Spolek pro ochranu osobních údajů

Poziční dokument Spolku pro ochranu osobních údajů:[1]

Kamerové systémy a užití systému pro rozpoznávání obličejů (facial recognition)

Úvod

V návaznosti na probíhající debatu týkající se využití systému pro rozpoznávání obličejů (dále jen „facial recognition“) ve veřejném prostoru a oprávněnosti provozování takových systémů, považuje Spolek pro ochranu osobních údajů (dále jen „Spolek“) za vhodné zaujmout stanovisko k právnímu režimu provozování kamerových systémů s funkcí facial recognition ve veřejném prostoru a přístupu k takto získaným osobním údajům včetně jejich uchovávání.

Tento poziční dokument se zabývá vybranými právními aspekty provozování kamer, resp. kamerových systémů, které samy o sobě představují zásah do soukromí a dále užívání systému facial recognition veřejnými subjekty ve veřejném prostoru. Předmětem stanoviska Spolku je právní analýza situací, kdy je provoz kamerového systému považován za zpracování osobních údajů (tj. zaznamenává automaticky vybraný veřejný prostor; a účelem pořízení tohoto záznamu je využití k identifikaci fyzických osob v souvislosti s určitým jednáním[2]) a jako takový podléhá obecným pravidlům pro zpracování osobních údajů.

Stávající právní úprava

Obecné požadavky na provozování kamerového systému, který je zpracováním osobních údajů

Při posuzování zákonnosti provozování kamerového systému je nezbytné určit, kdo je provozovatelem kamerového systému (může jím být správce systému i jiný subjekt), na základě jakého zákonného důvodu a za jakým konkrétním účelem osobní údaje zpracovává. Každý provozovatel kamerového systému je dále povinen dodržovat obecné zásady zpracování osobních údajů. Kamery tedy nesmí zejména nadměrně zasahovat do soukromí subjektů údajů, mohou být užívány pouze ke stanovenému účelu, kterého zároveň nelze dosáhnout jinak[3], záznamy mohou být uchovávány pouze po dobu nezbytnou k dosažení účelu a subjekt údajů musí být o existenci takového kamerového systému řádně informován. Pro dosažení co nejvyšší úrovně transparentnosti[4] vypracovává provozovatel kamerového systému pravidla zpracování osobních údajů, v souladu s nimiž jedná, a které nadto stanoví způsob nakládání s osobními údaji.

Pokud hovoříme o veřejných subjektech, kteří jsou provozovateli kamerových systémů (např. ve smyslu Policie ČR, obecní policie, města, příspěvkové organizace apod.) připadají vedle výslovného zákonného zmocnění v úvahu zejména tyto důvody zpracování osobních údajů: čl. 6 odst. 1 písm. c) GDPR (plnění

[1] Tento poziční dokument představuje názor příslušné komise Spolku na danou problematiku a není závazným výkladem zákona. Může obsahovat názory a doporučení (*vč. doporučení de lege ferenda*), která nemusí být akceptována příslušnými orgány veřejné správy.
[2] srov. https://www.uoou.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535
[3] Myšleno ve smyslu využití např. méně invazivních technik zásahu do soukromí subjektů údajů.
[4] Současně je vhodné při zpracování informačního memoranda poskytnout subjektům údajů konkrétní informace o zpracování osobních údajů i jinými způsoby při dodržení dostatečné granularity (např. obecná informace na „tabulce/baneru“ vs konkrétní informační memorandum).

Spolek pro ochranu osobních údajů se sídlem Hellichova 458/1, Malá Strana, 118 00 Praha 1, zapsaný ve veřejném rejstříku u Městského soudu v Praze, sp.zn. L 61299, IČO: 03493679

právní povinnosti) a čl. 6 odst. 1 písm. e) GDPR (plnění úkolu prováděného ve veřejném zájmu), resp. pro účely směrnice 2016/680 pak čl. 8 odst. 1 (splnění úkolu prováděného příslušným orgánem pro účely stanovené v čl. 1 odst. 1 této směrnice a v rozsahu nezbytném pro tyto účely a pokud má základ v právu EU nebo členského státu).

Oprávnění Policie České republiky a obecní policie provozovat kamerové systémy je dáno přímo zákonem. Podle § 62 zákona č. 273/2008 Sb., o Policii České republiky (dále jen „zákon o Policii ČR“) a § 24b zákona České národní rady č. 553/1991 Sb., o obecní policii (dále jen „zákon o obecní policii“) je policie oprávněna v nezbytných případech pořizovat zvukové, obrazové nebo jiné záznamy z míst veřejně přístupných (za současného splnění povinnosti tuto skutečnost uveřejnit, resp. informovat o zřízení takových systémů).[5,6] Policie ČR je dále výslovně oprávněna zpracovávat osobní údaje, pokud je to nezbytné k plnění jejích úkolů, zejm. ochrana bezpečnosti osob, majetku a veřejného pořádku, předcházení trestné činnosti (§ 79 odst. 2 zákona o Policii ČR). Podle § 24a zákona o obecní policii obecní policie zpracovává osobní údaje, které potřebuje k plnění úkolů stanovených tímto nebo jiným zvláštním zákonem.

Kamerový systém v Praze

Na podzim roku 2019 otevřel Magistrát hl. m. Prahy diskuzi nad legálností a potřebností provozování kamerového systému s facial recognition ve veřejném prostoru na vybraných místech Prahy, když požádal ÚOOÚ o stanovisko k zákonnosti takového jednání.[7] Dle dostupných informací však ke zprovoznění takového systému prozatím nedošlo.

V současné době je na území hl. m. Prahy provozován tzv. Městský kamerový systém (dále jen „MKS“), jehož zřizovatelem a provozovatelem je Odbor bezpečnosti a krizového řízení MHMP. Cílem MKS je působit preventivně i represivně při zajištění bezpečnosti osob, veřejného pořádku, ochrany zdraví a majetku.[8]

MKS integruje vybrané kamery různých organizací a provozovatelů[9], kteří mají dále jako klienti MKS upravená přístupová práva k monitorování prostřednictvím kamer. Z Usnesení Zastupitelstva hlavního města Prahy (číslo 20/51) ze dne 20. 10. 2016 k návrhu Koncepce rozvoje a zajištění provozu Městského kamerového systému hl. m. Prahy na období 10 let[10] (dále jen „Koncepce MKS“) vyplývá, že k pořizování záznamů z MKS a uchování, popř. exportu dat je oprávněna pouze Policie ČR a Městská policie Praha (na

---

[5] Zákon č. 273/2008 Sb., o Policii České republiky, § 62 *(1) Policie může, je-li to nezbytné pro plnění jejích úkolů, pořizovat zvukové, obrazové nebo jiné záznamy osob a věcí nacházejících se na místech veřejně přístupných a zvukové, obrazové nebo jiné záznamy o průběhu úkonu. (2) Jsou-li k pořizování záznamů podle odstavce 1 zřízeny stálé automatické technické systémy, policie informace o zřízení takových systémů vhodným způsobem uveřejní.*

[6] Zákon České národní rady č. 553/1991 Sb., o obecní policii, § 24b *(1) Obecní policie je oprávněna, je-li to potřebné pro plnění jejích úkolů podle tohoto nebo jiného zákona, pořizovat zvukové, obrazové nebo jiné záznamy z míst veřejně přístupných, popřípadě též zvukové, obrazové nebo jiné záznamy o průběhu zákroku nebo úkonu. (2) Jsou-li k pořizování záznamů podle odstavce 1 zřízeny stálé automatické technické systémy, je obecní policie povinna informace o zřízení takových systémů vhodným způsobem uveřejnit.*

[7] Krajské ředitelství policie hl. m. Prahy požádalo v listopadu 2019 Magistrát hl. m. Prahy o zprovoznění systému facial recognition na šesti místech v Praze. Magistrát hl. m. Prahy se rozhodl podat žádost k ÚOOÚ o jejich stanovisko k oprávněnosti takového kroku. Výše uvedené informace jsou dostupné z médií, např. https://domaci.ihned.cz/c1-66680630-prazska-policie-chce-vyzkouset-automaticke-rozpoznavani-obliceju-vyvolava-to-ale-strach-ze-zneuziti
https://www.lidovky.cz/domov/policie-nespousti-kamerove-poznavani-obliceje-v-praze-ujistuje-ministr-hamacek.A191121_134122_ln_domov_ele
https://region.rozhlas.cz/policie-chce-v-praze-testovat-sledovani-obliceju-neni-duvod-jen-chteji-hracku-8112396

[8] Některé podrobnosti např. zde: https://bezpecnost.praha.eu/clanky/kamerovy-system.

[9] Dopravní podnik HMP – kamery instalované v metru; Technická správa komunikací – dopravní přehledové kamery, úseková měření rychlosti, detekční kamery; Odbor bezpečnosti a krizového řízení HMP (dříve OKR – přehledové kamery na celém území HMP; Městské části – ochrana objektů majetku městské části; Správa služeb HMP.

[10] Dostupné zde:
http://zastupitelstvo.praha.eu/ina/tedusndetail.aspx?par=15719525400600121820819501600600121820519501300600121820619501000600121820 6&id=287332

základě zákonného zmocnění výše), zatímco další subjekty[11], které mají přístup k MKS, nedisponují oprávněním záznamy pořizovat ani je jinak užívat. Na dotaz směřovaný na Magistrát hl. m. Prahy bylo uvedeno, že záznamy z kamer jsou uchovávány po dobu 30 dnů na operativních úložištích[12].

Z veřejně dostupných zdrojů není zcela zjevná struktura provozování kamer, které jsou součástí MKS, jelikož se jako o provozovateli, zároveň také hovoří o odboru Magistrátu hl. m. Prahy i jednotlivých zřizovatelích kamer. Například Technická správa komunikací hl. m. Prahy však uvedla, že provozovatelem kamer MKS není (stejně jako Policie ČR) a pouze je spravuje. Podle Informace o zpracování osobních údajů Magistrátu hl. m. Prahy[13] je jediným odborem, který zpracovává osobní údaje z provozu kamerových systémů - odbor bezpečnosti. Deklarovaným účelem je „*dohled nad fungováním interního kamerového systému MHMP*" a dále jsou „*kamerové záznamy uchovávány pro případ dokumentace bezpečnostních incidentů*". Tyto záznamy jsou uchovávány s jasně rozlišitelnými obličeji.[14]

Systém facial recognition

Technologie rozpoznávání obličejů (tedy *facial recognition*) je systém automatického zpracování digitálního obrazu obsahujícího obličeje subjektů údajů, které je tento systém schopen obvykle identifikovat nebo verifikovat[15] v reálném čase.

Použitím technologie facial recognition obvykle dochází ke zpracování zvláštní kategorie osobních údajů, tj. biometrických údajů. Pokud je cílem zpracování těchto údajů jedinečná identifikace fyzických osob, což lze při užití této technologie ve veřejném prostoru bezpečnostními složkami státu přepokládat (deklarovaný cílem je zpravidla odhalení hledaných osob, snížení a odhalování kriminality atd.), podléhá pak takové zpracování osobních údajů režimu čl. 9 GDPR, resp. čl. 10 směrnice 2016/680. Zpracování biometrických údajů z kamerových systémů s funkcí facial recognition použitých ve veřejném prostoru by tedy v režimu GDPR mělo být možné pouze, pokud je naplněna některá z výjimek podle čl. 9 odst. 2 GDPR. Vzhledem k restriktivnímu výčtu těchto výjimek připadá v úvahu jen možnost zpracování těchto zvláštních kategorií osobních údajů na základě výjimky dle čl. 9 odst. 2 písm. g) GDPR, podle které je zpracování nezbytné „*z důvodu významného veřejného zájmu vyplývajícího z českého nebo unijního práva*". V režimu směrnice 2016/680 se pak jedná o právní základ podle čl. 10 písm. a) této směrnice.

Obdobně věc posuzuje Evropský sbor pro ochranu osobních údajů ve svých Pokynech ke zpracování osobních údajů prostřednictvím videotechniky.[16] Ten dovozuje, že v případech, kdy je facial recognition používán ve veřejných prostorech a kdy dochází k zachycení obličeje jakéhokoliv kolemjdoucího, je nezbytná existence výjimky podle čl. 9 odst. 2 GDPR pro zpracování biometrických údajů všech zachycených subjektů údajů. Rozhodující není, že jde o vyhledání konkrétních osob např. porovnáním záznamů s již existujícími šablonami.[17]

Vedle kategorizace biometrických údajů jako zvláštní kategorie osobních údajů a s tím souvisejících omezeních, neposkytuje česká právní úprava zvláštní ustanovení o užívání biometrických údajů.

---

[11] např. Dopravní podnik hl. m. Prahy, Technická správa komunikací hl. m. Prahy, Zdravotnická záchranná služba hl. m. Praha, Hasičský záchranný sbor hl. m. Prahy, Správa služeb hl. m Prahy

[12] Operativní úložiště integrují na jednom místě data z různých zdrojů, čímž umožňují a usnadňují jejich další využití a zpracování. Tato úložiště zpravidla slouží ke krátkodobému uchování aktuálních dat.

[13] Informace o zpracování osobních údajů, Magistrát hlavního města Praha, Dostupné zde: http://www.praha.eu/jnp/cz/o_meste/magistrat/gdpr/index.html

[14] Informace o zpracování osobních údajů, Magistrát hlavního města Praha, BEZ (Odbor bezpečnosti), Dostupné zde: http://www.praha.eu/file/2688824/Informacni_povinnost_BEZ.pdf

[15] Oproti běžnému kamerovému systému je tento systém přesnější a současně efektivnější při prošetřování trestné činnosti.

[16] European Data Protection Board. Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky, verze 2.0, 29. 1. 2020, Dostupné zde: https://edpb.europa.eu/our-work-tools/our-documents/pokyny/guidelines-32019-processing-personal-data-through-video-devices_cs

[17] tamtéž, zejm. bod 84

S ohledem na skutečnost, že jejich zpracování technologií facial recognition představuje významný zásah do soukromí osob se domníváme, že není přípustné tyto technologie ve veřejném prostoru užívat trvale ani preventivně.

Domníváme se, že z pohledu zásahu do soukromí je užití facial recognition srovnatelné například s odposlouchávání osob (pokud odhlédneme od rizik vyplývajících z chybovosti způsobené samotnou technologií[18]). Tento operativně pátrací prostředek ke sledování osob lze použít pouze za podmínek striktně vymezených zákonem (zákon č. 141/1961 Sb., trestní řád (dále jen „trestní řád")) se souhlasem státního zástupce nebo soudu. Analogicky by i používání facial recognition, s výjimkou situací, kdy bude existovat výslovný souhlas subjektu údajů (splňující veškeré náležitosti souhlasu, především pak jeho svobodného a dobrovolného udělení), mělo být přípustné pouze za splnění zákonných podmínek, a to vždy v souvislosti s konkrétním trestním řízením nebo na konkrétně vymezených místech s jasně deklarovaným a řádně odůvodněným účelem (zejména tedy místa vyžadující vysokou míru zabezpečení, jako jsou např. letiště nebo kritická datová centra) a za splněním podmínek zpracování osobních údajů.

Operativně pátracím prostředkem sledování osob ve smyslu § 158d odst. 1 trestního řádu se *rozumí získávání poznatků o osobách a věcech prováděné utajovaným[19] způsobem technickými nebo jinými prostředky*. Podle trestního řádu je možné operativně pátrací prostředky použít pouze v řízení vedeném o úmyslném trestném činu (§ 158b odst. 1 trestního řádu).

Pokud bychom na facial recognition nahlíželi jako na operativně pátrací prostředek, šlo by, vzhledem k tomu, že při používání kamer se systémem facial recognition jsou pořizovány zvukové, obrazové nebo jiné záznamy, o tzv. druhý typ sledování osob, k jehož užití je potřeba písemného povolení státního zástupce (§ 158d odst. 2 trestního řádu). Každé sledování osob, při kterém jsou pořizovány záznamy, je totiž možné uskutečnit pouze na základě písemného povolení státního zástupce (bez něj lze pořizovat záznamy, pouze s výslovným souhlasem osoby, do jejíž práv a svobod má být sledováním zasahováno, což je v případě kamerových systémů ve veřejném prostoru nemožné; nebo pokud věc nesnese odkladu, tehdy je však nutné souhlas státního zástupce dodatečně získat). Státní zástupce je oprávněn takové sledování povolit na zákonem omezenou dobu, a to pouze v případě, že obdrží odůvodněnou písemnou žádost, která se týká podezření na konkrétní trestnou činnost (§ 158d odst. 2 trestního řádu).

Prakticky by využití technologie facial recognition mohlo fungovat do jisté míry obdobně jako například odposlechy mobilních telefonů. Každý operátor je připraven tyto odposlechy umožnit, avšak orgány policie je mohou využít a poskytovatelé telekomunikačních služeb mají povinnost je zpřístupnit pouze v omezených případech na základě povolení státního zástupce/soudu v konkrétní věci. Stejně tak by měl být připraven systém facial recognition, jehož užití ve veřejném prostoru by podléhalo omezení trestního řádu.

Pokud se vrátíme k důvodu zpracování zvláštní kategorie osobních údajů podle čl. 9 GDPR (resp. čl. 10 směrnice 2016/680) je zřejmé, že zpracování biometrických údajů za účelem identifikace technologií

[18] Plošné zpracování zvláštní kategorie osobních údajů technologií facial recognition totiž nepřináší riziko jenom z pohledu identifikace osob a možnosti jejich sledování (tj. zásadu do soukromí), ale nedokonalost facial recognition technologií přináší zároveň nezanedbatelné riziko v podobě záměny osob způsobené nepřesností v procesu identifikace. Tyto nepřesnosti nadto postihují více některé skupiny osob než jiné. Z technického hlediska však bude do budoucna velmi obtížné zajistit i plnou validitu výstupů z plně „automatizovaných" kamerových systémů, které budou dle nastavených kritérií a parametrů schopny vyhodnocovat i další typy údajů.

[19] *„Utajeným způsobem se míní především utajení ve vztahu k osobám, které jsou sledovány nebo které nakládají se sledovanou věcí…"* (Šámal a kol., Trestní řád I, II, III, 7. vydání, 2013, s. 2001 – 2011) Domníváme se, že podmínka utajovanosti je u nasazení systému facial recognition splněna. Ačkoli lidé mohou být obeznámeni s existencí a možností využití systému facial recognition v daném městě, popř. na daném místě nedisponují informací o tom, zda je v danou chvíli někdo sleduje nebo ne. Nabízí se paralela s odposlechy telefonů, o kterých jsou lidé také obecně obeznámeni a utajovaná je pouze skutečnost, zda je konkrétní osoba v daném čase odposlouchávána.

facial recognition je v případě užití v rozsahu umožněném trestním řádem odůvodněné, neboť významný veřejný zájem je v případě probíhajícího trestního řízení a získání příslušného souhlasu, dán.

Zprovoznění systému facial recognition v Praze

Na základě shora uvedeného uzavíráme, že zprovoznění systému facial recognition v rámci MKS v Praze není otázkou názoru či volby Magistrátu hl. m. Prahy (což policie svou žádostí směřovanou Magistrátu hl. m. Prahy indikuje) nebo snad ÚOOÚ, ale vždy by mělo být umožněno pouze na základě zákona v kombinaci s konkrétním povolením uděleným příslušným orgánem, kterým je v případě využití pro účely trestního řízení státní zástupce. Zprovoznění tohoto systému/zpřístupnění údajů jím zaznamenaných také není možné žádat bez omezení, ale vždy pouze na základě a v rozsahu stanoveným trestním řádem, tj. v souvislosti s konkrétním trestním řízení vedeným pro úmyslný trestný čin na základě písemného povolení státního zástupce v územně i časově omezeném rozsahu.

Skutečnost, že oprávněnost využití technologie facial recognition nevychází z uvážení Magistrátu hl. m. Prahy potvrdil i ÚOOÚ ve svém vyjádření ze dne 3. 12. 2019 k žádosti o konzultaci ze strany Magistrátu hl. m. Prahy.[20] ÚOOÚ v tomto vyjádření nepřistoupil k posouzení zákonnosti zprovoznění facial recognition v rámci MKS, ale navrhl vhodný postup k takovému posouzení (zejm. projednání s pověřenci, vyhotovení posouzení vlivu na ochranu osobních údajů Policií ČR, která je spravujícím orgánem a projednání postupu s ÚOOÚ). ÚOOÚ však jednoznačně uzavírá, že využití systému facial recognition může představovat vysoké riziko[21] zásahu do práv a svobod subjektů údajů.

Úvahy de lege ferenda

I pokud bychom přistoupili na premisu, že využívání facial recognition systémů by mělo podléhat režimu trestního řádu pro nasazení operativně pátracích prostředků, domníváme se, že pro vyloučení veškerých pochybností by bylo vhodné přijmout speciální právní úpravu zamezující zneužití těchto systémů. Tato by měla být zakotvena na úrovni zákona a srozumitelně a proporčně upravovat, jak uchovávání dat z facial recognition systémů, tak jejich zpřístupnění či pořizování kopií ze záznamů.

Při pohledu na možnou budoucí úpravu užívání technologie facial recognition se nabízí odkázat na speciální úpravu pro získávání (resp. uchovávání) a užívání provozních a lokalizačních údajů z veřejných komunikačních sítí. Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) ukládá povinnost uchovávat provozní a lokalizační údaje, jejichž zpřístupnění je možné pouze na základě odůvodněného příkazu soudu vydaného na návrh státního zástupce (§ 88a trestního řádu) v rámci trestního řízení pro vymezené trestné činy. Doba ukládání dat získaných ze systémů facial recognition by měla být vždy důsledně vážena, neboť je zřejmé, že čím déle budou taková data ukládána, tím se případně zvyšuje riziko jejich zneužití či zpracování pro další (odlišný) účel.

Zahraniční přístup

Britský komisař (Information Commisioner´s Office) vydal 31. října 2019 stanovisko[22] k užívání technologií facial recognition při vymáhání práva orgány státu. Komisař v tomto stanovisku zejména

[20] Vyjádření k žádosti o konzultaci k městskému kamerovému systému hl. m. Prahy, čj. UOOU-04829/19-2, ze dne 3. 12. 2019. Dostupné zde: https://www.irozhlas.cz/sites/default/files/uploader_unmanaged/uoou_kamery_odp_191219-111704_cib.pdf

[21] Tento fakt by měl být ověřen a případně posouzen skrze vypracování Analýzy vlivu na ochranu osobních údajů, resp. DPIA, či minimálně testu proporcionality, kde by měla být zhodnocena faktická potřebnost existence takovéhoto systému naproti dalším typům možných bezpečnostních opatření.

[22] Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places, 31. října 2019, Reference: 2019/01, Dostupné zde: https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

apeluje na zajištění co nejvyšší úrovně transparentnosti a proporcionality při užívání facial recognition. Státní donucovací orgány by měly jednat natolik transparentně, aby přímo zasažení jednotlivci disponovali dostatkem informací, jak konkrétně orgány postupují při užívání technologie facial recognition a bylo tak dosaženo co nejvyšší právní jistoty. Přitom předvídatelnost zpracování biometrických dat je klíčovým parametrem pro samotné posouzení jejich oprávněného využívání. Komisař dále uvádí, že další kroky by měly směřovat ke kodifikaci zákonných standardů užití technologie facial recognition a ideálně i dalších způsobů zpracování biometrických údajů vládou. Komisař apeluje na přijetí závazného Code of Practice, který jasně stanoví, kdy a za jakých podmínek mohou donucovací orgány facial recognition používat.

I Evropská komise zastává stanovisko obezřetného přístupu k zavedení technologie facial recognition ve veřejném prostoru. Ve White Paper On Artificial Intelligence[23] říká, že takové zpracování osobních údajů, nejenže musí být v souladu s GDPR a Listinou základních práv Evropské unie, ale může být zákonné, pouze pokud je ospravedlnitelné, proporční a poskytuje dostatečné záruky.

Otázkou využitelnosti umělé inteligence včetně technologie facial recognition v oblastech civilního a vojenského využití a státní správy se ve svém Usnesení[24] z ledna 2021 zabýval také Evropský parlament. Podle něj by využití systému facial recognition mělo podléhat technickým normám, které zajistí jejich nezaujatou a nediskriminační povahu. Současně poukazuje na nutnost zajištění záruk proti zneužití těchto technologií a jejich využívání v souladu s principem přiměřenosti a nezbytnosti.

V srpnu 2020 vydal britský odvolací soud rozhodnutí[25], ve kterém shledal použití systému facial recognition policií ve veřejném prostoru nezákonným. Soud uzavřel, že nasazení automatického facial recognition v jižním Walesu je mimo jiné v rozporu s právem na ochranu osobních údajů ve smyslu čl. 8 odst. 2 Listiny základních práv Evropské unie. Odvolací soud dále judikoval, že policie by neměla bez ověření používat systém, u kterého existují pochybnosti o jeho neutralitě (pozn. ukazuje se, že přesnost technologie je nejvyšší u bílých mužů; u jiných genderů a ras se přesnost rozpoznávání významně snižuje[26]). Méně příznivý dopad na některé skupiny obyvatel by mohl být proto považován za diskriminační.

Lze konstatovat, že právě domácí vlády (na základě debaty s ostatními státy EU) by měly hrát hlavní roli při nastavení regulace užívání facial recognition. Tento aspekt akcentují dokonce i některé technologické společnosti, které technologii facial recognition vyvíjí.[27] Základem by měla být odborná diskuze s důrazem na dosažení proporčních, transparentních a nediskriminujících pravidel.

Závěr

Ačkoli je zřejmé, že umožnění facial recognition (tj. dodání a implementace technického zařízení umožňujícího využití technologie facial recognition) bude probíhat plošně, je nezbytné, aby navazující krok, tj. samotné využití této technologie ve veřejném prostoru představující zpracování zvláštní

[23] European Comission, White Paper On Artificial Intelligence - A European approach to excellence and trust, COM (2020) 65 final, 19.2.2020, s. 21-22

[24] Usnesení Evropského parlamentu ze dne 20. ledna 2021 na téma „Umělá inteligence: otázky výkladu a uplatňování mezinárodního práva v míře, v níž se to týká EU, v oblastech civilního a vojenského využití a státní správy mimo oblast trestního práva“, Dostupné zde: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_CS.html

[25] The Court Of Appeal of England and Wales, sp. zn. C1/2019/2670, ze dne 11. 8. 2020, Dostupné zde: https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html

[26] Tzv. „technology bias“. Algoritmické zkreslení popisuje systematické a opakovatelné chyby v počítačovém systému, které vytvářejí nespravedlivé výsledky, například privilegování jedné libovolné skupiny uživatelů před ostatními. Algoritmické zkreslení se vyskytuje napříč platformami, mimo jiné včetně výsledků vyhledávacích strojů a platforem sociálních médií, a může mít dopady od neúmyslného narušení soukromí až po posílení sociálních předsudků ohledně rasy, pohlaví, sexuality a etnického původu.

[27] srov. https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

kategorie osobních údajů podléhalo předem stanoveným striktním podmínkám a nezasahovalo nepřiměřeně do práv subjektů údajů.

Každé využití facial recognition by mělo být co do nejvyšší možné míry transparentní. Dotčené subjekty údajů by měly mít možnost jednoduše zjistit, kde je tato technologie umožněna, jaké osobní údaje jsou při jejím využití zpracovávány, jak dlouho a v neposlední řadě, kdo všechno k nim má přístup. Využití facial recognition bez dodržení těchto podmínek by mělo být oprávněné pouze v situacích stanovených výslovně zákonem.

Využití údajů ze strany orgánů činných v trestním řízení by mělo podléhat souhlasu státního zástupce (popř. soudu), který bude vydán na základě žádosti odůvodněné konkrétním případem. Takový souhlas by opravňoval orgány po stanovenou dobu ve stanoveném rozsahu systém facial recognition užívat.

Nikdy by tedy využití technologie facial recognition nemělo být svévolné, čistě preventivní (byť pod argumentem potenciální hrozby trestné činnosti), tajné ani plošné.

Mezi každým zásahem do základních práv a svobod a dosaženým cílem musí být vztah proporcionality. Domníváme se, že Česká republika jakožto jedna z nejbezpečnějších zemí světa[28] by neměla být jednou z prvních zemí Evropy, která sledování veřejného prostoru s využitím technologie facial recognition zavede. Vzhledem ke skutečnosti, že kriminalita v České republice obecně klesá[29], by byl takovýto postup ve zřejmém v rozporu se zásadou proporcionality.

Autoři: Mgr. Jana Pattynová, LL.M., JUDr. Klára Kocarová, Mgr. Dominik Vítek, Mgr. Vojtěch Rusz, JUDr. Vladan Rámiš, PhD.

Datum: únor 2021

[28] srov. https://www.idnes.cz/zpravy/zahranicni/bezpecnost-mir-svet-cesko-index.A190612_133201_zahranicni_remy
https://zahranicni.ihned.cz/c1-66588780-cesko-je-desatou-nejmirumilovnejsi-zemi-sveta-na-prvnich-mistech-je-island-novy-zeland-a-portugalsko

[29] srov. https://www.mapakriminality.cz/#tabulky
https://www.ceska-justice.cz/2018/02/kriminalita-klesla-za-dvacet-let-temer-polovinu-objasnenost-trestnych-cinu-opet-stoupa/