Leges, 2018, s. 263. ISBN: 978-80-7502-287-5.

Ibid. ISBN: 978-80-7502-287-5.

KOKEŠ, Marian. Článek 10 In: HUSSEINI, F., BARTOŇ, M., KOKEŠ, M., KOPA, M. a kol. *Listina základních práv a svobod. Komentář. 1. vydání*. [Systém Beck-online]. Praha: C. H. Beck, 2021. ISBN 978-80-7400-812-2.

KRATOCHVÍL, Jan. Článek 8 In: KMEC, J., KOSAŘ, D., KRATOCHVÍL, J., BOBEK, M. *Evropská úmluva o lidských právech. Komentář. 1. vydání.* [Systém Beck-online]. Praha: C. H. Beck, 2012. s. 863 – 962. ISBN: 978-80-7400-365-3.

MELZER, Filip. *Metodologie nalézání práva: úvod do právní argumentace.* Praha: C.H. Beck, 2010. s. 120. ISBN 978-80-7400-149-9.

NETT, Alexandr. *K problematice neúčinných důkazů v trestním řízení*. Brno: Vydavatelství MU, 1995. s. 6. ISBN 80-210-1163-7.

PORADA Viktor, POLÁK Peter, a kol. *Kriminalistika*. Plzeň: Aleš Čeněk, 2015. s. 31, 32. ISBN 978-80-7380558-6.

PJEŠČAK, Ján. a kol. *Kriminalistika*. Bratislava: Obzor, 1981. s. 41. ISBN: 65-056-81.

STRAUS, Jiří, NĚMEC, Miroslav, a kol. *Teorie a metodologie kriminalistiky*. Plzeň: Aleš Čeněk, 2009, s. 137. ISBN 978-80-7380-214-1.

STŘÍŽ, Igor et al. *Trestní zákoník a trestní řád 2. díl*. Praha: Linde Praha, 2010, s. 304. ISBN978-80-7201-803-1.

ŠÁMAL, Pavel. a kol. *Trestní řád I. 7. vydání.* Praha: C. H. Beck, 2013, s. 1333. ISBN: 978-80-7400-465-0.

VANGELI, Benedikt. *Zákon o Policii České republiky. Komentář. 2. vydání*. Praha: C. H. Beck, 2014, s. 351. ISBN 978-80-7400-543-5.

WAGNEROVÁ, Eliška. Článek 10. In WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK a Ivo POSPÍŠIL. *Listina základních práv a svobod - Komentář*. Wolters Kluwer, 2012, s. 287. ISBN: 978-80-7357-750-6.

WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK a Ivo POSPÍŠIL. *Listina základních práv a svobod - Komentář*. Wolters Kluwer, 2012, s. 129. ISBN: 978-80-7357-750-6.

WAGNEROVÁ, Eliška. Právo na soukromí: Kde má být svoboda, tam musí být soukromí. In ŠIMÍČEK, Vojtěch, ed. *Právo na soukromí*. Brno: Muni Press, 2011.s. 51. ISBN978-80-210-5449-3.

WINTR, Jan. *Metody a zásady interpretace práva.* Praha: Auditorium, 2013. s. 45. ISBN 978-80- 87284-36-0.

ZAORALOVÁ, Petra. *Procesní použitelnost důkazů v trestním řízení a její meze*. Praha: Leges, 2018, s. 38–39. ISBN 978-80-7502-310-0.

Zahraniční knihy

ZALNIERIUTE, Monika a Rita MATULIONYTE, eds. *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge: Cambridge University Press, 2024, s. 127–138, 660. DOI: 10.1017/9781009321211.012.

MITSILEGAS, Valsamis. *Surveillance and privacy in the digital age: European, transatlantic and global perspectives*

STAHL, Bernd Carsten. *Artificial Intelligence for a Better Future: An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies*. Cham: Springer International Publishing, 2021, s. 10. DOI: 10.1007/978-3-030-69978-9.

SMITH, Marcus, MANN, a Monique. Facial Recognition Technology and Potential for Bias and Discrimination. In: *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge University Press, 2024. DOI: 10.1017/9781009321211.008.

SMITH, Marcus, MILLER, Seumas. *Biometric Identification, Law and Ethics.* Springer 2021. s. 23. ISBN 978-3-030-90256-8.

České odborné články

CIDLINA, Václav, PROKŮPEK, Jan, Legalita zavedení technologie rozpoznávání obličeje, In: *Bulletin Advokacie*, roč. 7-8/2020. s. 43.

MATEJKA, Ján, KRAUSOVÁ, Alžběta, GÜTTLER, Vojen. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie*, roč. 9., č. 18, s. 91–129. DOI 10.5817/RPT2018-1-5.

MATEJKA, Ján, MATOCHOVÁ, Soňa, PROKEŠ Josef. Analysis of Biometric Data Under the General Data Protection Regulation. *Acta Informatica Pragensia*. 2019, roč. 8, č. 2. DOI: 10.18267/j.aip.126.

MULÁK, Jiří. Základní zásady trestního řízení – jejich výjimečnost a výjimky z nich. *AUC IURIDICA*. 2023, roč. 69, č. 3, s. 40. DOI: 10.14712/23366478.2023.25.

NOVOTNÝ, Jiří. Dokazování v trestním řízení. *Forenzní vědy, právo, kriminalistika*. 2024, roč. 9, č. 1. DOI: 10.37355/fvpk-2024/1-01.

TIBITANZLOVÁ, Alena, ZAORÁLOVÁ, Petra. Použitelnost soukromých zvukových a obrazových záznamů jako důkazu v trestním řízení In: *Bulletin advokacie*. roč. 2023, č. 9.

ŠÁMAL, Pavel. Provádění dokazování v hlavním líčení a úprava absolutní a relativní neúčinnosti důkazů ve věcném záměru nového trestního řádu. *Trestněprávní revue.* roč. 2008, č. 12.

ZEMAN, P. Dokazování v českém trestním řízení po roce 1990 očima soudců a státních zástupců. *Trestněprávní revue*. roč. 2009, č. 6. ISSN 1213-5313.

Zahraniční odborné články

ANTEBI, Liran. *What is Artificial Intelligence?* Institute for National Security Studies, 2021, s. 31. [cit. 27.09.2024]. Dostupné také z: https://www.jstor.org/stable/resrep30590.7 (vlastní předklad).

BUOLAMWINI, Joy, GEBRU, a Timnit. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. PMLR, 2018 [cit. 04.07.2024]. Dostupné z: https://proceedings.mlr.press/v81/buolamwini18a.html.

BROWN, Tristan G., STATMAN, Alexander, SUI, Celine. Public Debate on Facial Recognition Technologies in China. *MIT Case Studies in Social and Ethical Responsibilities of Computing*. MIT Schwarzman College of Computing, 2021, č. Summer 2021. DOI: 10.21428/2c646de5.37712c5c.

GROTHER, Patrick, NGAN, Mei, HANAOKA, Kayee. Face recognition vendor test part 3: demographic effects. Gaithersburg, *MD: National Institute of Standards and Technology*, 2019, s. 7. DOI: 10.6028/NIST.IR.8280.

LUNTER, Jan. Beating the bias in facial recognition technology. *Biometric Technology Today*. Elsevier, 2020, roč. 2020, č. 9. DOI: 10.1016/S0969-4765(20)30122-3.

KNIGHT, Adam. Technologies of Risk and Discipline in China's Social Credit System. In: CREEMERS, R. J. E. H. TREVASKES, S. *Law and the Party in China: Ideology and Organisation*. Cambridge: Cambridge University Press. 2020. s. 237-263. Dostupné z: https://www.cambridge.org/core/books/abs/law-and-the-party-in-china/technologies-of-risk-and-discipline-in-chinas-social-credit-

MARTINEZ*,* Rex. Artificial Intelligence Distinguishing Between Types & definitions. *Nevada Law Journal*. Vol. 19: Iss. 3, Article 9 s. 1038. Dostupné z: https://scholars.law.unlv.edu/cgi/viewcontent.cgi?article=1799&context=nlj

NUTTER, Patrick W. Machine Learning Evidence: Admissibility and Weight. [online]. In: JOURNAL OF CONSTITUTIONAL LAW, 2019, roč. 21, č. 3. Dostupné z: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1691&context=jcl947Ibid., s. 947.

OLUSHOLA, Bayo. Overview of Biometric and Facial Recognition Techniques, *Journal of Computer Engineering.* Issue 4, Volume 20. s. 1. Dostupné také z: https://www.iosrjournals.org/iosr-jce/papers/Vol20-issue4/Version-1/A2004010105.pdf.

SALEEM, Sharzeel, SHINEY, J., SHAN, B. P., MISHRA. V.K. Face recognition using facial features. *Materials Today: Proceedings*,Volume 80, Part 3, 2023, s.1. ISSN 2214-7853.

PHILLIPS, P. Jonathon, An Other-Race Effect for Face Recognition Algorithms. *ACM Transactions on Applied Perception,* 2011. s.2. Dostupné z: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906254.

Důvodové zprávy

Důvodová zpráva k zákonu č. 111/2019 Sb., změna některých zákonů v souvislosti s přijetím zákona o zpracování osobních údajů [k § 66a zákona č. 273/2008 Sb.] [Systém Beck-online]. [cit. 03.10.2024]. Dostupné z:https://app-beck-online-cz.ezproxy.is.cuni.cz/bo/chapterview-document.seam?documentId=oz5f6mrqge4v6mjrgfpwi6q&rowIndex=0.

Judikatura

Nález Ústavního soudu České republiky ze dne 29. 7. 2013, sp. zn. I. ÚS 671/13. In: *Nalus* [online]. Ústavní soud [cit. 26.9.2024].

Nález Ústavního soudu České republiky ze dne 6. 2. 2009, sp. zn. II.ÚS 3201/08. In: *Nalus* [online]. Ústavní soud [cit.26.9.2024].

Nález Ústavního soudu České republiky ze dne 22.3.2011, sp. zn Pl. ÚS 24/10. In: *Nalus* [online]. Ústavní soud [cit. 3.7.2024].

Nález Ústavního soudu ze dne 15.12.2015, sp. zn. I. ÚS 1587/15. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024].

Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024].

Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024].

Nález Ústavního soudu ze dne 8.2.2010, sp. zn. IV.ÚS 2425/09. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024].

Nález Ústavního soudu ze dne 18. 12. 2006, sp. zn. I. ÚS 321/06. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024].

Nález Ústavního soudu ze dne 28. 3. 1996, sp. zn. I. ÚS 198/95. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024].

Nález Ústavního soudu ze dne ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024].

Nález Ústavního soudu ze dne 13. 8. 2002, sp. zn. Pl.ÚS 3/02. In: *Nalus* [online]. Ústavní soud [cit. 4.7.2024].

Nález Ústavního soudu ze dne 23. 5. 2007, sp. zn. II.ÚS 615/06. In: *Nalus* [online]. Ústavní soud [cit. 26.9.2024].

Nález Ústavního soudu ze dne 8. 2. 2010, sp. zn. IV.ÚS 2425/09. In: *Nalus* [online]. Ústavní soud [cit. 26.9.2024].

Nález Ústavního soudu ze dne 8. 3. 2012, sp. zn. III. ÚS 2260/10. In: *Salvia* [online]. Ústavní soud [cit. 26.9.2024].

Nález Ústavního soudu České republiky ze dne30. 11. 1995, sp. zn. II.ÚS 62/95 [online]. Ústavní soud [cit. 9.7.2024].

Usnesení Ústavního soudu ze dne 20. 10. 2011, sp. zn. II. ÚS 143/06. In: *Salvia* [online]. Ústavní soud [cit. 7.7.2024].

Rozsudek Nejvyššího správního soudu ze dne 19.10.2017, č.j. 4 Tdo 1055/2017. [online]. Nejvyšší správní soud [cit. 04.10.2024].

Rozsudek Nejvyššího správního soudu ze dne 27.4.2017, č.j. 1 As 134/2016-28 In: *Beck online* [online]. Nejvyšší správní soud [cit. 3.7.2024].

Rozsudek Nejvyššího správního soudu ze dne 18. 11. 2011, č.j. 2 As 45/2010-68. In: *Sbírka Nejvyšší soud* [online]. Nejvyšší správní soud [cit. 4.7.2024].

Usnesení Nejvyššího soudu ze dne 25.03.1992, sp. zn. 6 To 12/92. In: *Sbírka Nejvyšší soud* [online]. Nejvyšší soud [cit. 26.9.2024].

Usnesení Nejvyššího soudu ze dne 01.09.2020, čj. 7 Tdo 865/2020. In: *Sbírka Nejvyšší soud* [online]. Nejvyšší soud [cit. 4.7.2024].

Usnesení Nejvyššího soudu ze dne 3.06.2009, čj. 3 Tdo 593/2009 In: *Aspi* [online]. Nejvyšší soud [cit. 4.7.2024].

Rozsudek Nejvyššího správního soudu ze dne 18. 11. 2011, č.j. 2 As 45/2010-68. In: *Sbírka Nejvyšší soud* [online]. Nejvyšší správní soud [cit. 4.7.2024].

Usnesení Vrchního soudu ze dne 1.07.2016, čj. VSOL 5 To 46/2016. In: *Salvia* [online]. Nejvyšší soud [cit. 26.9.2024].

Rozhodnutí ESLP ze dne 13. 2. 2020, ve věci Gaughran proti Spojenému království. č. 45245/15.

Rozhodnutí ESLP ze dne 4. prosince 2008, ve věci S. a Marper proti Spojenému království. č. 30562/04 a 30566/04.

Rozhodnutí ESLP ze dne 11.6.2020, ve věci P. N. proti Německu. č. 74440/17.

Rozhodnutí ESLP ze dne 4. 7. 2023, ve věci Glukhin proti Rusku, č. 11519/20.

Rozsudek ESLP ze dne 6. září 1978, ve věci Klass a ostatní proti Německu, č. 5029/71.

Rozhodnutí ESLP ze dne 4. 5. 2000, ve věci Rotaru proti Rumunsku. č. 28341.

Zpravodajské příspěvky

DAVIES, Dave. Facial Recognition And Beyond: Journalist Ventures Inside China's „Surveillance State". *NPR* [online]. 2021 [cit. 03.07.2024]. Dostupné z: https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta

Dubai Police to use biometrics to prevent crime. In: *Gulf News*. [online]. 20. 2. 2017 [cit. 03.07.2024]. Dostupné z: https://gulfnews.com/uae/dubai-police-to-use-biometrics-to-prevent-crime-1.1981638;

Dubai Police develop next-gen video surveillance biometrics, solve 3,000 crimes In: *Arabian Business* [online] 15. 3. 2023 [cit. 03.07.2024]. Dostupné z: https://www.arabianbusiness.com/industries/technology/dubai-police-develop-next-gen-video-surveillance-biometrics-solve-3000-crimes.

Dubai Police to introduce advanced body scanners to accurately identify suspects. In: *Zawya.* [online]. [cit. 03.07.2024]. Dostupné z: https://www.zawya.com/en/legal/crime-and-security/dubai-police-to-introduce-advanced-body-scanners-to-accurately-identify-suspects-q1qbg9lk.

HILL, Kashmir. Clearview AI Successfully Appeals $9 Million Fine in the U.K. In: *The New York Times* [online]. 2023 [cit. 03.07.2024]. Dostupné z: https://www.nytimes.com/2023/10/18/technology/clearview-ai-privacy-fine-britain.html.

How facial recognition is helping Putin curb dissent. *Reuters* [online]. 2023 [cit. 03.07.2024]. Dostupné z: https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/.

MCDONALD, Ryan Mac, Caroline Haskins, Logan. Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA. In: *BuzzFeed News* [online]. 28. 2. 2020 [cit. 03.07.2024]. Dostupné z: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

Pražští policisté „otevírají diskusi" o technologii na rozpoznávání obličejů. Hřib je proti. In: *Česká televize* [online]. [cit. 03.07.2024]. Dostupné z: https://ct24.ceskatelevize.cz/clanek/regiony/prazsti-policiste-oteviraji-diskusi-o-technologii-na-rozpoznavani-obliceju-hrib-je-proti-56924.

The Top 10 Most Surveilled Cities in the World. In: *US News* [online]. 2020 [cit. 26.09.2024]. Dostupné z: https://www.usnews.com/news/cities/articles/2020-08-14/the-top-10-most-surveilled-cities-in-the-world.

TROJÁNEK, Hynek. TZ: Policie již téměř rok využívá analytický nástroj na rozpoznávání tváří. Podrobnosti jeho fungování tají In: *Digitální svobody* [online]. 2023 [cit. 03.10.2024]. 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/.

Události, komentáře In: *Česká televize* [online]. 17. dubna 2023 [cit. 03.07.2024]. Dostupné z: https://www.ceskatelevize.cz/porady/1096898594-udalosti-komentare/223411000370417/.

World's first AI EagleEye Intelligent Patrol by Zenith makes a groundbreaking debut at Intersec Dubai. In: *Gulf News.* [online]. 20.1.2023 [cit. 03.10.2024]. Dostupné z: https://gulfnews.com/business/corporate-news/worlds-first-ai-eagleeye-intelligent-patrol-by-zenith-makes-a-groundbreaking-debut-at-intersec-dubai-1.1674220000046.

ZULHUSNI, Muhammad. How does the INTERPOL BioHub capture most wanted criminals? In: *Tech Wire Asia* [online]. 6. 12. 2023 [cit. 03.07.2024]. Dostupné z: https://techwireasia.com/2023/12/how-does-the-interpol-biometric-tool-capture-the-most-wanted/.

Ostatní webové příspěvky

Akt o umělé inteligenci (AI): Rada s konečnou platností schválila celosvětově první pravidla pro AI. In: *Consilium* [online] [cit. 07.07.2024]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/.

Aktualizace: Vyjádření k provozování informačního systému Digitálních podob osob - Policie České republiky [online]. [cit. 03.07.2024]. Dostupné z: https://www.policie.cz/clanek/vyjadreni-k-provozovani-informacniho-systemu-digitalnich-podob-osob.aspx.

Bezpečnější cestování i lepší výměna informací In: *MVCR* [online] [cit. 04.10.2024]. Dostupné z: https://www.mvcr.cz/clanek/bezpecnejsi-cestovani-i-lepsi-vymena-informaci-resort-vnitra-pripravil-zmenu-zakona-o-policii-i-o-zpracovani-osobnich-udaju.aspx.

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe [online]. 25. 4. 2018 [cit.03.10.2024]. Dostupné z: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51625.

Evropský hospodářský a sociální výbor. Bod 2.1. stanoviska Evropského hospodářského a sociálního výboru k tématu Umělá inteligence – dopady umělé inteligence na jednotný trh (digitální), výrobu, spotřebu, zaměstnanost a společnost. 2017. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52016IE5369&from=ES.

Hluboké učení vs. strojové učení - Azure Machine Learning. In: *Microsoft*. [online]. 19. 1. 2024 [cit. 01.07.2024]. Dostupné z: https://learn.microsoft.com/cs-cz/azure/machine-learning/concept-deep-learning-vs-machine-learning?view=azureml-api-2.

Human Rights Watch. United Arab Emirates: Events of 2022. In: *World Report 2023* [online]. 2023 [cit. 03.07.2024]. Dostupné z: https://www.hrw.org/world-report/2023/country-chapters/united-arab-emirates.

China's camps to erase Muslim beliefs. In: *Amnesty Internationa*l [online]. 15.3.2024 [cit. 03.10.2024]. Dostupné z: https://www.amnesty.org.uk/chinas-uighur-muslims-truth-behind-headlines.

MACH, Václav. Český Minority Report: Využití umělé inteligence Policií České republiky [online]. *Iuridicum Remedium (IuRe),* 2023. s. 35. Dostupné z: https://digitalnisvobody.cz/wp-content/uploads/2024/01/cesky_minority_report_iure_23.pdf.

Ministerstvo vnitra rozšíří zabezpečení Letiště Václava Havla o 145 kamer s automatickým rozpoznáváním obličejů - Ministerstvo vnitra České republiky. In: *MVCR* [online]. [cit. 01.10.2024]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-rozsiri-zabezpeceni-letiste-vaclava-havla-o-145-kamer-s-automatickym-rozpoznavanim-obliceju.aspx.

Ministerstvo vnitra pokračuje ve zvyšování bezpečnosti na mezinárodních letištích - Ministerstvo vnitra České republiky. In: *MVCR* [online]. [cit. 03.07.2024]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-pokracuje-ve-zvysovani-bezpecnosti-na-mezinarodnich-letistich.aspx.

Odborná skupina na vysoké úrovni pro umělou inteligenci. Definice UI: Hlavní Schopnosti a Obory. [online] 2018 [cit.03.10.2024] . Dostupné z: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60663.

Russia Uses Facial Recognition to Hunt Down Draft Evaders In: *Human Rights Watch* [online]. 2022 [cit. 03.10.2024]. Dostupné z: https://www.hrw.org/news/2022/10/26/russia-uses-facial-recognition-hunt-down-draft-evaders.

Systém detekce obličejů - Policie České republiky. In: *Policie* [online]. 2020. [cit. 01.07.2024]. Dostupné z: https://www.policie.cz/clanek/zverejnene-informace-2020-system-detekce-obliceju.aspx.

Stop governments spying on activists. In: *Amnesty International* [online]. 6. 10. 2020 [cit. 03.07.2024]. Dostupné z: https://www.amnesty.org/en/latest/campaigns/2020/10/stopspying/.

Stálá kontrolní komise pro kontrolu použití odposlechů a záznamů telekomunikačního provozu, sledování osob a věcí a rušení elektronických komunikací, Usnesení č. 25 ze dne 23. února 2017, dostupné z: https://www.psp.cz/sqw/text/text2.sqw?idd=102715.

Types of Biometrics: Face - Key Considerations In: *biometrics institute* [online] [cit. 03.10.2024]. Dostupné z: https://www.biometricsinstitute.org/types-of-biometrics-face-key-considerations/.

Úřad pro ochranu osobních údajů. Stanovisko. In: *UOOU*. [online]. 16. 8. 2019 [cit. 03.07.2024]. Dostupné z: https://uoou.gov.cz/uoou-k-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech.

Vyjádření k provozování informačního systému Digitálních podob osob In: Policie [online]. 20. července 2023. [cit. 2.10.2024]. Dostupné z: https://www.policie.cz/clanek/vyjadreni-k-provozovani-informacniho-systemu-digitalnich-podob-osob.aspx.

Využití systémů na rozpoznávání obličeje k identifikaci pachatelů trestných činů

Abstrakt

Tato diplomová práce analyzuje problematiku využití FR systémů pro identifikaci pachatelů trestných činů v kontextu českého právního řádu. Práce se zaměřuje především na soulad užívání FR systémů s právním řádem České republiky. V jednotlivých kapitolách je zkoumáno využití FR systémů pro hledání osob, vyhledávání důkazů a vytváření výstupů. Tato práce ukazuje, že současná právní úprava vyžaduje revizi a upřesnění podmínek použití FR systémů, aby se především minimalizovaly zásahy do práva na soukromí. Na závěr je představena nová evropská regulace, Akt o AI, která stanovuje nová pravidla pro používání FR systémů a reflektuje potřebu ochrany osobních práv v digitální éře.

Klíčová slova:

FR systém, AI, právo na soukromí

Use of Facial Recognition Systems for Identifying Criminal Offenders

Abstract

This thesis analyzes the issue of using FR systems for identifying criminal offenders within the context of the Czech legal framework. The thesis focuses primarily on the compatibility of FR systems with the legal order of the Czech Republic. The individual chapters explore the use of FR systems for locating persons, gathering evidence, and generating outputs. This work demonstrates that the current legal framework requires revision and clarification of the conditions for the use of FR systems, primarily to minimize infringements on the right to privacy. The thesis concludes by presenting the new European regulation, the AI Act, which sets new rules for the use of FR systems and reflects the need to protect personal rights in the digital era.

Key words:

FR system, AI, right to privacy