Pokyny 05/2022 k používání technologie rozpoznávání obličeje v oblasti prosazování práva

Verze 2.0

Přijato dne 26. dubna 2023

Historie verzí

Verze 1.0	12. května 2022	Přijetí pokynů k veřejné konzultaci
Verze 2.0	26. dubna 2023	Přijetí pokynů po veřejné konzultaci

Obsah

SHRNUTÍ

Stále více donucovacích orgánů používá nebo hodlá používat technologii rozpoznávání obličeje. Lze ji použít k **autentizaci** nebo k **identifikaci** osoby a lze ji uplatnit na videozáznamy (např. v uzavřeném televizním okruhu, CCTV) nebo fotografie. Nachází využití k různým účelům, včetně vyhledávání osob v policejních seznamech zájmových osob nebo sledování pohybu dané osoby ve veřejném prostoru.

Technologie rozpoznávání obličeje je založena na zpracování **biometrických údajů**, a proto zahrnuje zpracování zvláštních kategorií osobních údajů. Technologie rozpoznávání obličeje často využívá prvky založené na **umělé inteligenci** (UI) nebo strojovém učení. To sice umožňuje zpracování osobních údajů ve velkém měřítku, ale zároveň přináší riziko diskriminace a falešných výsledků. Technologii rozpoznávání obličeje lze použít v kontrolovaných situacích 1 : 1, ale také v případě velkých davů a důležitých dopravních uzlů.

Technologie rozpoznávání obličeje je **pro donucovací orgány citlivý nástroj.** Donucovací orgány jsou výkonnými orgány a mají svrchované pravomoci. Technologie rozpoznávání obličeje může zasahovat do základních práv, a to i nad rámec práva na ochranu osobních údajů, a může ovlivnit naši sociální a demokratickou politickou stabilitu.

Z hlediska ochrany osobních údajů v kontextu prosazování práva musí být splněny **požadavky směrnice o prosazování práva**. Určitý rámec týkající se používání technologie rozpoznávání obličeje je stanoven ve směrnici o prosazování práva, zejména v čl. 3 bodu 13 této směrnice (pojem „biometrické údaje“), článku 4 (zásady zpracování osobních údajů), článku 8 (zákonnost zpracování), článku 10 (zpracování zvláštních kategorií osobních údajů) a článku 11 směrnice (automatizované individuální rozhodování).

Uplatňováním technologie rozpoznávání obličeje může být dotčeno i několik dalších základních práv. **Listina základních práv EU** (dále jen „Listina“) má tudíž zásadní význam pro výklad směrnice o prosazování práva, zejména právo na ochranu osobních údajů uvedené v článku 8 Listiny, ale také právo na soukromí stanovené v článku 7 Listiny.

Legislativní opatření, která slouží jako právní základ pro zpracování osobních údajů, přímo zasahují do práv zaručených články 7 a 8 Listiny. Zpracování biometrických údajů za všech okolností představuje závažný zásah samo o sobě. Tento zásah nezávisí na výsledku, např. na nalezení shody. Každé omezení výkonu základních práv a svobod musí být stanoveno zákonem a respektovat podstatu těchto práv a svobod.

Právní základ musí být **dostatečně jasný**, aby občané měli přiměřenou představu o podmínkách a okolnostech, za nichž jsou orgány oprávněny uchýlit se k jakýmkoli opatřením v oblasti shromažďování údajů a tajného sledování. Pouhé provedení obecného ustanovení v článku 10 směrnice o prosazování práva do vnitrostátního práva by postrádalo přesnost a předvídatelnost.

Předtím, než vnitrostátní zákonodárce vytvoří nový právní základ pro jakoukoli formu zpracování biometrických údajů získaných na základě rozpoznávání obličeje, měl by být **konzultován** příslušný dozorový úřad pro ochranu osobních údajů.

Legislativní opatření musí být **vhodná** pro dosažení legitimních cílů sledovaných danou právní úpravou. **Cíl obecného zájmu** – jakkoli zásadní – sám o sobě neodůvodňuje omezení základního práva. Legislativní opatření by měla **rozlišovat** a zaměřovat se na osoby, na které se vztahuje s ohledem na cíl, např. boj proti konkrétní závažné trestné činnosti. Pokud se opatření vztahuje obecně na všechny osoby bez takového rozlišení, omezení nebo výjimky, zásah je o to větší. Míra zásahu je větší i tehdy, pokud se zpracování osobních údajů týká významné části obyvatelstva.

Údaje musí být zpracovány způsobem, který zajišťuje použitelnost a účinnost pravidel a zásad EU pro ochranu osobních údajů. Na základě okolností každé jednotlivé situace musí být v rámci **posouzení nezbytnosti a přiměřenosti** rovněž identifikovány a zváženy všechny možné důsledky pro ostatní základní práva. Pokud jsou údaje systematicky zpracovávány bez vědomí subjektů údajů, je pravděpodobné, že to vyvolá **obecný pocit neustálého sledování**. To může mít neblahé dopady na některá nebo všechna dotčená základní práva, jako je lidská důstojnost podle článku 1 Listiny, svoboda myšlení, svědomí a náboženského vyznání podle článku 10 Listiny, svoboda projevu podle článku 11 Listiny a svoboda shromažďování a sdružování podle článku 12 Listiny.

Zpracování zvláštních kategorií údajů, jako jsou biometrické údaje, lze považovat za „**zcela nezbytné**" (článek 10 směrnice o prosazování práva) pouze tehdy, pokud se zásah do ochrany osobních údajů a omezení této ochrany omezí na to, co je naprosto nezbytné, tj. nevyhnutelné, a vyloučí se jakékoli zpracování obecné nebo systematické povahy.

Skutečnost, že fotografie byla subjektem údajů **zjevně zveřejněna** (článek 10 směrnice o prosazování práva), neznamená, že související biometrické údaje, které lze z fotografie získat pomocí zvláštních technických prostředků, mohou být považovány za zjevně zveřejněné. Výchozí nastavení služby, např. zpřístupnění šablon veřejnosti, nebo absence možnosti volby, např. šablony jsou zveřejněny, aniž by uživatel mohl toto nastavení změnit, by v žádném případě nemělo být chápáno jako zjevné zveřejnění.

Článek 11 směrnice o prosazování práva stanoví rámec pro **automatizované individuální rozhodování**. Používání technologie rozpoznávání obličeje zahrnuje používání zvláštních kategorií údajů a může vést k profilování, a to v závislosti na způsobu a účelu použití této technologie. V souladu s právem Unie a čl. 11 odst. 3 směrnice o prosazování práva je v každém případě zakázáno profilování, které vede k diskriminaci fyzických osob na základě zvláštních kategorií osobních údajů.

Článek 6 směrnice o prosazování práva se týká nutnosti **rozlišovat mezi různými kategoriemi subjektů údajů**. Pokud jde o subjekty údajů, u nichž neexistuje žádný důkaz naznačující, že by jejich jednání mohlo mít souvislost, byť nepřímou nebo vzdálenou, s legitimním cílem podle směrnice o prosazování práva, neexistuje s největší pravděpodobností žádné odůvodnění zásahu.

Zásada minimalizace údajů (čl. 4 odst. 1 písm. e) směrnice o prosazování práva) rovněž vyžaduje, aby byl veškerý videomateriál, který není relevantní pro účel zpracování, před použitím vždy odstraněn nebo anonymizován (např. rozmazáním bez možnosti zpětného získání údajů).

Správce musí pečlivě zvážit, jak (nebo zda může) splnit požadavky týkající se **práv subjektu údajů** před zahájením jakéhokoli zpracování s využitím technologie rozpoznávání obličeje, jelikož tato technologie často zahrnuje zpracování zvláštních kategorií osobních údajů bez zjevné interakce se subjektem údajů.

Účinný výkon práv subjektu údajů závisí na tom, zda správce plní své **informační povinnosti** (článek 13 směrnice o prosazování práva). Při posuzování toho, zda nastal „zvláštní případ" podle čl. 13 odst. 2 směrnice o prosazování práva, je třeba vzít v úvahu několik faktorů, včetně toho, zda jsou osobní údaje shromažďovány bez vědomí subjektu údajů, neboť to by byl jediný způsob, jak umožnit subjektům údajů účinně vykonávat svá práva. Pokud se rozhodování provádí výhradně na základě technologie rozpoznávání obličeje, je třeba subjekty údajů informovat o prvcích automatizovaného rozhodování.

Pokud jde o **žádosti o přístup** v případě, kdy jsou biometrické údaje uloženy a spojeny s totožností také pomocí alfanumerických údajů, pak v souladu se zásadou minimalizace údajů, by příslušný orgán měl mít možnost potvrdit žádost o přístup na základě vyhledávání podle těchto alfanumerických údajů a bez zahájení dalšího zpracování biometrických údajů jiných osob (tj. vyhledávání pomocí technologie rozpoznávání obličeje v databázi).

Rizika pro subjekty údajů jsou obzvláště závažná, pokud jsou v policejní databázi uloženy a/nebo sdíleny s jinými subjekty nepřesné údaje. Správce musí v souladu s tím **provést opravu** uložených údajů a systémů založených na technologii rozpoznávání obličeje (viz také 47. bod odůvodnění směrnice o prosazování práva).

Právo na **omezení** je obzvláště důležité, pokud jde o technologii rozpoznávání obličeje (založenou na algoritmu (algoritmech), a tedy nikdy nevykazující konečný výsledek) v situacích, kdy se shromažďuje velké množství údajů a přesnost a kvalita identifikace se může lišit.

Povinným požadavkem před použitím technologie rozpoznávání obličeje je provedení **posouzení vlivu na ochranu osobních údajů**, srov. článek 27 směrnice o prosazování práva. EDPB doporučuje zveřejnit výsledky těchto posouzení nebo alespoň hlavní zjištění a závěry posouzení vlivu na ochranu osobních údajů jako opatření, které má posílit důvěru a transparentnost.

Většina případů zavádění a používání technologie rozpoznávání obličeje obsahuje inherentní vysoké riziko pro práva a svobody subjektů údajů. Proto by měl orgán, který technologii rozpoznávání obličeje zavádí, před zavedením systému **konzultovat** s příslušným dozorovým úřadem.

Vzhledem k jedinečné povaze biometrických údajů by měl orgán, který zavádí a/nebo používá technologii rozpoznávání obličeje, věnovat zvláštní pozornost **zabezpečení zpracování** v souladu s článkem 29 směrnice o prosazování práva. Donucovací orgán by měl zejména zajistit, aby systém odpovídal příslušným normám, a zavést opatření na ochranu biometrických šablon. Zásady a záruky ochrany osobních údajů musí být v technologii zakotveny před zahájením jejich zpracování. Proto i v případě, že donucovací orgán hodlá uplatňovat a využívat technologii rozpoznávání obličeje od externích poskytovatelů, musí například prostřednictvím zadávacího řízení zajistit, aby byly zavedeny pouze technologie rozpoznávání obličeje založené na zásadách **záměrné a standardní ochrany osobních údajů**.

Vedení logů (srovnej článek 25 směrnice o prosazování práva) je důležitou zárukou pro ověřování zákonnosti zpracování, a to jak interně (tj. vlastní kontrola ze strany dotčeného správce/zpracovatele), tak ze strany externích dozorových úřadů. V souvislosti se systémy rozpoznávání obličejů se doporučuje vést logy také pro změny referenční databáze a pokusy o identifikaci nebo ověření, včetně uživatele, výsledku a míry jistoty. Vedení logů je však pouze jedním ze základních prvků celkové **zásady odpovědnosti** (viz čl. 4 odst. 4 směrnice o prosazování práva). Správce musí být schopen prokázat soulad zpracování se základními zásadami ochrany osobních údajů podle čl. 4 odst. 1 až 3 směrnice o prosazování práva.

EDPB připomíná **výzvu** vydanou společně s EIOÚ k **zákazu** některých druhů zpracování v souvislosti s 1) biometrickou identifikací jednotlivců na dálku na veřejně přístupných místech; 2) systémy rozpoznávání obličeje s podporou umělé inteligence, které podle biometrických údajů rozřazují jednotlivce do skupin podle etnického původu, pohlaví a politické či sexuální orientace nebo na základě jiných důvodů k diskriminaci; 3) používání technologií rozpoznávání obličeje nebo podobných technologií k odvozování emocí fyzické osoby a 4) zpracování osobních údajů v kontextu prosazování práva, které by se opíralo o databázi zaplněnou hromadně a bez rozlišování shromážděnými osobními údaji, např. „scrapingem“ fotografií a obrázků obličejů dostupných na internetu.

Ústřední zárukou dotčených základních práv je **účinný dohled** ze strany příslušných dozorových úřadů pro ochranu osobních údajů. Členské státy proto musí zajistit, aby zdroje dozorových úřadů byly přiměřené a dostatečné k tomu, aby jim umožnily plnit jejich mandát.

Tyto **pokyny jsou určeny** tvůrcům právních předpisů na úrovni EU a členských států, jakož i donucovacím orgánům a jejich úředníkům, kteří zavádějí a využívají systémy technologie rozpoznávání obličeje. Jsou určeny i jednotlivcům, pokud o tuto tematiku mají zájem obecně nebo jako subjekty údajů, zejména pokud jde o práva subjektů údajů.

Cílem pokynů je informovat o určitých vlastnostech technologie rozpoznávání obličeje a o použitelném právním rámci v souvislosti s prosazováním práva (zejména o směrnici o prosazování práva).

- Kromě toho poskytují **nástroj na podporu první klasifikace citlivosti daného případu použití** (příloha I).
- Obsahují také **praktické pokyny pro donucovací orgány, které chtějí pořídit a provozovat technologii rozpoznávání obličeje** (příloha II).
- Pokyny rovněž popisují několik typických **případů použití a uvádějí řadu relevantních úvah**, zejména pokud jde o test nezbytnosti a přiměřenosti (příloha III).

1 ÚVOD

1. Technologii rozpoznávání obličeje lze použít k automatickému rozpoznání jednotlivců na základě jejich obličeje. Tato technologie je často založena na umělé inteligenci, jako jsou technologie strojového učení. Aplikace technologie rozpoznávání obličeje jsou stále častěji testovány a používány v různých oblastech, od individuálního použití až po použití v soukromých organizacích a veřejné správě. Výhody z používání technologie rozpoznávání obličeje očekávají také donucovací orgány. Slibuje řešení poměrně nových problémů, jako jsou šetření zahrnující velké množství zachycených důkazů, ale také známých problémů, zejména s ohledem na nedostatečné personální zajištění úkolů v oblasti pozorování a pátrání.

2. Zvýšený zájem o technologie rozpoznávání obličeje panuje do značné míry kvůli jejich efektivitě a škálovatelnosti. S tím souvisí nevýhody nedílně spojené s touto technologií a jejím používáním – a to i ve velkém měřítku. Ačkoli po stisknutí tlačítka mohou být analyzovány tisíce souborů osobních údajů, již nepatrné účinky algoritmické diskriminace nebo nesprávné identifikace mohou mít za následek vysoký počet jednotlivců, kteří budou významně dotčeni, pokud jde o jejich chování a každodenní život. Rozsah zpracování osobních údajů a zejména biometrických údajů je dalším klíčovým prvkem technologie rozpoznávání obličeje, neboť zpracování osobních údajů představuje zásah do základního práva na ochranu osobních údajů podle článku 8 Listiny základních práv Evropské unie.

3. Uplatňování technologie rozpoznávání obličeje donucovacími orgány bude mít – a do jisté míry již má – významné dopady na jednotlivce a skupiny osob, včetně menšin. Tyto důsledky budou mít rovněž značný dopad na způsob našeho soužití a na naši sociální a demokratickou politickou stabilitu, která přikládá značnou hodnotu pluralismu a odlišným politickým názorům. Právo na ochranu osobních údajů je často jedním z klíčových předpokladů pro zajištění dalších základních práv. Uplatňování technologie rozpoznávání obličeje je značně náchylné k zásahu do základních práv nad rámec práva na ochranu osobních údajů.

4. EDPB proto považuje za důležité přispět k pokračujícímu začleňování technologie rozpoznávání obličeje do oblasti prosazování práva, na kterou se vztahuje směrnice o prosazování práva[1],

[1] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či

resp. vnitrostátní právní předpisy, kterými se tato směrnice provádí, a tyto pokyny vydat. Pokyny mají poskytovat relevantní informace normotvůrcům na úrovni EU a na vnitrostátní úrovni, jakož i donucovacím orgánům a jejich úředníkům při provádění a používání systémů založených na technologii rozpoznávání obličeje. Oblast působnosti pokynů je omezena na technologie rozpoznávání obličeje. Jiné formy zpracování osobních údajů na základě biometrických údajů donucovacími orgány, zejména pokud jsou zpracovány na dálku, však mohou představovat podobná nebo další rizika pro jednotlivce, skupiny a společnost. V závislosti na daných okolnostech mohou některé aspekty těchto pokynů sloužit jako užitečný zdroj i v těchto případech. V neposlední řadě zde mohou najít důležité informace také fyzické osoby, které mají zájem o tuto tematiku obecně nebo jako subjekty údajů, zejména pokud jde o práva subjektů údajů.

5. Pokyny sestávají z hlavního dokumentu a tří příloh. Předkládaný hlavní dokument představuje danou technologii a platný právní rámec. V příloze I lze nalézt šablonu jako pomůcku pro určení některých hlavních aspektů pro klasifikaci závažnosti zásahu do základních práv pro danou oblast použití. Donucovací orgány, které chtějí pořídit a provozovat systém založený na technologii rozpoznávání obličeje, mohou najít praktické pokyny v příloze II. V závislosti na oblasti použití technologie rozpoznávání obličeje by mohly být relevantní různé úvahy. Soubor hypotetických scénářů a příslušné úvahy lze nalézt v příloze III.

2 TECHNOLOGIE

2.1 Jedna biometrická technologie, dvě odlišné funkce

6. Rozpoznávání obličeje je pravděpodobnostní technologie, která dokáže automaticky rozpoznat jednotlivce na základě jejich obličeje za účelem jejich autentizace nebo identifikace.

7. Technologie rozpoznávání obličeje spadá do širší kategorie biometrických technologií. Biometrické údaje zahrnují všechny automatizované postupy používané k rozpoznání jednotlivce prostřednictvím kvantifikace fyzických, fyziologických nebo behaviorálních charakteristik (otisky prstů, struktura oční duhovky, hlas, chůze, vzory krevních cév atd.). Tyto vlastnosti jsou definovány jako „biometrické údaje“, protože umožňují nebo potvrzují jedinečnou identifikaci dané osoby.

8. Tak je tomu i v případě lidských obličejů, přesněji řečeno jejich technického zpracování pomocí zařízení pro rozpoznávání obličejů: pořízením obrazu obličeje (fotografie nebo videa), který se nazývá biometrický „vzorek“, je možné získat digitální reprezentaci specifických charakteristik tohoto obličeje (ta se označuje jako „šablona“).

9. Biometrická šablona je digitální reprezentace jedinečných prvků, které byly získány z biometrického vzorku a mohou být uloženy v biometrické databázi[2]. Tato šablona má být jedinečná a specifická pro každou osobu a je v zásadě trvalá v čase[3]. Ve fázi rozpoznávání zařízení porovnává tuto šablonu s jinými šablonami, které byly dříve vytvořeny nebo vypočteny přímo z biometrických vzorků, jako jsou obličeje nacházející se na snímku, fotografii nebo videu. „Rozpoznávání obličeje“ je tedy dvoufázový proces: shromáždění obrazu obličeje a jeho převedení do podoby šablony, po níž následuje rozpoznání tohoto obličeje porovnáním příslušné šablony s jednou nebo více dalšími šablonami.

---

stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

[2] Guidelines on facial recognition (Pokyny pro rozpoznávání obličeje), Poradní výbor Úmluvy č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat, Rada Evropy, červen 2021.

[3] To může záviset na typu biometrie a věku subjektu údajů.

10. Stejně jako jakýkoli jiný biometrický proces může rozpoznávání obličeje plnit dvě odlišné funkce:

- **autentizace** osoby, jejímž cílem je ověřit, zda osoba je ta, za koho se vydává. V tomto případě systém porovná předem zaznamenanou biometrickou šablonu nebo vzorek (např. uložený na čipové kartě nebo v biometrickém pasu) s jediným obličejem, například s obličejem osoby, která se dostavila na kontrolní stanoviště, aby ověřil, zda se jedná o jednu a tutéž osobu. Tato funkce se proto opírá o porovnání dvou šablon. Tomu se také říká **ověření** 1 : 1.

- **identifikace** osoby s cílem nalézt osobu ve skupině jednotlivců v určité oblasti, na obrázku nebo v databázi. V tomto případě musí systém zpracovat každý zachycený obličej, vygenerovat biometrickou šablonu a poté zkontrolovat, zda se shoduje s osobou, kterou systém zná. Tato funkce se tedy opírá o porovnání jedné šablony s databází šablon nebo vzorků (výchozí hodnota). Tato identifikace se také nazývá identifikace 1 : více. Může například propojit záznam o jménu osoby (příjmení, křestní jméno) s obličejem, pokud je porovnáván s databází fotografií přiřazených k příjmením a křestním jménům. Může také zahrnovat sledování osoby v davu, aniž by nutně došlo k propojení s občanskou identitou dané osoby.

11. V obou případech jsou použité techniky rozpoznávání obličeje založeny na odhadované shodě mezi šablonami: šablonou, která se srovnává, a výchozí hodnotou (výchozími hodnotami). Z tohoto hlediska se jedná o pravděpodobnostní technologii: srovnání odvodí vyšší nebo nižší pravděpodobnost toho, že daná osoba je skutečně osobou, která má být autentizována nebo identifikována; pokud tato pravděpodobnost přesáhne určitou prahovou hodnotu v systému definovanou uživatelem nebo vývojářem systému, systém bude předpokládat, že existuje shoda.

12. Ačkoliv obě funkce – autentizace a identifikace – jsou odlišné, obě se týkají zpracování biometrických údajů identifikované nebo identifikovatelné fyzické osoby, a proto představují zpracování osobních údajů, a konkrétněji zpracování zvláštních kategorií osobních údajů.

13. Rozpoznávání obličeje je součástí širšího spektra technik zpracování videozáznamu. Některé videokamery mohou natáčet lidi ve vymezené oblasti, zejména jejich obličeje, ale nemohou být jako takové použity k automatickému rozpoznávání jednotlivců. Totéž platí pro obyčejnou fotografii: fotoaparát není systémem pro rozpoznávání obličeje, protože fotografie osob musí být zpracovány zvláštním způsobem, aby bylo možné získat biometrické údaje.

14. Samotná detekce obličejů takzvanými „chytrými“ fotoaparáty také nemusí nutně představovat systém rozpoznávání obličejů. Digitální techniky pro odhalování abnormálního chování nebo projevů násilí nebo pro rozpoznávání emocí v obličeji, nebo dokonce siluet sice také vyvolávají důležité otázky ohledně etiky a účinnosti, ale nelze je považovat za biometrické systémy zpracovávající zvláštní kategorie osobních údajů, pokud jejich cílem není jednoznačná identifikace určité osoby a pokud příslušné zpracování osobních údajů nezahrnuje jiné zvláštní kategorie osobních údajů. Tyto příklady do jisté míry souvisí s rozpoznáváním obličeje a stále podléhají pravidlům pro ochranu osobních údajů[4]. Kromě toho lze tento typ detekčního systému používat ve spojení s jinými systémy, jejichž cílem je identifikace osoby, a tudíž jej lze považovat za technologii rozpoznávání obličeje.

15. Na rozdíl například od systémů pro zachycování a zpracování videozáznamů, které vyžadují instalaci fyzických zařízení, je rozpoznávání obličeje softwarovou funkcí, kterou lze zavést v rámci stávajících systémů (kamery, databáze snímků atd.). Tato funkce může být tudíž propojena s mnoha systémy nebo

[4] Článek 10 směrnice o prosazování práva (nebo článek 9 obecného nařízení o ochraně osobních údajů) se však vztahuje na systémy, které se používají ke kategorizaci osob na základě jejich biometrických údajů do skupin podle etnického původu, jakož i politické nebo sexuální orientace nebo jiných zvláštních kategorií osobních údajů.

k nim připojena jako rozhraní a může být kombinována s dalšími funkcemi. Toto začlenění do již existující infrastruktury vyžaduje zvláštní pozornost, protože obnáší inherentní rizika, že technologie rozpoznávání obličeje by mohla být bez potíží a snadno skrytá[5].

2.2 Široká škála účelů a aplikací

16. Nad rámec tematického záběru těchto pokynů a mimo oblast působnosti směrnice o prosazování práva lze rozpoznávání obličeje používat k mnoha účelům, a to jak komerčním, tak pro řešení problémů v oblasti veřejné bezpečnosti nebo prosazování práva. Lze jej použít v mnoha různých kontextech: v osobním vztahu mezi uživatelem a službou (přístup k aplikaci), pro přístup na určité místo (fyzické filtrování) nebo bez jakéhokoliv zvláštního omezení ve veřejném prostoru (rozpoznávání obličejů naživo). Lze jej použít na jakýkoli typ subjektu údajů: zákazníka služby, zaměstnance, náhodného přihlížejícího, hledanou osobu nebo osobu zapojenou do soudního nebo správního řízení atd. Některá použití jsou již běžná a rozšířená; jiná jsou v tomto okamžiku v experimentální nebo spekulativní fázi. Ačkoli se tyto pokyny nezabývají všemi těmito použitími a aplikacemi, EDPB připomíná, že mohou být zavedeny pouze tehdy, pokud jsou v souladu s platným právním rámcem, a zejména s obecným nařízením o ochraně osobních údajů a příslušnými vnitrostátními právními předpisy[6]. I v souvislosti se směrnicí o prosazování práva mohou být údaje zpracovávané za použití technologie rozpoznávání obličeje v návaznosti na funkce autentizace nebo identifikace dále zpracovány pro jiné účely, např. kategorizace.

17. Konkrétněji by bylo možné zvážit škálu možných použití v závislosti na míře kontroly, kterou lidé mají nad svými osobními údaji, na účinných prostředcích, které mají k dispozici pro výkon této kontroly, a na jejich právu na iniciativu v souvislosti se zahájením používání a používáním této technologie, na důsledcích, které pro ně budou mít (v případě rozpoznání nebo nerozpoznání), a na rozsahu prováděného zpracování. Rozpoznávání obličeje na základě šablony uložené na osobním zařízení (čipová karta, chytrý telefon atd.), které patří dané osobě, a které se používá k autentizaci a ryze osobnímu použití prostřednictvím k tomu určeného rozhraní, nepředstavuje stejná rizika jako například použití pro účely identifikace v nekontrolovaném prostředí bez aktivního zapojení subjektů údajů, kdy je šablona každého obličeje vstupujícího do oblasti monitorování porovnána se šablonami ze širokého průřezu populace uloženými v databázi. Mezi těmito dvěma extrémy se nachází velmi rozmanité spektrum použití a souvisejících problémů týkajících se ochrany osobních údajů.

18. Pro další ilustraci kontextu, v němž se v současné době diskutuje o technologiích rozpoznávání obličeje nebo jejich zavádění, ať už pro účely autentizace, nebo identifikace, považuje EDPB za vhodné uvést řadu příkladů. Níže uvedené příklady jsou výhradně popisné a neměly by být považovány za žádný druh předběžného posouzení jejich souladu s acquis EU v oblasti ochrany osobních údajů.

Příklady autentizace pomocí rozpoznávání obličeje

19. Autentizace může být navržena tak, aby uživatelé nad ní měli plnou kontrolu, například tak, aby umožňovala přístup ke službám nebo aplikacím výhradně v domácím prostředí. V tomto ohledu ji vlastníci chytrých telefonů ve velké míře využívají k odblokování svého zařízení namísto ověřování pomocí hesla.

20. Ověřování pomocí rozpoznávání obličeje lze použít také ke kontrole totožnosti osoby, která chce využít služeb veřejných nebo soukromých třetích stran. Tyto postupy tak nabízejí způsob, jak vytvořit digitální

[5] Například u kamer připevněných na těle, které se v praxi používají stále více.
[6] Další pokyny naleznete také v pokynech EDPB 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky přijatých dne 29. ledna 2020.

identitu pomocí mobilní aplikace (chytrého telefonu, tabletu atd.), kterou lze následně využít pro přístup k on-line administrativním službám.

21. Kromě toho může být cílem autentizace na základě rozpoznávání obličeje kontrola fyzického přístupu na jedno nebo více předem určených míst, jako jsou vchody do budov nebo určité hraniční přechody. Tato funkce se například uplatňuje při některých zpracováních pro účely překročení hranic, kdy se obličej osoby na zařízení na kontrolním stanovišti porovnává s obličejem uloženým v jejím dokladu totožnosti (cestovním pasu nebo povolení k pobytu s bezpečnostními prvky).

Příklady identifikace pomocí rozpoznávání obličeje

22. Identifikaci lze využít mnoha ještě rozmanitějšími způsoby. Patří mezi ně zejména níže uvedená použití, která jsou v současné době v EU předmětem zkoumání, experimentů nebo plánů.

- vyhledávání identity neidentifikované osoby (oběti, podezřelého atd.) v databázi fotografií,
- monitorování pohybu osoby ve veřejném prostoru. Její obličej se porovnává s biometrickými šablonami osob, které cestují nebo cestovaly ve sledované oblasti, například při opuštění zavazadla nebo po spáchání trestného činu,
- rekonstrukce cesty osoby a jejích následných interakcí s jinými osobami prostřednictvím opožděného porovnání týchž prvků, například ve snaze identifikovat její kontakty,
- biometrická identifikace hledaných osob na dálku ve veřejných prostranstvích. Všechny obličeje zachycené naživo bezpečnostními videokamerami jsou v reálném čase porovnávány s databází bezpečnostních složek,
- automatické rozpoznávání osob na snímku, například za účelem identifikace jejich vztahů na sociální síti, kterou využívá. Snímek je porovnán se šablonami všech osob v síti, které s touto funkcí souhlasily, aby bylo možné navrhnout jmenovitou identifikaci těchto vztahů,
- přístup ke službám, přičemž některé bankomaty rozpoznávají své zákazníky porovnáním obličeje zachyceného kamerou s databází obličejů, kterou má banka k dispozici,
- sledování cesty cestujícího v určité fázi cesty. Šablona vypočtená v reálném čase pro každou osobu, která prochází kontrolou u bran nacházejících se v určitých fázích cesty (místa odbavení zavazadel, nástupní brány atd.), se porovnává se šablonami osob, které byly v systému dříve zaregistrovány.

23. Kromě používání technologie rozpoznávání obličeje v oblasti prosazování práva, také široká škála sledovaných aplikací jistě vyžaduje komplexní diskusi a rozpracování příslušné politiky, aby bylo možné zajistit jednotnost a soulad s acquis EU v oblasti ochrany osobních údajů.

2.3 Spolehlivost, přesnost a rizika pro subjekty údajů

24. Stejně jako každá technologie může být i rozpoznávání obličeje zdrojem problémů, pokud jde o jeho zavádění, zejména s ohledem na jeho spolehlivost a účinnost při autentizaci nebo identifikaci, jakož s ohledem na celkový problém kvality a přesnosti „zdrojových“ údajů a výsledku zpracování na základě technologie rozpoznávání obličeje.

25. Tyto technologické výzvy s sebou přináší zvláštní rizika pro dotčené subjekty údajů, která jsou o to významnější nebo závažnější v oblasti prosazování práva s ohledem na možné dopady na subjekty údajů, ať už právní, nebo jiné povahy, které se jich významně dotýkají. V této souvislosti se zdá být také užitečné zdůraznit, že následné použití technologie rozpoznávání obličeje není samo o sobě

bezpečnější, protože jednotlivci mohou být sledováni v různých časech a na různých místech. Následné použití tedy rovněž představuje specifická rizika, která je třeba posuzovat případ od případu.[7]

26. Jak zdůraznila Agentura EU pro základní práva ve své zprávě z roku 2019, „určení nezbytné úrovně přesnosti softwaru pro rozpoznávání obličeje je náročné: existuje mnoho různých způsobů hodnocení a posouzení přesnosti, a to i v závislosti na úkolu, účelu a kontextu jeho používání. Při použití této technologie na místech, která navštěvují miliony lidí, jako jsou vlaková nádraží nebo letiště, znamená relativně malý podíl chyb (např. 0,01 %)[8], že budou chybně označeny stovky lidí. Kromě toho může být u některých kategorií osob pravděpodobnost chybného přiřazení vyšší než u jiných, jak je popsáno v části 3. Existují různé způsoby, jak vypočítat a interpretovat míru chyb, a proto je nutná opatrnost. Pokud jde o přesnost a chybovost, jsou navíc důležité otázky týkající se toho, jak snadno lze systém oklamat například pomocí falešných snímků obličeje (tzv. „spoofing“), a to zejména pro účely prosazování práva.“[9]

27. V této souvislosti EDPB považuje za důležité připomenout, že technologie rozpoznávání obličeje, bez ohledu na to, zda je používána pro účely autentizace nebo identifikace, neposkytuje spolehlivě přesný výsledek, ale opírá se o pravděpodobnost, že dva obličeje nebo snímky obličeje náleží téže osobě[10]. Kvalita tohoto výsledku se dále snižuje, pokud je kvalita vstupních biometrických vzorků pro rozpoznávání obličeje nízká. Faktory nízké kvality mohou být rozmazanost vstupních snímků, nízké rozlišení kamery či fotoaparátu, pohyb a nedostatečné osvětlení. Dalšími aspekty s významným dopadem na výsledky jsou četnost výskytu a spoofing, např. když se pachatelé snaží buď vyhnout průchodu kolem kamer, nebo oklamat technologii rozpoznávání obličeje. V řadě studií se také upozorňuje na to, že takové statistické výsledky algoritmického zpracování mohou být také předmětem zkreslení, zejména v důsledku kvality zdrojových dat a databází, které sloužily ke „školení“ technologie, nebo jiných faktorů, jako je volba místa nasazení. Dále je třeba zdůraznit dopad technologie rozpoznávání obličeje na další základní práva, jako je respektování soukromého a rodinného života, svoboda projevu a informací, svoboda shromažďování a sdružování atd.

28. Je proto nezbytné, aby spolehlivost a přesnost technologie rozpoznávání obličeje byly brány v úvahu jako kritéria pro posouzení souladu s klíčovými zásadami ochrany osobních údajů podle článku 4 směrnice o prosazování práva, a zejména pokud jde o korektnost a přesnost.

29. EDPB zdůrazňuje, že pro kvalitní algoritmy jsou zásadní kvalitní údaje, a zároveň vyzdvihuje, že správci údajů musí v rámci své povinnosti vyvozování odpovědnosti provádět pravidelné a systematické hodnocení algoritmického zpracování, aby byla zajištěna zejména přesnost, korektnost a spolehlivost výsledku takového zpracování osobních údajů. Osobní údaje používané pro účely hodnocení, školení a dalšího rozvoje systémů založených na technologii rozpoznávání obličeje mohou být zpracovávány pouze na základě dostatečného právního základu a v souladu se společnými zásadami ochrany osobních údajů.

[7] Viz příklady uvedené v příloze III.

[8] Tato míra přesnosti vychází z citované zprávy a představuje míru, která je mnohem lepší než současné výsledky algoritmů v aplikacích založených na technologii rozpoznávání obličeje.

[9] Technologie rozpoznávání obličeje: aspekty základních práv v kontextu prosazování práva, Agentura Evropské unie pro základní práva, 21. listopadu 2019.

[10] Tato pravděpodobnost se označuje jako „míra jistoty“.

3 POUŽITELNÝ PRÁVNÍ RÁMEC

30. Používání technologií rozpoznávání obličeje je nedílně spjato se zpracováním osobních údajů, včetně zvláštních kategorií údajů. Kromě toho má přímý nebo nepřímý dopad do řady základních práv zakotvených v Listině základních práv EU. To je obzvláště důležité v oblasti prosazování práva a trestního soudnictví. Jakékoli použití technologií rozpoznávání obličeje by proto mělo být prováděno důsledně v souladu s platným právním rámcem.

31. Při posuzování budoucích legislativních a správních opatření, jakož i při provádění stávajících právních předpisů v jednotlivých konkrétních případech, které zahrnují technologie rozpoznávání obličeje, je vhodné zvážit níže uvedené informace. Relevantnost příslušných požadavků se liší v závislosti na konkrétních okolnostech. Vzhledem k tomu, že nelze předvídat všechny budoucí okolnosti, má se za to, že se jedná pouze o podpůrné požadavky, a nelze je vykládat jako vyčerpávající výčet.

3.1 Obecný právní rámec – Listina základních práv EU a Evropská úmluva o lidských právech (EÚLP)

3.1.1 Použitelnost Listiny

32. Listina základních práv EU je určena orgánům, institucím a jiným subjektům Unie a členským státům při provádění práva Unie.

33. Právní úprava zpracování biometrických údajů pro účely vymáhání práva podle čl. 1 odst. 1 směrnice o prosazování práva nevyhnutelně vyvolává otázku dodržování základních práv, zejména respektování soukromého života a komunikace podle článku 7 Listiny a práva na ochranu osobních údajů podle článku 8 Listiny.

34. Shromažďování a analýza videozáznamů fyzických osob, včetně jejich obličejů, znamená zpracování osobních údajů. Při technickém zpracování snímku se zpracovávají také biometrické údaje. Technické zpracování údajů týkajících se obličeje fyzické osoby v závislosti na čase a místě umožňuje vyvodit závěry ohledně soukromého života dotčených osob. Tyto závěry se mohou týkat rasového nebo etnického původu, zdravotního stavu, náboženství, zvyklostí každodenního života, místa trvalého nebo přechodného pobytu, denního nebo jiného pohybu, vykonávaných činností, sociálních vztahů těchto osob a sociálního prostředí, v němž se pohybují. Velké spektrum informací, které mohou být odhaleny uplatňováním technologie rozpoznávání obličeje, jasně ukazuje možný dopad do práva na ochranu osobních údajů stanovené v článku 8 Listiny, ale také na právo na soukromí stanovené v článku 7 Listiny.

35. Za takových okolností nelze vyloučit ani to, že by shromažďování, analýza a další zpracování dotčených biometrických údajů (obličeje) mohlo mít vliv na pocit možnosti svobodného jednání u lidí, i když by toto jednání bylo plně v souladu se svobodnou a otevřenou společností. To může mít rovněž závažné důsledky pro výkon jejich základních práv, jako je právo na svobodu myšlení, svědomí a náboženského vyznání, na svobodu pokojného shromažďování a na svobodu sdružování podle článků 1, 10, 11 a 12 Listiny. Takové zpracování zahrnuje rovněž další rizika, jako je riziko zneužití osobních informací shromážděných příslušnými orgány v důsledku nezákonného přístupu k osobním údajům a jejich využívání, porušení zabezpečení údajů atd. Tato rizika často závisí na zpracování a jeho okolnostech, jako je riziko neoprávněného přístupu a použití ze strany policistů nebo jiných neoprávněných stran. Některá rizika však jednoduše vyplývají z jedinečné povahy biometrických údajů. Na rozdíl od adresy nebo telefonního čísla není možné, aby subjekt údajů změnil své jedinečné vlastnosti, jako je obličej

nebo duhovka. V případě neoprávněného přístupu nebo náhodného zveřejnění biometrických údajů by to vedlo k ohrožení údajů, pokud jde o jejich používání jako hesel nebo šifrovacích klíčů, nebo by to mohlo být použito k dalším neoprávněným činnostem v oblasti sledování ke škodě subjektu údajů.

3.1.2 Zásah do práv stanovených v Listině

36. Zpracování biometrických údajů za všech okolností představuje závažný zásah samo o sobě. Tento zásah nezávisí na výsledku, např. na nalezení shody. Zpracování představuje zásah i v případě, že je biometrická šablona okamžitě vymazána poté, co porovnání s policejní databází vyústí v nenalezení shody.

37. Zásah do základních práv subjektů údajů může vyplývat z právního jednání, které buď směřuje k omezení příslušného základního práva, nebo má jeho omezení za následek[11]. Může rovněž vyplývat z jednání orgánu veřejné moci se stejným účelem nebo účinkem, nebo dokonce z jednání soukromého subjektu, který je právními předpisy pověřen výkonem veřejné moci a veřejných pravomocí.

38. Legislativní opatření, které slouží jako právní základ pro zpracování osobních údajů, přímo zasahuje do práv zaručených články 7 a 8 Listiny[12].

39. Používání biometrických údajů a technologie rozpoznávání obličeje v mnoha případech rovněž ovlivňuje zejména právo na lidskou důstojnost zaručené článkem 1 Listiny. Má-li být zachována lidská důstojnost, nesmí se s jednotlivci zacházet jako s pouhými věcmi. Technologie rozpoznávání obličeje přepočítává existenční a vysoce osobní vlastnosti, tj. rysy obličeje, do strojově čitelné podoby s cílem použít je jako lidskou „registrační značku“ nebo průkaz totožnosti, čímž z obličeje dělá věc.

40. Takové zpracování může zasáhnout i do dalších základních práv, jako jsou práva podle článků 10, 11 a 12 Listiny, pokud jsou odrazující účinky zamýšleným důsledkem příslušného kamerového dohledu ze strany donucovacích orgánů, nebo z tohoto sledování vyplývají.

41. Kromě toho by měla být pečlivě zvážena potenciální rizika spojená s používáním technologií rozpoznávání obličeje donucovacími orgány s ohledem na právo na spravedlivý proces a presumpci neviny podle článků 47 a 48 Listiny. Výsledek použití technologie rozpoznávání obličeje, např. shoda, může vést nejen k tomu, že osoba bude podrobena další policejní kontrole, ale může být také rozhodujícím důkazem v soudním řízení. Nedostatky technologie rozpoznávání obličeje, jako je možná předpojatost, diskriminace nebo chybná identifikace („falešně pozitivní“ výsledek), tak mohou vést k závažným důsledkům i pro trestní řízení. Kromě toho může být při hodnocení důkazů výsledek použití technologie rozpoznávání obličeje upřednostněn, i když existují důkazy, které tomu odporují („automatizační předpojatost“).

3.1.3 Odůvodnění zásahu

42. Podle čl. 52 odst. 1 Listiny musí být každé omezení výkonu základních práv a svobod stanoveno zákonem a respektovat podstatu těchto práv a svobod. Při dodržení zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Evropská unie, nebo potřebě ochrany práv a svobod druhého.

3.1.3.1 Stanoveno zákonem

43. Článek 52 odst. 1 Listiny stanoví požadavek konkrétního právního základu. Tento právní základ musí být dostatečně jasný, aby občanům dostatečně naznačil podmínky a okolnosti, za nichž jsou orgány

[11] SDEU, C-219/91 – Ter Voort, RoC 1992 I-05485, bod 36 a násl.; SDEU, C-200/96 – Metronome, RoC 1998 I-1953, bod 28.
[12] SDEU, C-594/12, bod 36; SDEU, C-291/12, bod 23 a následující.

oprávněny přistoupit k jakýmkoli opatřením v oblasti shromažďování údajů a tajného sledování[13]. Musí dostatečně jasně uvádět rozsah a způsob výkonu příslušné diskreční pravomoci svěřené orgánům veřejné moci tak, aby byla jednotlivcům zajištěna minimální míra ochrany, na kterou mají v demokratické společnosti v právním státě nárok[14]. Zákonnost navíc vyžaduje přiměřené záruky, které zajistí, že bude respektováno zejména právo jednotlivce podle článku 8 Listiny. Tyto zásady se rovněž vztahují na zpracování osobních údajů pro účely hodnocení, školení a dalšího vývoje systémů založených na technologii rozpoznávání obličeje.

44. Vzhledem k tomu, že biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby představují zvláštní kategorie údajů uvedené v článku 10 směrnice o prosazování práva, různé aplikace založené na technologii rozpoznávání obličeje ve většině případů patrně budou vyžadovat zvláštní zákon, který by přesně popisoval aplikaci a podmínky jejího použití. To zahrnuje zejména druhy trestných činů a případně vhodnou prahovou hodnotu závažnosti těchto trestných činů, aby byla mimo jiné účinně vyloučena drobná kriminalita.[15]

3.1.3.2 Podstata základních práv na soukromí a na ochranu osobních údajů stanovených v článcích 7 a 8 Listiny

45. Omezení základních práv, která bezprostředně hrozí v rámci každé jednotlivé situace, musí stále zajistit, že bude respektována podstata daného konkrétního práva. Podstatou se rozumí samotné jádro příslušného základního práva[16]. Rovněž je třeba respektovat lidskou důstojnost, a to i v případech, kdy je právo omezeno[17].

46. Znaky možného porušení nedotknutelné podstaty jsou následující:

- Ustanovení, které ukládá omezení bez ohledu na individuální chování nebo výjimečné okolnosti dané osoby[18].
- Obrátit se na soud není možné nebo je tomu bráněno[19].
- Před závažným omezením se neberou v úvahu okolnosti dotčeného jednotlivce[20].
- S ohledem na práva podle článků 7 a 8 Listiny: Podstatu těchto práv by kromě rozsáhlého shromažďování metadat o komunikaci mohlo porušit získání informací o obsahu elektronické komunikace[21].
- S ohledem na práva podle článků 7, 8 a 11 Listiny: Právní předpisy, které vyžadují, aby poskytovatelé přístupu k online veřejným komunikačním službám a poskytovatelé hostingových služeb obecně a bez rozlišování uchovávali mimo jiné osobní údaje týkající se těchto služeb[22].
- S ohledem na práva podle článku 8 Listiny: Neexistence základních zásad ochrany a zabezpečení údajů by rovněž mohla představovat porušení podstaty tohoto práva[23].

[13] ESLP, Shimovolos proti Rusku, bod 68; Vukota-Bojić proti Švýcarsku.
[14] ESLP, Piechowicz proti Polsku, bod 212.
[15] Viz např. rozsudky SDEU ve věcech C-817/19 Ligue des droits humains, bod 151 a násl., C-207/16 Ministerio Fiscal, bod 56.
[16] SDEU C-279/09, RoC 2010 I-13849, bod 60.
[17] Vysvětlení k Listině základních práv, hlava I, vysvětlení k článku 1, Úř. věst. C 303, 14.12.2007, s. 17–35.
[18] SDEU C-601/15, bod 52.
[19] SDEU C-400/10, RoC 2010 I-08965, bod 55.
[20] SDEU C-408/03, RoC 2006 I-02647, bod 68.
[21] SDEU – 203/15 - Tele2 Sverige, bod. 101 s odkazem na SDEU - C-293/12 a C-594/12, bod 39.
[22] SDEU C-512/18, La Quadrature du Net, bod 209 a násl.
[23] SDEU – C-594/12, bod 40.

3.1.3.3 Legitimní cíl

47. Jak již bylo vysvětleno v bodě 3.1.3, omezení základních práv musí skutečně splňovat cíle obecného zájmu uznané Evropskou unií nebo naplňovat potřebu chránit práva a svobody jiných osob.

48. Unie uznává jak cíle uvedené v článku 3 Smlouvy o Evropské unii, tak další zájmy chráněné zvláštními ustanoveními Smluv[24], tj. mimo jiné prostor svobody, bezpečnosti a práva, předcházení trestné činnosti a boj proti ní. Ve svých vztazích s okolním světem by Unie měla přispívat k míru a bezpečnosti a ochraně lidských práv.

49. Potřebou chránit práva a svobody jiných osob se rozumí práva osob, která jsou chráněna právem Evropské unie nebo jejích členských států. Posouzení musí být provedeno s cílem sladit požadavky na ochranu příslušných práv a nastolit mezi nimi spravedlivou rovnováhu[25].

3.1.3.4 Zkouška nezbytnosti a přiměřenosti

50. Jedná-li se o zásahy do základních práv, může se ukázat, že rozsah posuzovací pravomoci vnitrostátního zákonodárce a normotvůrce Unie může být omezený. To závisí na řadě faktorů, včetně dotyčné oblasti, povahy dotčeného práva zaručeného Listinou, povahy a závažnosti zásahu a jeho účelu[26]. Legislativní opatření musí být vhodná k dosažení legitimních cílů sledovaných danou právní úpravou. Kromě toho nesmí opatření překročit meze toho, co je přiměřené a nezbytné k dosažení těchto cílů[27]. Cíl obecného zájmu – jakkoli zásadní – sám o sobě neodůvodňuje omezení základního práva[28].

51. Podle ustálené judikatury Soudního dvora Evropské unie se výjimky a omezení týkající se ochrany osobních údajů musí uplatňovat pouze v mezích toho, co je naprosto nezbytné[29]. To rovněž znamená, že k dosažení tohoto cíle nesmí být k dispozici žádné méně rušivé prostředky. Je třeba pečlivě určit a posoudit možné alternativy, jako je – v závislosti na daném účelu – další personál, častější policejní dohled nebo dodatečné pouliční osvětlení. Legislativní opatření by měla rozlišovat a zaměřovat se na osoby, na které se vztahují, s ohledem na cíl, např. boj proti závažné trestné činnosti. Vztahuje-li se obecně na všechny osoby bez takového rozlišování, omezení nebo výjimky, zvyšuje se intenzita zásahu[30]. Míra zásahu je větší i tehdy, pokud se zpracování údajů týká významné části obyvatelstva[31].

52. Ochrana osobních údajů, která vyplývá z výslovné povinnosti stanovené v čl. 8 odst. 1 Listiny, má zvláštní význam pro právo na respektování soukromého života zakotvené v článku 7 Listiny[32]. Právní předpisy musí stanovit jasná a přesná pravidla pro rozsah a použití dotčeného opatření a stanovit záruky, tak aby osoby, jejichž údaje se zpracovávají, měly dostatečné záruky umožňující účinně chránit jejich osobní údaje proti riziku zneužití a proti veškerému neoprávněnému přístupování k údajům a jejich protiprávnímu využívání[33]. Potřeba takových záruk je tím významnější v případě, kdy jsou osobní

[24] Vysvětlení k Listině základních práv, hlava I, Vysvětlení k článku 52, Úř. věst. C 303, 14.12.2007, s. 17–35.
[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Art. 52 Rn. 31–32.
[26] SDEU – C-594/12, bod 47 s následujícími zdroji: viz obdobně, pokud jde o článek 8 EÚLP, ESLP, S. a Marper v. Spojené království [velký senát], č. 30562/04 a 30566/04, bod 102, ESLP 2008-V.
[27] SDEU – C-594/12, odst. 46 s následujícími zdroji: věc C-343/09 Afton Chemical EU:C:2010:419, bod 45; Volker und Markus Schecke a Eifert, EU:C:2010:662, bod 74; věci C-581/10 a C-629/10 Nelson a další, EU:C:2012:657, bod 71; věc C-283/11 Sky Österreich, EU:C:2013:28, bod 50 a věc C-101/12 Schaible EU:C:2013:661, bod 29.
[28] SDEU – C-594/12, bod 51.
[29] SDEU – C-594/12, bod 52, s následujícími zdroji: věc C-473/12 IPI EU:C:2013:715, bod 39 a citovaná judikatura.
[30] SDEU – C-594/12, bod 57.
[31] SDEU – C-594/12, bod 56.
[32] SDEU – C-594/12, bod 53.
[33] SDEU – C-594/12, bod 54, s následujícími zdroji: viz obdobně, pokud jde o článek 8 EÚLP, ESLP, Liberty a další v. Spojené království, 1. července 2008, č. 58243/00, body 62 a 63; Rotaru v. Rumunsko, body 57 až 59 a S. a Marper v. Spojené království, bod 99.

údaje zpracovány automaticky a existuje značné riziko neoprávněného přistupování k těmto údajům[34]. Kromě toho může jako ochrana přispět i vnitřní nebo vnější, např. soudní, povolení k nasazení technologie rozpoznávání obličeje, které se může ukázat jako nezbytné v některých případech závažných zásahů.[35]

53. Stanovená pravidla je třeba přizpůsobit konkrétní situaci, např. množství zpracovávaných údajů, povaze údajů[36] a riziku nezákonného přístupu k údajům. To vyžaduje pravidla, která by měla především jasně a striktně upravit ochranu a bezpečnost dotčených údajů, aby byla zaručena jejich plná integrita a důvěrná povaha[37].

54. Pokud jde o vztah mezi správcem a zpracovatelem, nemělo by být povoleno, aby zpracovatelé při určování úrovně zabezpečení osobních údajů zohledňovali pouze ekonomické hledisko; to by mohlo ohrozit dostatečně vysokou úroveň ochrany[38].

55. Právní akt musí stanovit hmotněprávní a procesní podmínky a objektivní kritéria, podle nichž se vymezí přístup příslušných orgánů k údajům a jejich následné využití. Pro účely předcházení, odhalování nebo stíhání trestných činů by dotčené trestné činy musely být považovány za dostatečně závažné, aby odůvodnily rozsah a závažnost těchto zásahů do základních práv zakotvených například v článcích 7 a 8 Listiny[39].

56. Údaje musí být zpracovány způsobem, který zajišťuje použitelnost a účinnost pravidel EU pro ochranu osobních údajů; zejména pravidel stanovených v článku 8 Listiny, který stanoví, že dodržování požadavků na ochranu a bezpečnost podléhá kontrole nezávislého orgánu. V takové situaci může být relevantní zeměpisné místo, kde zpracování probíhá[40].

57. Pokud jde o jednotlivé kroky zpracování osobních údajů, je třeba rozlišovat mezi kategoriemi údajů podle jejich případné užitečnosti pro účely sledovaného cíle nebo podle dotčených osob[41]. Stanovení podmínek zpracování, například určení doby uchovávání, musí být založeno na objektivních kritériích, aby bylo zaručeno omezení zásahu na nezbytné minimum[42].

58. Na základě každé jednotlivé situace musí být v posouzení nezbytnosti a přiměřenosti identifikovány a zváženy všechny důsledky, které spadají do působnosti jiných základních práv, jako je lidská důstojnost podle článku 1 Listiny, svoboda myšlení, svědomí a náboženského vyznání podle článku 10 Listiny, svoboda projevu podle článku 11 Listiny a svoboda shromažďování a sdružování podle článku 12 Listiny.

59. Kromě toho je třeba vzít v úvahu, že pokud by byly údaje systematicky zpracovávány bez vědomí subjektů údajů, je pravděpodobné, že vznikne obecný dojem o neustálém dohledu[43]. To může vést k odrazujícím účinkům, pokud jde o některá nebo všechna dotčená základní práva.

---

[34] SDEU – C-594/12, bod 55, s následujícími zdroji: viz obdobně, pokud jde o článek 8 EÚLP, S. a Marper v. Spojené království, bod 103, a M. K. proti Francii, 18. dubna 2013, č. 19522/09, bod 35.
[35] ESLP, Szabó a Vissy proti Maďarsku, body 73–77.
[36] Viz rovněž zvýšené požadavky na technická a organizační opatření při zpracování zvláštních kategorií údajů, čl. 29 odst. 1 směrnice o prosazování práva.
[37] SDEU – C-594/12, bod 66.
[38] SDEU – C-594/12, bod 67.
[39] SDEU – C-594/12, body 60 a 61.
[40] SDEU – C-594/12, bod 68.
[41] SDEU – C-594/12, bod 63.
[42] SDEU – C-594/12, bod 64.
[43] SDEU – C-594/12, bod 37.

60. Pro usnadnění posuzování nezbytnosti a přiměřenosti legislativních opatření týkajících se rozpoznávání obličeje v oblasti vymáhání práva a pro jejich použitelnost v praxi by vnitrostátní normotvůrci a normotvůrci Unie mohli využít dostupné praktické nástroje určené speciálně pro tento úkol. Zejména by mohl být použit soubor nástrojů pro posouzení nezbytnosti a přiměřenosti[44], který poskytl Evropský inspektor ochrany údajů.

3.1.3.5 Článek 52 odst. 3 a článek 53 Listiny (úroveň ochrany, rovněž ve vztahu k ochraně podle EÚLP)

61. Podle čl. 52 odst. 3 a článku 53 Listiny musí být smysl a rozsah těch práv uvedených v Listině, která odpovídají právům zaručeným v EÚLP, stejné jako ty, které jim přikládá EÚLP. Zatímco zejména v případě článku 7 Listiny lze nalézt ekvivalent v EÚLP, v případě článku 8 Listiny tomu tak není[45]. Ustanovení čl. 52 odst. 3 Listiny nebrání tomu, aby právo Unie poskytovalo širší ochranu. Vzhledem k tomu, že EÚLP nepředstavuje právní nástroj, který byl formálně začleněn do unijního práva, musí být unijní právní předpisy zkoumány s ohledem na základní práva zaručená Listinou[46].

62. Podle článku 8 EÚLP nesmí státní orgán do výkonu tohoto práva na respektování soukromého a rodinného života zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

63. EÚLP rovněž stanoví normy, pokud jde o způsob, jakým lze omezení uplatňovat. Jedním ze základních požadavků, kromě zásady právního státu, je předvídatelnost. Má-li být uspokojen požadavek předvídatelnosti, musí právo pro jednotlivce dostatečně jasně stanovit okolnosti, za nichž se mohou orgány k užití těchto opatření uchýlit[47]. Tento požadavek uznává SDEU a právo EU v oblasti ochrany osobních údajů (viz oddíl 3.2.1.1).

64. Dále musí být plně respektována ustanovení Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat[48], která blíže vymezují práva uvedená v článku 8 EÚLP. Přesto je třeba vzít v úvahu, že tato ustanovení představují pouze minimální normu s ohledem na převládající právo Unie.

3.2 Zvláštní právní rámec – směrnice o prosazování práva

65. Určitý rámec, pokud jde o využívání technologie rozpoznávání obličeje, nabízí směrnice o prosazování práva. V první řadě se v čl. 3 odst. 13 směrnice o prosazování práva definuje pojem „biometrické údaje“[49]. Podrobnosti viz oddíl 2.1 výše. Za druhé, v čl. 8 odst. 2 se objasňuje, že má-li být zpracování zákonné, musí být – kromě toho, že je nezbytné pro účely uvedené v čl. 1 odst. 1 směrnice o

[44] Evropský inspektor ochrany údajů: Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit (Posuzování nezbytnosti opatření omezujících základní právo na ochranu osobních údajů: soubor nástrojů, 11. dubna 2017); Evropský inspektor ochrany údajů: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (Pokyny Evropského inspektora ochrany údajů k posuzování přiměřenosti opatření omezujících základní právo na soukromí a na ochranu osobních údajů, 19. prosince 2019).

[45] SDEU – C-203/15 – Tele2 Sverige, bod 129.

[46] SDEU – C-311/18, bod 99.

[47] Evropský soud pro lidská práva, rozsudek ve věci COPLAND proti SPOJENÉMU KRÁLOVSTVÍ, 3. dubna 2007, stížnost č. 62617/00, bod 46.

[48] Řada smluv Rady Evropy č. 108.

[49] Článek 3 bod 13 směrnice o prosazování práva: „Biometrickými údaji“ [se rozumí] osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje její jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.

prosazování práva – upraveno ve vnitrostátním právu, které stanoví alespoň cíle zpracování, osobní údaje, jež mají být zpracovány, a účel zpracování. Dalšími ustanoveními, která mají zvláštní význam, pokud jde o biometrické údaje, jsou články 10 a 11 směrnice o prosazování práva. Článek 10 je třeba vykládat ve spojení s článkem 8 směrnice o prosazování práva[50]. Zásady zpracování osobních údajů stanovené v článku 4 směrnice o prosazování práva by měly být vždy dodržovány a jakékoli posouzení případného biometrického zpracování prostřednictvím technologie rozpoznávání obličeje by se mělo řídit těmito zásadami.

3.2.1 Zpracování zvláštních kategorií údajů pro účely vymáhání práva

66. Podle článku 10 směrnice o prosazování práva je zpracování zvláštních kategorií údajů, jako jsou biometrické údaje, povoleno pouze tehdy, pokud je zcela nezbytné a pokud existují vhodné záruky práv a svobod subjektu údajů. Kromě toho je dovoleno pouze v případech, pokud je povoleno právem Unie nebo členského státu, na ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, nebo pokud se týká údajů zjevně zveřejněných subjektem údajů. Toto obecné ustanovení zdůrazňuje citlivost zpracování zvláštních kategorií údajů.

3.2.1.1 Povoleno právem Unie nebo členského státu

67. Pokud jde o nezbytný typ legislativního opatření, 33. bod odůvodnění směrnice o prosazování práva uvádí, že „[o]dkazy v této směrnici na právo či právní předpis, právní základ či legislativní opatření členského státu neznamenají nutně legislativní akt přijatý parlamentem, aniž jsou dotčeny požadavky vyplývající z ústavního řádu dotčeného členského státu“[51].

68. Čl. 52 odst. 1 Listiny stanoví, že každé omezení výkonu práv a svobod uznaných touto listinou musí být „stanoveno zákonem“. V tomto ustanovení znovu zaznívá výraz „v souladu se zákonem“ uvedený v čl. 8 odst. 2 EÚLP, kterým se rozumí nejen dodržování platných právních předpisů, ale který se týká rovněž kvality těchto právních předpisů, aniž by byla dotčena povaha aktu, a požaduje, aby byly slučitelné se zásadami právního státu.

69. V 33. bodě odůvodnění směrnice o prosazování práva se dále uvádí, že „[t]oto právo, právní předpisy, právní základ či legislativní opatření členského státu by však měly být jasné a přesné a jejich použití by mělo být předvídatelné pro osoby, na něž se vztahují, jak to vyžaduje judikatura Soudního dvora a Evropského soudu pro lidská práva. Právo členského státu upravující oblast zpracování osobních údajů v rámci oblasti působnosti této směrnice by mělo specifikovat alespoň cíle, osobní údaje, které mají být zpracovány, účely zpracování, postupy k zachování neporušenosti a důvěrné povahy údajů a postupy jejich zničení“.

70. Vnitrostátní právo musí být dostatečně jasné co do svého znění, aby subjekty údajů dostatečně znaly okolnosti a podmínky, za nichž jsou správci oprávněni uchýlit se k takovým opatřením. To zahrnuje možné podmínky pro zpracování, jako jsou specifické druhy důkazů, jakož i nezbytnost soudního nebo interního povolení. Příslušný právní předpis může být technologicky neutrální, pokud jsou dostatečně zohledněna konkrétní rizika a charakteristiky zpracování osobních údajů systémy založenými na technologii rozpoznávání obličeje. V souladu se směrnicí o prosazování práva a judikaturou Soudního dvora Evropské unie (SDEU) a Evropského soudu pro lidská práva (ESLP) je skutečně nezbytné, aby byla legislativní opatření, jejichž cílem je poskytnout právní základ pro opatření k rozpoznávání obličeje, pro subjekty údajů předvídatelná.

---

[50] WP258, Stanovisko k některým klíčovým otázkám směrnice o prosazování práva (EU 2016/680), s. 7.

[51] Druh zvažovaných legislativních opatření musí být v souladu s právem EU nebo s vnitrostátním právem. V závislosti na míře zásahu způsobeného daným omezením by na vnitrostátní úrovni mohlo být zapotřebí zvláštní legislativní opatření zohledňující úroveň normy.

71. Na legislativní opatření se nelze odvolávat jako na právní předpis povolující zpracování biometrických údajů prostřednictvím technologie rozpoznávání obličeje pro účely prosazování práva, pokud se jedná o pouhé provedení obecného ustanovení uvedeného v článku 10 směrnice o prosazování práva.

72. Kromě biometrických údajů upravuje článek 10 směrnice o prosazování práva zpracování dalších zvláštních kategorií údajů, jako je sexuální orientace, politické názory a náboženské vyznání, a pokrývá tak široké spektrum případů zpracování. Kromě toho by takové ustanovení postrádalo konkrétní požadavky uvádějící okolnosti a podmínky, za nichž by donucovací orgány byly oprávněny uchýlit se k používání technologie rozpoznávání obličeje. Vzhledem k odkazu na jiné druhy údajů a výslovné potřebě zvláštních záruk bez dalších specifikací nelze vnitrostátní ustanovení provádějící článek 10 směrnice o prosazování práva do vnitrostátního práva – s podobně obecným a abstraktním zněním – použít jako právní základ pro zpracování biometrických údajů zahrnující rozpoznávání obličeje, neboť by postrádalo přesnost a předvídatelnost. V souladu s čl. 28 odst. 2 nebo čl. 46 odst. 1 písm. c) směrnice o prosazování práva by měl být předtím, než normotvůrce vytvoří nový právní základ pro jakoukoli formu zpracování biometrických údajů prostřednictvím rozpoznávání obličeje, konzultován vnitrostátní dozorový úřad pro ochranu údajů.

3.2.1.2 Zcela nezbytné

73. Zpracování lze považovat za „zcela nezbytné“ pouze tehdy, pokud se zásah do ochrany osobních údajů a její omezení omezuje na to, co je naprosto nezbytné[52]. Doplnění výrazu „zcela“ znamená, že normotvůrce zamýšlel, aby ke zpracování zvláštních kategorií údajů docházelo pouze za podmínek, které jsou ještě přísnější než podmínky nezbytnosti (viz výše bod 3.1.3.4). Tento požadavek by měl být vykládán v tom smyslu, že je nezbytný. Omezuje prostor pro uvážení, který je donucovacímu orgánu přiznán v rámci testu nezbytnosti, na absolutní minimum. V souladu s ustálenou judikaturou Soudního dvora Evropské unie je podmínka, aby zpracování bylo „zcela nezbytné“, rovněž úzce spojena s požadavkem objektivních kritérií pro vymezení okolností a podmínek, za nichž lze zpracování provést, čímž je vyloučeno jakékoli zpracování obecné nebo systematické povahy[53].

3.2.1.3 Zjevně zveřejněno

74. Při posuzování, zda se zpracování týká údajů zjevně zveřejněných subjektem údajů, je třeba připomenout, že fotografie jako taková není systematicky považována za biometrický údaj[54]. Proto skutečnost, že fotografie byla subjektem údajů zjevně zveřejněna, neznamená, že související biometrické údaje, které lze z fotografie získat pomocí zvláštních technických prostředků, se považují za zjevně zveřejněné.

75. Stejně jako u osobních údajů obecně platí, že aby bylo možné biometrické údaje považovat za zjevně zveřejněné subjektem údajů, musí subjekt údajů úmyslně volně zpřístupnit a zveřejnit biometrickou šablonu (a nikoli pouze snímek obličeje) prostřednictvím otevřeného zdroje. Pokud biometrické údaje zveřejní třetí strana, nelze to považovat za zjevné zveřejnění údajů subjektem údajů.

76. Kromě toho nestačí vykládat chování subjektu údajů, aby bylo možné mít za to, že biometrické údaje byly zjevně zveřejněny. Například v případě sociálních sítí nebo online platforem se EDPB domnívá, že

[52] Pro soudržnou judikaturu týkající se základního práva na respektování soukromého života viz SDEU, věc C-73/07, bod 56 (Satakunnan Markkinapörssi a Satamedia); SDEU, věci C-92/09 a C-93/09 bod 77 (Schecke a Eifert); SDEU, věc C-594/12, bod 52 (Digital Rights); SDEU, věc C-362/14, bod 92 (Schrems).
[53] SDEU, věc C-623/17, bod 78.
[54] Srov. 51. bod odůvodnění obecného nařízení o ochraně osobních údajů: „zpracování fotografií by nemělo být systematicky považováno za zpracování zvláštních kategorií osobních údajů, neboť na fotografie se definice biometrických údajů vztahuje pouze v případech, kdy jsou zpracovávány zvláštními technickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci fyzické osoby “.

skutečnost, že subjekt údajů neuplatnil nebo nenastavil konkrétní prvky ochrany soukromí, nestačí k tomu, aby se mělo za to, že tento subjekt údajů zjevně zveřejnil své osobní údaje a že tyto údaje (např. fotografie) mohou být zpracovány do podoby biometrických šablon a použity pro účely identifikace bez souhlasu subjektu údajů. Obecněji řečeno, výchozí nastavení služby, např. zpřístupnění šablon veřejnosti, nebo absence možnosti volby, např. šablony jsou zveřejněny, aniž by uživatel mohl toto nastavení změnit, by neměly být v žádném případě vykládány jako údaje zjevně zveřejněné.

3.2.2 Automatizované individuální rozhodování, včetně profilování

77. V čl. 11 odst. 1 směrnice o prosazování práva se stanoví povinnost členských států obecně zakázat rozhodnutí založená výhradně na automatizovaném zpracování, včetně profilování, které má pro subjekt údajů nepříznivé právní účinky nebo se ho významně dotýká. Jako výjimka z tohoto obecného zákazu může být takové zpracování možné pouze tehdy, je-li povoleno právem Unie nebo členského státu, kterému správce podléhá a jež poskytuje vhodné záruky práv a svobod subjektu údajů, alespoň práva na lidský zásah ze strany správce. Lze ji používat pouze restriktivně. Toto omezení platí pro běžné (tj. nikoli zvláštní) kategorie osobních údajů. Pro výjimku podle čl. 11 odst. 2 směrnice o prosazování práva platí ještě přísnější omezení a restriktivnější použití. Znovu se zdůrazňuje, že rozhodnutí podle prvního odstavce se nesmějí opírat o zvláštní kategorie osobních údajů, tj. biometrické údaje za účelem jedinečné identifikace fyzické osoby. Výjimku lze stanovit pouze tehdy, jsou-li zavedeny vhodné záruky pro práva a svobody subjektu údajů a oprávněné zájmy dotčené fyzické osoby. Tuto výjimku je třeba číst jako doplnění ustanovení článku 10 směrnice o prosazování práva a s ohledem na toto ustanovení.

78. V závislosti na systému technologie rozpoznávání obličeje nemusí ani lidský zásah při posuzování výsledků technologie rozpoznávání obličeje sám o sobě nutně poskytovat dostatečnou záruku dodržování práv jednotlivců, zejména práva na ochranu osobních údajů, a to s ohledem na možnou předpojatost a chybovost, která může vyplývat ze samotného zpracování. Kromě toho lze lidský zásah považovat za záruku pouze tehdy, pokud zasahující osoba může během lidského zásahu kriticky zpochybnit výsledky technologie rozpoznávání obličeje. Je zásadní umožnit dané osobě pochopit systém založený na technologii rozpoznávání obličeje a jeho omezení, jakož i správně interpretovat jeho výsledky. Je rovněž nezbytné vytvořit pracoviště a organizaci, které vyvažují účinky automatického zkreslení a brání podpoře nekritického přijímání výsledků, např. v důsledku časového tlaku, zatěžujících postupů, potenciálně negativních dopadů na profesní dráhu atd.

79. Podle čl. 11 odst. 3 směrnice o prosazování práva je profilování, které vede k diskriminaci fyzických osob na základě zvláštních kategorií osobních údajů, jako jsou biometrické údaje, v souladu s právem Unie zakázáno. Podle čl. 3 odst. 4 směrnice o prosazování práva se „profilováním“ rozumí jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu. Při zvažování, zda jsou zavedeny vhodné záruky na ochranu práv a svobod subjektu údajů a oprávněných zájmů dotčené fyzické osoby, je třeba mít na paměti, že využití technologie rozpoznávání obličeje může vést k profilování v závislosti na způsobu a účelu, k němu se technologie rozpoznávání obličeje používá. V souladu s právem Unie a čl. 11 odst. 3 směrnice o prosazování práva je v každém případě zakázáno profilování, které vede k diskriminaci fyzických osob na základě zvláštních kategorií osobních údajů.

3.2.3 Kategorie subjektů údajů

80. Článek 6 směrnice o prosazování práva se týká nutnosti rozlišovat mezi různými kategoriemi subjektů údajů. Toto rozlišení je třeba provádět v příslušných případech a v maximální možné míře. Musí

prokázat účinek na způsob zpracování údajů. Z příkladů uvedených v článku 6 směrnice o prosazování práva lze vyvodit, že zpracování osobních údajů musí zpravidla splňovat kritéria nezbytnosti a přiměřenosti, a to i s ohledem na danou kategorii subjektů údajů[55]. Z toho lze dále vyvodit, že pokud jde o subjekty údajů, u nichž neexistuje žádný důvod se domnívat, že by jejich chování mohlo, byť nepřímo nebo vzdáleně, souviset s legitimním cílem podle směrnice o prosazování práva, neexistuje s největší pravděpodobností žádné odůvodnění zásahu[56]. Pokud není možné nebo proveditelné rozlišování podle článku 6 směrnice o prosazování práva, je třeba při posuzování nezbytnosti a přiměřenosti zásahu důsledně zvážit výjimku z pravidla uvedeného v článku 6 směrnice o prosazování práva. Rozlišování mezi různými kategoriemi subjektů údajů se jeví jako základní požadavek, pokud jde o zpracování osobních údajů zahrnující rozpoznávání obličeje, a to i s ohledem na možné falešně pozitivní nebo falešně negativní shody, které mohou mít významný dopad na subjekty údajů i na průběh vyšetřování.

81. Jak již bylo řečeno, při provádění práva Unie musí být respektována ustanovení Listiny základních práv Evropské unie, srov. článek 52 Listiny. Rámec a kritéria, které směrnice o prosazování práva stanoví, je proto třeba chápat s ohledem na Listinu. Právní akty EU a jejích členských států nesmí toto opatření porušovat a musí zajistit plnou účinnost Listiny.

3.2.4 Práva subjektu údajů

82. EDPB již poskytl pokyny k právům subjektů údajů podle Obecného nařízení o ochraně osobních údajů v různých aspektech[57]. Směrnice o prosazování práva stanoví podobná práva subjektů údajů a obecné pokyny k tomu byly poskytnuty ve stanovisku pracovní skupiny zřízené podle článku 29, které schválil EDPB[58]. Za určitých okolností směrnice o prosazování práva umožňuje určitá omezení těchto práv. Parametry pro tato omezení budou dále rozpracovány v oddíle 3.2.4.6. „Legitimní omezení práv subjektu údajů“.

83. Ačkoli se všechna práva subjektu údajů uvedená v kapitole III směrnice o prosazování práva přirozeně vztahují i na zpracování osobních údajů prostřednictvím technologie rozpoznávání obličeje, následující kapitola se zaměří na některá práva a aspekty, k nimž by mohlo být obzvláště zajímavé obdržet pokyny. Tato kapitola a analýza v ní uvedená jsou navíc podmíněny tím, že dané zpracování prostřednictvím technologie rozpoznávání obličeje vyhoví právním požadavkům popsaným v předchozí kapitole.

84. Vzhledem k povaze zpracování osobních údajů prostřednictvím technologie rozpoznávání obličeje (zpracování zvláštních kategorií osobních údajů často bez zjevné interakce se subjektem údajů) musí správce před zahájením jakéhokoli zpracování prostřednictvím technologie rozpoznávání obličeje pečlivě zvážit, jak (a zda vůbec) může splnit požadavky směrnice o prosazování práva. Zejména provede pečlivou analýzu těchto aspektů:

- kdo jsou subjekty údajů (často více než jeden subjekt, který je hlavním cílem pro účely zpracování),
- jak jsou subjekty údajů informovány o zpracování prostřednictvím technologie rozpoznávání obličeje (viz oddíl 3.2.4.1),
- jak mohou subjekty údajů vykonávat svá práva (v tomto případě mohou představovat zvláštní výzvu dodržování práva na informace a práva na přístup, jakož i práva na opravu nebo práva na

[55] Srov. také SDEU – C-594/12, body 56–59.
[56] Srov. také SDEU – C-594/12, bod 58.
[57] Viz například Pokyny EDPB 1/2022 k právům subjektů údajů – právo na přístup a Pokyny EDPB 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky.
[58] WP258, Stanovisko k některým klíčovým otázkám směrnice o prosazování práva (EU 2016/680).

omezení v případě, že se technologie rozpoznávání obličeje používá pro všechna ověření kromě ověření 1 : 1 v přímém kontaktu se subjektem údajů).

3.2.4.1 Sdělení práv a informací subjektům údajů stručným, srozumitelným a snadno přístupným způsobem

85. Technologie rozpoznávání obličeje přináší určité výzvy k zajištění toho, aby subjekty údajů byly informovány, že jsou zpracovávány jejich biometrické údaje. Zvláště náročné je to v případě, že donucovací orgán analyzuje prostřednictvím technologie rozpoznávání obličeje videomateriál, který pochází od třetí strany nebo který poskytla třetí strana, protože donucovací orgán má jen malou možnost – a většinou žádnou – informovat subjekt údajů v době shromažďování (např. prostřednictvím cedule na místě). Jakýkoli videomateriál, který není relevantní pro vyšetřování (nebo účel zpracování), by měl být před nasazením jakéhokoli zpracování biometrických údajů vždy odstraněn nebo anonymizován (např. rozmazáním bez možnosti zpětného získání údajů), aby se předešlo riziku nesplnění zásady minimalizace uvedené v čl. 4 odst. 1 písm. e) směrnice o prosazování práva a informačních povinností uvedených v čl. 13 odst. 2 směrnice o prosazování práva. Je povinností správce posoudit, jaké informace asi budou důležité pro subjekt údajů při výkonu jeho práv, a zajistit, aby byly poskytnuty nezbytné informace. Účinný výkon práv subjektu údajů závisí na tom, zda správce plní své informační povinnosti.

86. Článek 13 odst. 1 směrnice o prosazování práva stanoví, jaké minimální informace musí být subjektu údajů obecně poskytnuty. Tyto informace mohou být poskytovány prostřednictvím webových stránek správce, v tištěné podobě (např. leták dostupný na vyžádání) nebo z jiných, pro subjekt údajů snadno dostupných zdrojů. Správce údajů musí v každém případě zajistit, aby byly účinně poskytovány informace týkající se alespoň následujících prvků:

- údaje o totožnosti a kontaktní údaje správce, včetně pověřence pro ochranu osobních údajů,
- účel zpracování a že zpracování probíhá prostřednictvím technologie rozpoznávání obličeje,
- právo podat stížnost u příslušného dozorovému úřadu a kontaktní údaje tohoto úřadu,
- právo požadovat přístup k osobním údajům, jejich opravu nebo výmaz anebo omezení jejich zpracování.

87. Kromě toho v konkrétních případech vymezených ve vnitrostátním právu, které by měly být v souladu s čl. 13 odst. 2 směrnice o prosazování práva[59], jako například zpracování založené na technologii rozpoznávání obličeje, musí být subjektu údajů přímo poskytnuty tyto informace:

- právní základ zpracování,
- informace o tom, kde osobní údaje sebrány bez vědomí subjektu údajů,
- doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby,
- případné kategorie příjemců osobních údajů (včetně příjemců ve třetích zemích nebo v mezinárodních organizacích).

88. Zatímco čl. 13 odst. 1 směrnice o prosazování práva se týká obecných informací zpřístupňovaných veřejnosti, čl. 13 odst. 2 směrnice o prosazování práva se týká dodatečných informací, které mají být poskytnuty konkrétnímu subjektu údajů ve zvláštních případech, například pokud jsou údaje

[59] Např. § 56 odst. 1 německého spolkového zákona o ochraně osobních údajů, který mimo jiné stanoví, jaké informace je třeba poskytnout subjektům údajů při tajných operacích.

shromažďovány přímo od subjektu údajů nebo nepřímo bez jeho vědomí[60]. V čl. 13 odst. 2 směrnice o prosazování práva neexistuje jasná definice toho, co se rozumí „zvláštními případy". Odkazuje však na situace, kdy musí být subjekty údajů informovány o zpracování, které se jich osobně konkrétně týká, a musí jim být poskytnuty odpovídající informace, aby mohly účinně vykonávat svá práva. EDPB se domnívá, že při posuzování toho, zda nastal „zvláštní případ", je třeba vzít v úvahu několik faktorů, včetně toho, zda jsou osobní údaje shromažďovány bez vědomí subjektu údajů, neboť by to pak byl jediný způsob, jak umožnit subjektům údajů účinně vykonávat svá práva. Další příklady „zvláštních případů" by mohly nastat, pokud by byly osobní údaje dále zpracovávány v rámci postupu mezinárodní trestní spolupráce nebo v situaci, kdy jsou osobní údaje zpracovávány v rámci tajných operací, jak je stanoveno ve vnitrostátních právních předpisech. Z 38. bodu odůvodnění směrnice o prosazování práva dále vyplývá, že pokud se rozhodování provádí výhradně na základě technologie rozpoznávání obličeje, je třeba subjekty údajů informovat o prvcích automatizovaného rozhodování. To by rovněž naznačovalo, že se jedná o zvláštní případ, kdy by subjektu údajů měly být poskytnuty dodatečné informace v souladu s čl. 13 odst. 2 směrnice o prosazování práva[61].

89. V neposlední řadě je třeba poznamenat, že podle čl. 13 odst. 3 směrnice o prosazování práva mohou členské státy přijmout legislativní opatření, která omezují povinnost poskytovat informace ve zvláštních případech a při sledování určitých cílů. To platí v takovém rozsahu a na takovou dobu, jak je to v demokratické společnosti s náležitým přihlédnutím k základním právům a oprávněným zájmům dotčeného subjektu údajů nezbytné a přiměřené.

3.2.4.2 Právo na přístup

90. Subjekt údajů má obecně právo obdržet kladné nebo záporné potvrzení o jakémkoli zpracování svých osobních údajů, a pokud je odpověď kladná, přístup k osobním údajům jako takovým, jakož i další informace uvedené v článku 14 směrnice o prosazování práva. Pokud jde o technologii rozpoznávání obličeje, pokud jsou biometrické údaje uloženy a spojeny s totožností také pomocí alfanumerických údajů, mělo by to příslušnému orgánu umožnit vydat potvrzení žádosti o přístup na základě vyhledávání podle těchto alfanumerických údajů a bez zahájení dalšího zpracování biometrických údajů jiných osob (tj. vyhledávání pomocí technologie rozpoznávání obličeje v databázi). Musí být dodržena zásada minimalizace údajů a nemělo by být uchováváno více údajů, než je nezbytné s ohledem na účel zpracování.

3.2.4.3 Právo na opravu osobních údajů

91. Vzhledem k tomu, že technologie rozpoznávání obličeje nezajišťuje absolutní přesnost, je obzvláště důležité, aby správci pozorně sledovali žádosti o opravu osobních údajů. Může se také jednat o případ, kdy byl subjekt údajů na základě technologie rozpoznávání obličeje zařazen do nesprávné kategorie, např. byl neoprávněně zařazen do kategorie podezřelých na základě původního předpokladu o postupu na videozáznamu. Rizika pro subjekty údajů jsou obzvláště závažná, pokud jsou tyto nepřesné údaje uloženy v policejní databázi a/nebo sdíleny s jinými subjekty. Správce musí odpovídajícím způsobem opravit uchovávané údaje a systémy založené na technologii rozpoznávání obličeje, viz 47. bod odůvodnění směrnice o prosazování práva.

[60] WP258, Stanovisko k některým klíčovým otázkám směrnice o prosazování práva (EU 2016/680), s. 17–18.

[61] Všimněte si rozdílu mezi slovy „poskytované subjektu údajů" (made available to the data subject) v čl. 13 odst. 1 směrnice o prosazování práva a „poskytne subjektu údajů" (give to the data subject) v čl. 13 odst. 2 směrnice o prosazování práva. V čl. 13 odst. 2 směrnice o prosazování práva musí správce zajistit, aby se informace dostaly k subjektu údajů, přičemž informace zveřejněné na internetových stránkách nebudou dostatečné.

3.2.4.4 Právo na výmaz

92. Technologie rozpoznávání obličeje bude za většiny okolností – v případě, že se nebude používat pro ověřování/autentizaci 1 : 1 – představovat zpracování velkého počtu biometrických údajů subjektů údajů. Je proto důležité, aby správce předem zvážil, kam až mu účel a nezbytnost umožňuje zajít, aby žádost o výmaz v souladu s článkem 16 směrnice o prosazování práva mohla být vyřízena bez zbytečného odkladu (protože správce musí mimo jiné vymazat osobní údaje, které jsou zpracovávány nad rámec toho, co umožňují platné právní předpisy v návaznosti na články 4, 8 a 10 směrnice o prosazování práva).

3.2.4.5 Právo na omezení

93. V případě, že subjekt údajů napadne přesnost údajů a tuto přesnost nelze ověřit (nebo pokud musí být osobní údaje uchovávány pro účely budoucího využití jako důkazu), má správce povinnost omezit osobní údaje tohoto subjektu údajů v souladu s článkem 16 směrnice o prosazování práva. To je obzvláště důležité, pokud jde o technologii rozpoznávání obličeje (založenou na algoritmu (algoritmech), a tedy nikdy nevykazující konečný výsledek) v situacích, kdy se shromažďuje velké množství údajů a přesnost a kvalita identifikace se může lišit. U videomateriálu nízké kvality (např. z místa činu) se zvyšuje riziko falešně pozitivních výsledků. Kromě toho, pokud snímky obličeje v seznamu zájmových osob nejsou pravidelně aktualizovány, i to zvyšuje riziko falešně pozitivních nebo falešně negativních výsledků. Ve zvláštních případech, kdy údaje nelze vymazat, protože existují oprávněné důvody se domnívat, že by výmaz mohl poškodit oprávněné zájmy subjektu údajů, by měly být údaje místo toho omezeny a zpracovávány pouze pro účel, který brání jejich výmazu (viz 47. bod odůvodnění směrnice o prosazování práva).

3.2.4.6 Legitimní omezení práv subjektu údajů

94. Pokud jde o informační povinnosti správce a právo subjektů údajů na přístup, jsou omezení přípustná pouze tehdy, pokud jsou stanovena zákonem, který musí představovat nezbytné a přiměřené opatření v demokratické společnosti s náležitým přihlédnutím k základním právům a oprávněným zájmům dotčené fyzické osoby (viz čl. 13 odst. 3 a 4, článek 15 a čl. 16 odst. 4 směrnice o prosazování práva). Pokud se technologie rozpoznávání obličeje používá pro účely prosazování práva, lze očekávat, že bude používána za okolností, kdy by to bylo v rozporu se sledovaným účelem informovat subjekt údajů nebo umožnit přístup k údajům. To by platilo například pro policejní vyšetřování trestného činu nebo na ochranu národní nebo veřejné bezpečnosti.

95. Právo na přístup neznamená automaticky přístup ke všem informacím, např. v trestním řízení, kde se vyskytují osobní údaje. Příklad toho, kdy by bylo schůdné povolit omezení tohoto práva, by mohl nastat v průběhu vyšetřování trestného činu.

3.2.4.7 Výkon práv prostřednictvím dozorového úřadu

96. V případech, kdy jsou omezení výkonu práv legitimní podle kapitoly III směrnice o prosazování práva, může subjekt údajů požádat úřad pro ochranu osobních údajů, aby uplatnil svá práva jeho jménem, a to kontrolou zákonnosti zpracování údajů správcem. Je povinností správce informovat subjekt údajů o možnosti vykonávat svá práva tímto způsobem (viz článek 17 směrnice o prosazování práva a čl. 46 odst. 1 písm. g) směrnice o prosazování práva). V případě využívání technologie rozpoznávání obličeje to znamená, že správce musí zajistit vhodná opatření, aby bylo možné takovou žádost vyřídit, např. umožnit vyhledávání v zaznamenaném materiálu za předpokladu, že subjekt údajů poskytne dostatečné informace, aby bylo možné najít jeho osobní údaje.

3.2.5 Další právní požadavky a záruky

3.2.5.1 Článek 27 Posouzení vlivu na ochranu osobních údajů

97. Posouzení vlivu na ochranu osobních údajů (DPIA) před použitím technologie rozpoznávání obličeje je povinným požadavkem, protože tento druh zpracování, zejména s využitím nových technologií a s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování, může mít za následek vysoké riziko pro práva a svobody fyzických osob. Vzhledem k tomu, že používání technologie rozpoznávání obličeje zahrnuje systematické automatizované zpracování zvláštních kategorií údajů, lze předpokládat, že v takových případech bude správce zpravidla povinen provést posouzení vlivu na ochranu osobních údajů. Posouzení vlivu na ochranu osobních údajů by mělo obsahovat alespoň obecný popis zamýšlených operací zpracování, posouzení nezbytnosti a přiměřenosti operací zpracování ve vztahu k účelům, posouzení rizik z hlediska práv a svobod subjektů údajů, plánovaná opatření k řešení těchto rizik, záruky, bezpečnostní opatření a mechanismy k zajištění ochrany osobních údajů a k doložení souladu. EDPB doporučuje zveřejnit výsledky těchto posouzení nebo alespoň hlavní zjištění a závěry posouzení vlivu na ochranu osobních údajů jako opatření, které má posílit důvěru a transparentnost[62].

3.2.5.2 Článek 28 Předchozí konzultace dozorového úřadu

98. Podle článku 28 směrnice o prosazování práva musí správce nebo zpracovatel před zpracováním konzultovat s dozorovým úřadem, pokud: a) z posouzení vlivu na ochranu osobních údajů vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika, nebo b) že druh zpracování, zejména při využití nových technologií, mechanismů nebo postupů, s sebou nese vysoké riziko pro práva a svobody subjektů údajů. Jak již bylo vysvětleno v oddíle 2.3 těchto pokynů, EDPB se domnívá, že většina případů zavádění a používání technologie rozpoznávání obličeje obsahuje inherentní vysoké riziko pro práva a svobody subjektů údajů. Proto by kromě posouzení vlivu na ochranu osobních údajů měl orgán, který technologii rozpoznávání obličeje zavádí, před zavedením systému konzultovat s příslušným dozorovým úřadem.

3.2.5.3 Článek 29 Zabezpečení zpracování

99. Jedinečná povaha biometrických údajů znemožňuje subjektu údajů, aby je v případě narušení změnil, např. v důsledku porušení zabezpečení údajů. Příslušný orgán, který zavádí a/nebo používá technologii rozpoznávání obličeje, by měl věnovat zvláštní pozornost zabezpečení zpracování v souladu s článkem 29 směrnice o prosazování práva. Donucovací orgán by měl zejména zajistit, aby systém odpovídal příslušným normám, a zavést opatření na ochranu biometrických šablon[63]. Tato povinnost je o to důležitější, pokud donucovací orgán využívá poskytovatele služeb třetí strany (zpracovatele údajů).

3.2.5.4 Článek 20 Záměrná a standardní ochrana osobních údajů

100. Cílem záměrné a standardní ochrany osobních údajů v souladu s článkem 20 směrnice o prosazování práva je zajistit, aby zásady a záruky ochrany osobních údajů, jako je minimalizace údajů a omezení jejich uchovávání, byly do dané technologie začleněny prostřednictvím vhodných technických a organizačních opatření, jako je pseudonymizace, a to i před zahájením zpracování osobních údajů, a aby byly uplatňovány po celou dobu jejího životního cyklu. Vzhledem k inherentnímu vysokému riziku pro práva a svobody fyzických osob by volba takových opatření neměla záviset výlučně na ekonomických hlediscích[64], ale místo toho je třeba usilovat o zavedení nejmodernějších technologií v oblasti ochrany údajů. Ve stejném duchu platí, že pokud donucovací orgán hodlá uplatňovat a využívat technologii rozpoznávání obličeje od externích poskytovatelů, musí například prostřednictvím

[62] Více informací naleznete v dokumentu WP248 rev.01 Pokyny pro posouzení vlivu na ochranu osobních údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“.
[63] Viz například: ISO/IEC 24745 Informační technologie, kybernetická bezpečnost a ochrana soukromí – Ochrana biometrických informací.
[64] Viz 53. bod odůvodnění směrnice o prosazování práva.

zadávacího řízení zajistit, aby byly zavedeny pouze technologie rozpoznávání obličeje založené na zásadách záměrné a standardní ochrany údajů[65]. To rovněž znamená, že transparentnost fungování technologie rozpoznávání obličeje není omezena požadavky týkajícími se obchodního tajemství nebo právy duševního vlastnictví.

3.2.5.5 Článek 25 Vedení logů

101. Směrnice o prosazování práva stanoví různé metody prokazování zákonnosti zpracování správcem nebo zpracovatelem a zajištění neporušenosti a zabezpečení údajů. V tomto ohledu jsou systémové logy velmi užitečným nástrojem a důležitou zárukou pro ověřování zákonnosti zpracování, a to jak interně (tj. vlastní kontrola), tak ze strany externích dozorových úřadů, jako jsou úřady pro ochranu osobních údajů. Podle článku 25 směrnice o prosazování práva by měly být v systémech automatizovaného zpracování vedeny logy alespoň pro následující operace zpracování: shromáždění, pozměnění, nahlédnutí, sdělení, včetně předání, zkombinování a výmaz. Logy o nahlédnutí a sdělení by navíc měly umožňovat zjištění důvodů těchto operací, datum a čas, kdy byly učiněny, a je-li to možné, totožnost osoby, která do osobních údajů nahlédla nebo která je zpřístupnila, a totožnost příjemců těchto osobních údajů. Dále se v souvislosti se systémy rozpoznávání obličeje doporučuje vedení logů následujících dalších operací zpracování (částečně nad rámec článku 25 směrnice o prosazování práva):

- změny referenční databáze (doplnění, výmaz nebo aktualizace). Log by měl uchovávat kopii příslušného (doplněného, vymazaného nebo aktualizovaného) snímku, pokud není jinak možné ověřit zákonnost nebo výsledek operací zpracování,
- pokusy o identifikaci nebo ověření, včetně výsledku a míry jistoty. Měla by důsledně platit zásada minimalizace tak, aby se namísto uchovávání referenčního snímku uchovával v lozích pouze identifikátor snímku z referenční databáze. Je třeba se vyhýbat vedení logů vstupních biometrických údajů, pokud to není nezbytné (např. pouze v případech shody),
- identifikační číslo uživatele, který požádal o pokus o identifikaci nebo ověření,
- veškeré osobní údaje uložené v lozích systémů podléhají přísným účelovým omezením (např. audity) a neměly by být používány k jiným účelům (např. aby bylo možné nadále provádět rozpoznávání/ověřování včetně snímku, který byl vymazán z referenčních databází). Měla by být použita bezpečnostní opatření k zajištění neporušenosti logů, přičemž se důrazně doporučují automatické monitorovací systémy k odhalení zneužití logů. Pokud jde o logy referenční databáze, měla by být bezpečnostní opatření rovnocenná referenční databázi v případě uchovávání snímků obličeje. Rovněž by měly být zavedeny automatické procesy, které zajistí dodržování doby uchovávání údajů v případě logů.

3.2.5.6 Článek 4 odst. 4 Odpovědnost

102. Správce musí být schopen doložit soulad zpracování se zásadami uvedenými v čl. 4 odst. 1 až 3, srov. čl. 4 odst. 4 směrnice o prosazování práva. V tomto ohledu je zásadní systematická a aktuální dokumentace systému (včetně aktualizací, modernizací a zaškolení algoritmu), technických a organizačních opatření (včetně monitorování výkonnosti systému a možného lidského zásahu) a zpracování osobních údajů. Pro doložení zákonnosti zpracování je zvláště důležitým prvkem vedení logů podle článku 25 směrnice o prosazování práva (viz oddíl 3.2.5.5). Zásada odpovědnosti se vztahuje nejen na systém a zpracování, ale také na dokumentaci procesních záruk, jako jsou posouzení

[65] Další informace naleznete v Pokynech EDPB o záměrné a standardní ochraně osobních údajů, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

nezbytnosti a přiměřenosti, posouzení vlivu na ochranu osobních údajů, jakož i interní konzultace (např. schválení projektu vedením nebo interní rozhodnutí o hodnotách míry jistoty) a externí konzultace (např. úřad pro ochranu osobních údajů). Řada prvků, které jsou v tomto ohledu relevantní, je uvedena v příloze II.

3.2.5.7 Článek 47 Účinný dohled

103. Účinný dohled ze strany příslušných úřadů pro ochranu osobních údajů je jednou z nejdůležitějších záruk, pokud jde o základní práva a svobody jednotlivců dotčených používáním technologie rozpoznávání obličeje. Vybavení nezbytnými lidskými, technickými a finančními zdroji, prostorami a infrastrukturou každého dozorového úřadu pro ochranu osobních údajů je nezbytným předpokladem pro účinné plnění jeho úkolů a výkon jeho pravomocí[66]. Ještě důležitější než počet dostupných zaměstnanců jsou dovednosti odborníků, které by měly pokrývat velmi širokou tematickou škálu – od vyšetřování trestných činů a policejní spolupráce až po analýzu dat velkého objemu a umělou inteligenci. Členské státy by proto měly zajistit, aby zdroje dozorových úřadů byly přiměřené a dostatečné k tomu, aby jim umožnily vykonávat jejich mandát chránit práva subjektů údajů a bedlivě sledovat veškerý vývoj v tomto ohledu.[67]

4 ZÁVĚR

104. Používání technologií rozpoznávání obličeje je neodmyslitelně spojeno se zpracováním značného množství osobních údajů, včetně zvláštních kategorií údajů. Obličej a obecněji biometrické údaje jsou trvalou a nedílnou součástí totožnosti osoby. Používání rozpoznávání obličeje má proto přímý nebo nepřímý dopad na řadu základních práv a svobod zakotvených v Listině základních práv EU, které mohou překračovat rámec ochrany soukromí a osobních údajů, jako je lidská důstojnost, svoboda pohybu, svoboda shromažďování a další. To je obzvláště důležité v oblasti prosazování práva a trestního soudnictví.

105. EDPB chápe, že donucovací orgány mají potřebu využívat co nejlepší nástroje k rychlému identifikování pachatelů teroristických a dalších závažných trestných činů. Tyto nástroje by však měly být používány důsledně v souladu s platným právním rámcem a pouze v případech, kdy splňují požadavky nezbytnosti a přiměřenosti, jak je stanoveno v čl. 52 odst. 1 Listiny. Navíc ačkoli moderní technologie mohou být součástí řešení, v žádném případě nepředstavují „všelék“.

106. Existují určité případy použití technologií rozpoznávání obličeje, které představují nepřijatelně vysoké riziko pro jednotlivce a společnost („červené linie“). Z těchto důvodů EDPB a EIOÚ vyzvali k jejich všeobecnému zákazu[68].

107. Zejména biometrická identifikace osob na veřejně přístupných místech na dálku představuje vysoké riziko zásahu do soukromého života jednotlivců a nemá místo v demokratické společnosti, protože ze své podstaty znamená hromadné sledování. Ve stejném duchu se EDPB domnívá, že systémy rozpoznávání obličeje podporované umělou inteligencí zařazující jednotlivce na základě jejich

[66] Viz sdělení Komise „První zpráva o uplatňování a fungování směrnice (EU) o prosazování práva v oblasti ochrany údajů 2016/680 („směrnice o prosazování práva“)“, COM(2022) 364 final, s. 3.4.1.
[67] Viz Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62 (Příspěvek EDPB k hodnocení Evropské komise týkajícímu se směrnice o prosazování práva v oblasti ochrany údajů podle článku 62), bod 14, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf.
[68] Viz EDPB-EIOÚ Společné stanovisko 5/2021 k návrhu nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci) https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

biometrických údajů do skupin podle etnického původu, pohlaví, jakož i politické nebo sexuální orientace, jsou neslučitelné s Listinou. Kromě toho je EDPB přesvědčen, že používání rozpoznávání obličeje nebo podobných technologií k odvozování emocí fyzických osob je vysoce nežádoucí a mělo by být zakázáno, případně s několika řádně odůvodněnými výjimkami. Kromě toho se EDPB domnívá, že zpracování osobních údajů v kontextu prosazování práva, které by se opíralo o databázi zaplněnou hromadným a nevybíravým shromažďováním osobních údajů, např. „scrapingu“ fotografií a snímků obličejů dostupných na internetu, zejména těch, které jsou zpřístupněny prostřednictvím sociálních sítí, by z podstaty nesplňovalo požadavek naprosté nezbytnosti stanovený právem Unie.

5 PŘÍLOHY

Příloha I: Podpůrný vzor

Příloha II: Praktické pokyny pro řízení projektů zahrnujících technologii rozpoznávání obličeje v rámci donucovacích orgánů

Příloha III: Praktické příklady

PŘÍLOHA I – VZOR PRO POPIS SCÉNÁŘŮ

(S informativními rámečky pro aspekty řešené v rámci daného scénáře)

Popis zpracování:

- Popis zpracování, kontext (souvislost s trestným činem), účel

Zdroj informací:

- Typy subjektů údajů: ☐ všichni občané ☐ odsouzení ☐ podezřelí
  ☐ děti ☐ jiné zranitelné subjekty údajů
- Zdroj snímku: ☐ veřejně přístupné prostory ☐ internet
  ☐ soukromý subjekt ☐ jiné fyzické osoby ☐ jiný .....
- Souvislost s trestnou činností: ☐ je přímá časová ☐ není přímá časová
  ☐ je přímá zeměpisná ☐ není přímá zeměpisná
  ☐ není nutná
- Způsob zachycení informací: ☐ na dálku ☐ v kabině nebo kontrolovaném prostředí
- Kontext – dopad na jiná základní práva:
  ☐ ne
  ano, konkrétně na ☐ svobodu shromažďování
  ☐ na svobodu projevu
  ☐ různé:.....
- Možnosti dalších zdrojů informací o subjektu údajů:
  ☐ doklad totožnosti ☐ používání veřejného telefonu ☐ registrační značka vozidla
  ☐ jiné .....

Referenční databáze (s níž se porovnávají zachycené informace):

- Specifičnost: ☐ databáze pro obecné účely ☐ specifické databáze týkající se určité oblasti trestné činnosti
- Popis zaplňování těchto referenčních databází (a právní základ)
- Změna účelu databáze (např. primárním cílem bylo zabezpečení soukromého majetku): ☐ ANO
  ☐ NE

Algoritmus:

- Typ zpracování: ☐ ověření (autentizace) 1 : 1 ☐ identifikace 1 : více.
- Úvahy týkající se přesnosti
- Technické záruky

Výsledek:

- Dopad ☐ přímý (např. subjekt údajů může být zatčen, vyslýchán, diskriminační chování)
  ☐ nepřímý (používá se pro statistické modely, bez závažných právních kroků proti subjektům údajů)

- Automatizované rozhodnutí: ☐ ANO ☐ NE
- Doba uchovávání

Právní analýza:

- Analýza nezbytnosti a přiměřenosti – účel/závažnost trestného činu / počet osob, které nejsou zapojeny, ale jsou zpracováním dotčeny
- Druh předchozího informování subjektu údajů: ☐ při vstupu do konkrétní oblasti
  ☐ na internetových stránkách donucovacího orgánu obecně
  ☐ na internetových stránkách donucovacího orgánu pro zvláštní zpracování
  ☐ jiné .....
- Platný právní rámec:
  ☐ směrnice o prosazování práva z větší části zkopírována do vnitrostátního práva
  ☐ obecné vnitrostátní právní předpisy pro používání biometrických údajů donucovacími orgány
  ☐ zvláštní vnitrostátní právní předpisy pro toto zpracování (rozpoznávání obličeje) pro tento příslušný orgán
  ☐ zvláštní vnitrostátní právní předpisy pro toto zpracování (automatizované rozhodování)

Závěr:

Obecné úvahy o tom, zda je pravděpodobné, že popsané zpracování je slučitelné s právem EU (a některé odkazy na právní podmínky)

PŘÍLOHA II – PRAKTICKÉ POKYNY PRO ŘÍZENÍ PROJEKTŮ ZAHRNUJÍCÍCH TECHNOLOGII ROZPOZNÁVÁNÍ OBLIČEJE V RÁMCI DONUCOVACÍCH ORGÁNŮ

Tato příloha obsahuje některé další praktické pokyny pro donucovací orgány, které plánují zahájit projekt zahrnující technologii rozpoznávání obličeje. Poskytuje více informací o organizačních a technických opatřeních, která je třeba zvážit při zavádění projektu, a neměla by být považována za vyčerpávající seznam kroků/opatření, která je třeba přijmout. Je třeba ji číst ve spojení s pokyny EDPB 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky[69] a s veškerými nařízeními EU/EHP a pokyny EDPB týkajícími se používání umělé inteligence.

Tato příloha obsahuje pokyny vycházející z předpokladu, že donucovací orgány budou pořizovat technologii rozpoznávání obličeje (jako komerčně dostupné produkty). Pokud donucovací orgán plánuje vyvinout (dále vyškolit) technologii rozpoznávání obličeje, platí dodatečné požadavky na výběr nezbytných datových souborů pro školení, validaci a testování, které se uplatní během vývoje, a na role/opatření pro vývojové prostředí. Podobně může i komerčně dostupný produkt vyžadovat další úpravy pro zamýšlené použití, přičemž v takovém případě by měly být splněny výše uvedené požadavky na výběr datových souborů pro testování, validaci a školení.

Příslušnost k témuž donucovacímu orgánu sama o sobě neposkytuje plný přístup k biometrickým údajům. Stejně jako u jiných kategorií osobních údajů nelze biometrické údaje shromážděné pro určitý účel prosazování práva na základě konkrétního právního základu použít bez řádného právního základu pro jiný účel prosazování práva (čl. 4 odst. 2 směrnice (EU) 2016/680 (směrnice o prosazování práva)). Vývoj/školení nástroje založeného na technologii rozpoznávání obličeje jsou rovněž považovány za jiný účel a mělo by být posouzeno, zda zpracování biometrických údajů za účelem měření výkonnosti / výcviku technologie, aby se zabránilo dopadu nízké výkonnosti na subjekty údajů, je nezbytné a přiměřené s ohledem na původní účel zpracování.

1. ÚLOHY A POVINNOSTI

Pokud donucovací orgán využívá technologii rozpoznávání obličeje k plnění svých úkolů spadajících do oblasti působnosti směrnice o prosazování práva (prevence, vyšetřování, odhalování či stíhání trestných činů atd., podle článku 3 směrnice o prosazování práva), může být považována za správce technologie rozpoznávání obličeje. Donucovací orgány se však skládají z několika jednotek/oddělení, které mohou být do tohoto zpracování zapojeny, a to buď určením procesů využívajících technologie rozpoznávání obličeje, nebo jejím využíváním v praxi. Vzhledem ke zvláštnostem této technologie může být nutné zapojit různé jednotky, aby buď poskytovaly podporu při měření výkonnosti technologii, nebo aby jí poskytly další školení.

Do projektu zahrnujícím technologii rozpoznávání obličeje může být nutné zapojit několik zúčastněných stran[70] v rámci donucovacích orgánů:

[69] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[70] Následující úlohy ukazují různé zúčastněné strany a jejich povinnosti v rámci projektu využívajícího technologii rozpoznávání obličeje. I když formulace použité k popisu rolí v této příloze nejsou preskriptivní, každý donucovací orgán musí definovat a přidělit podobné role podle okolností své organizace. Může se stát, že jedna jednotka

- Nejvyšší vedení – schvaluje projekt po zvážení rizik s ohledem na potenciální přínosy.
- Pověřenec pro ochranu osobních údajů a/nebo právní oddělení donucovacího orgánu – pomáhá při posuzování zákonnosti provádění určitého projektu využívajícího technologii rozpoznávání obličeje, pomáhá při provádění posouzení vlivu na ochranu osobních údajů, zajišťuje dodržování a výkon práv subjektů údajů.
- Vlastník procesu – působí jako konkrétní jednotka v rámci příslušného donucovacího orgánu, která rozvíjí projekt, rozhoduje o podrobnostech projektu využívajícího technologii rozpoznávání obličeje, včetně požadavků na výkonnost systému; rozhoduje o vhodné metrice měření korektnosti; stanovuje míru jistoty[71]; stanovuje přijatelné prahové hodnoty pro předpojatost; identifikuje potenciální rizika, která projekt využívající technologii rozpoznávání obličeje představuje pro práva a svobody jednotlivců (také na základě konzultace s pověřencem pro ochranu osobních údajů a oddělením IT zabývajícím se UI a/nebo datovou vědou (viz níže)) a předkládá je vrcholnému vedení. Vlastník procesu před rozhodnutím o podrobnostech projektu využívajícím technologii rozpoznávání obličeje rovněž konzultuje správce referenční databáze, aby pochopil jak účel používání referenční databáze, tak i její technické podrobnosti. V případě přeškolení pořízené technologie rozpoznávání obličeje bude vlastník procesu rovněž zodpovědný za výběr datových souboru pro školení. Za provedení posouzení vlivu na ochranu osobních údajů je odpovědný vlastník procesu jako jednotka pověřená vypracováním podrobností projektu a rozhodováním o nich.
- Oddělení IT zabývající se UI a/nebo datovou vědou – pomáhá při provádění posouzení vlivu na ochranu osobních údajů; vysvětluje dostupnou metriku pro měření výkonnosti systému, jeho korektnosti[72] a možné předpojatosti; zavádí technologii a technické záruky, aby se zabránilo neoprávněnému přístupu ke shromážděným údajům, kybernetickým útokům atd. V případě změny výcviku pořízené technologie rozpoznávání obličeje provede oddělení IT zabývající se UI a/nebo datovou vědou školení systému na základě datového souboru pro výcvik poskytnutého vlastníkem procesu. Toto oddělení bude rovněž pověřeno stanovením opatření ke zmírnění rizik, která společně identifikovali vlastníci procesů (např. rizika specifická pro UI, jako jsou útoky na model za účelem dovození informací (inference attack)).
- Koncoví uživatelé (např. policisté v terénu nebo ve forenzních laboratořích) – provádějí porovnání s databází; kriticky přezkoumávají výsledky s ohledem na předchozí důkazy a poskytují zpětnou vazbu vlastníkovi procesu, pokud jde o falešně pozitivní výsledky a náznaky možné diskriminace.
- Správce referenční databáze – zvláštní jednotka v rámci příslušného donucovacího orgánu, která má na starosti shromažďování a správu referenční databáze, tj. databáze, s níž budou snímky porovnávány, včetně mazání snímků obličeje po uplynutí stanovené doby uchovávání. Tato databáze může být vytvořena speciálně pro zamýšlený projekt využívající technologii rozpoznávání obličeje nebo se může jednat o již existují databázi pro slučitelné účely. Správce referenční databáze je odpovědný za stanovení toho, kdy a za jakých okolností lze snímky obličeje uchovávat, jakož i za stanovení jejich požadavků na uchovávání údajů (podle časových nebo jiných kritérií).

Vzhledem k tomu, že většina případů zavádění a používání služby technologie rozpoznávání obličeje obnáší vysoké inherentní riziko pro práva a svobody subjektů údajů, měl by být rovněž zapojen

kumuluje více než jednu roli, například vlastníka procesu a správce referenční databáze nebo vlastníka procesu a oddělení IT zabývajícího se UI a/nebo datovou vědou (v případě, že jednotka vlastníka procesu má všechny potřebné technické znalosti).

[71] Mírou jistoty se rozumí úroveň jistoty predikce (shody) ve formě pravděpodobnosti. Např. při porovnání dvou šablon je 90% jistota, že patří stejné osobě. Míra jistoty se liší od výkonnosti technologie porovnávání obličeje, ale má na výkonnost vliv. Čím vyšší je prahová hodnota jistoty, tím méně je ve výsledcích technologie rozpoznávání obličeje falešně pozitivních a více falešně negativních shod.

[72] Korektnost lze definovat jako nedostatek nekalé, protiprávní diskriminace, jako je předpojatost na základě pohlaví nebo rasy.

dozorový úřad pro ochranu osobních údajů v rámci předchozí konzultace požadované v článku 28 směrnice o prosazování práva.

2. POČÁTEK / PŘED POŘÍZENÍM SYSTÉMU VYUŽÍVAJÍCÍHO TECHNOLOGII ROZPOZNÁVÁNÍ OBLIČEJE

Vlastník procesu v donucovacím orgánu by měl mít nejprve jasnou představu o postupu či postupech, kterými se řídí použití nástroje využívajícího technologii rozpoznávání obličeje (případ či případy použití), a zajistit, aby existoval právní základ pro odůvodnění případu zamýšleného použití. Na základě toho musí:

- Formálně popsat případ použití. Je třeba popsat problém, který je nutné vyřešit, a způsob, jakým technologie rozpoznávání obličeje poskytne řešení, jakož i přehled procesu (úkolu), v němž bude technologie používána. V tomto ohledu by donucovací orgány měly zdokumentovat alespoň[73]:
  - Kategorie osobních údajů zaznamenaných v rámci procesu
  - Cíle a konkrétní účely, pro které bude technologie rozpoznávání obličeje použita, včetně možných důsledků pro subjekt údajů po nalezení shody.
  - Kdy a jak budou snímky obličeje shromažďovány (včetně informací o kontextu tohoto shromažďování, např. u letištní brány, videozáznamy z bezpečnostních kamer před obchodem, kde byl spáchán trestný čin, atd., a kategorií subjektů údajů, jejichž biometrické údaje budou zpracovávány).
  - Databáze, s níž budou snímky porovnávány (referenční databáze), jakož i informace o tom, jak byla vytvořena, o její velikosti a kvalitě biometrických údajů, které obsahuje.
  - Donucovací orgány, které budou oprávněny používat systém využívající technologii rozpoznávání obličeje a jednat na základě takto získaných informací v kontextu prosazování práva (jejich profily a přístupová práva musí definovat vlastník procesu).
  - Předpokládaná doba uchovávání vstupních údajů nebo okamžik, který určí konec této doby (například uzavření nebo zastavení trestního řízení v souladu s vnitrostátním procesním právem, pro které byly původně shromážděny), jakož i případné následné kroky (vymazání těchto údajů, anonymizace a použití pro statistické nebo výzkumné účely atd.).
  - Vedení logů a dostupnost logů a uchovávaných záznamů.
  - Metriky výkonnosti (např. správnost, přesnost, odezva, skóre F1) a jejich minimální přijatelné prahové hodnoty.[74]
  - Odhad počtu osob, na které se technologie rozpoznávání obličeje použije, v jakém časovém období / při jaké příležitosti.

[73] Příloha I obsahuje seznam prvků, které pomohou správci popsat případ použití technologie rozpoznávání obličeje.

[74] Existují různé metriky pro hodnocení výkonnosti systému využívajícího technologii rozpoznávání obličeje. Každá metrika poskytuje odlišný pohled na výsledky systému a jeho úspěch při poskytování přiměřeného přehledu o tom, zda systém využívající technologii rozpoznávání obličeje funguje dobře, či nikoli, závisí na případu použití technologie rozpoznávání obličeje. Pokud se zaměříme na dosažení vysokých procentních podílů správného nalezení shody obličeje, lze použít metriku, jako je přesnost a odezva. Tyto metriky však neměří, jak dobře technologie rozpoznávání obličeje nakládá s negativními příklady (kolik z nich bylo systémem nesprávně přiřazeno). Vlastník procesu podporovaný oddělením IT zabývajícím se UI a/nebo datovou vědou by měl být schopen stanovit požadavky na výkonnost a vyjádřit je nejvhodnější metrikou podle případu použití technologie rozpoznávání obličeje.

- Provést posouzení nezbytnosti a přiměřenosti[75]. Skutečnost, že tato technologie existuje, by neměla být důvodem pro její použití. Vlastník procesu musí nejprve posoudit, zda existuje vhodný právní základ pro zamýšlené zpracování. Za tímto účelem je třeba konzultovat s pověřencem pro ochranu osobních údajů a právním oddělením. Hybnou silou pro zavádění technologie rozpoznávání obličeje by mělo být to, že se jedná o nezbytné a přiměřené řešení konkrétně definovaného problému donucovacích orgánů. To je třeba posoudit podle účelu/závažnosti trestného činu / počtu osob, které nejsou zapojeny, ale jsou ovlivněny systémem využívajícím technologii rozpoznávání obličeje. Pro posouzení zákonnosti je třeba vzít v úvahu alespoň následující skutečnosti: směrnici o prosazování práva[76], obecného nařízení o ochraně osobních údajů[77] [78], jakýkoliv stávající právní rámec pro umělou inteligenci[79] a všechny doprovodné pokyny poskytnuté dozorovými úřady pro ochranu osobních údajů (např. pokyny EDPB 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky[80]). Tyto akty právních předpisů EU by měly být vždy potvrzeny platnými vnitrostátními požadavky, zejména v oblasti trestního práva procesního. Posouzení přiměřenosti by mělo určit základní práva subjektů údajů, která mohou být dotčena (nad rámec ochrany soukromí a ochrany údajů). Mělo by rovněž popsat a zvážit veškerá omezení (nebo absence omezení) uložená v případě použití systému využívajícího technologii rozpoznávání obličeje. Například zda bude systém fungovat nepřetržitě nebo dočasně a zda bude omezen na určitou zeměpisnou oblast.
- Provést posouzení vlivu na ochranu osobních údajů [81]. Mělo by být provedeno posouzení vlivu na ochranu osobních údajů, neboť zavedení technologie zpracování obličeje v oblasti prosazování práva může mít za následek vysoké riziko pro práva a svobody jednotlivců[82]. Posouzení vlivu na ochranu osobních údajů by mělo obsahovat zejména: obecný popis zamýšlených operací

[75] Lze zvážit další kroky k zajištění nezbytnosti, pokud jde o přizpůsobení a používání systému, takže popis případu použití může být během posouzení nezbytnosti a přiměřenosti rovněž mírně pozměněn.

[76] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů.

[77] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

[78] V případech, kdy by vědecký projekt zaměřený na výzkum využívání technologie rozpoznávání obličeje musel zpracovávat osobní údaje, ale na takové zpracování by se nevztahovalo ustanovení čl. 4 odst. 3 směrnice o prosazování práva, obecně by bylo použitelné obecné nařízení o ochraně osobních údajů (čl. 9 odst. 2 směrnice o prosazování práva). V případě pilotních projektů, po nichž by následovaly operace v oblasti prosazování práva, by byla stále použitelná směrnice o prosazování práva.

[79] Existuje například návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, KTERÝM SE STANOVÍ HARMONIZOVANÁ PRAVIDLA PRO UMĚLOU INTELIGENCI (AKT O UMĚLÉ INTELIGENCI) A MĚNÍ URČITÉ LEGISLATIVNÍ AKTY UNIE, který však zatím nebyl přijat jako nařízení.

[80] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[81] Další pokyny k posouzení vlivu na ochranu osobních údajů naleznete zde: Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679, WP 248 rev.01, k dispozici na adrese: https://ec.europa.eu/newsroom/article29/items/611236 a v dokumentu EIOÚ Accountability on the ground toolkit (Nástroj pro odpovědnost v praxi), část II, k dispozici na adrese https://edps.europa.eu/node/4582_en.

[82] Na technologii rozpoznávání obličeje se mohou v závislosti na případu použití použít níže uvedená kritéria vedoucí ke zpracování s vysokým rizikem (z pokynů pro posouzení vlivu na ochranu údajů, WP 248 rev.01): Systematické monitorování, údaje zpracovávané v rozsáhlém měřítku, přiřazování nebo slučování datových souborů, nové použití nebo využití nových technologických nebo organizačních řešení.

zpracování[83], posouzení rizik z hlediska práv a svobod subjektů údajů[84], plánovaná opatření k řešení těchto rizik, záruky, bezpečnostní opatření a mechanismy k zajištění ochrany osobních údajů a k doložení souladu. Posouzení vlivu na ochranu osobních údajů je neustále probíhající proces, a proto by měly být doplňovány veškeré nové prvky zpracování a posouzení rizik by mělo být aktualizováno v každé fázi projektu.

- Získat souhlas vrcholného vedení tím, že vysvětlíte rizika pro práva a svobody subjektů údajů (na základě případu použití a technologie) a příslušné plány řešení rizik.

3. BĚHEM ZADÁVÁNÍ VEŘEJNÝCH ZAKÁZEK A PŘED NASAZENÍM TECHNOLOGIE ROZPOZNÁVÁNÍ OBLIČEJE

- Zvolit kritéria pro výběr technologie rozpoznávání obličeje (algoritmus). Vlastník procesu by měl rozhodnout o kritériích pro výběr algoritmu s pomocí oddělení IT zabývajícího se UI a/nebo datovou vědou. V praxi by tato kritéria zahrnovala měření korektnosti a měření výkonnosti, o nichž bylo rozhodnuto v popisu případu použití. Tato kritéria by měla zahrnovat také informace týkající se dat, na kterých byl algoritmus vyškolen. Aby se omezila předpojatost, musí soubor pro účely školení, testování a validace zahrnovat v dostatečné míře vzorky všech charakteristik subjektů údajů, na které má být technologie rozpoznávání obličej použita (například s ohledem na věk, pohlaví a rasu). Poskytovatel technologie rozpoznávání obličeje by měl poskytovat informace a metriky o datových souborech pro školení, testování a validaci technologie rozpoznávání obličeje a popsat opatření přijatá k měření a zmírnění potenciální protiprávní diskriminace a předpojatosti. Vlastník procesu musí pokud možno zkontrolovat, zda existoval právní základ pro to, aby poskytovatel použil tento datový soubor pro účely školení algoritmů (na základě informací, které poskytovatel zpřístupní). Vlastník procesu by měl rovněž zajistit, aby poskytovatel technologie rozpoznávání obličeje uplatňoval bezpečnostní normy týkající se biometrických údajů, jako je norma ISO/IEC 24745, která poskytuje pokyny pro ochranu biometrických informací v rámci různých požadavků na důvěrnost, neporušenost a obnovitelnost/odvolatelnost během uchovávání a předávání a požadavky a pokyny pro bezpečnou správu a zpracování biometrických informací v souladu s ochranou soukromí.

- Zajistit „přeškolení“ algoritmu (v případě potřeby). Vlastník procesu by měl zajistit, aby součástí pořizovaných služeb bylo rovněž doladění systému využívajícího technologie rozpoznávání obličeje za účelem dosažení vyšší přesnosti před použitím. V případě, že je pro splnění metrik přesnosti nutné dodatečné školení pořízeného systému využívajícího technologii rozpoznávání obličeje, musí vlastník procesu kromě rozhodnutí o přeškolení rozhodnout s pomocí oddělení IT zabývajícího se UI a/nebo datovou vědou o vhodném reprezentativním datovém souboru, který bude použit, a zkontrolovat zákonnost jeho použití.
- Nastavit vhodné záruky k ošetření rizik spojených se zabezpečením, předpojatostí a nízkou výkonností. To zahrnuje zavedení postupu pro sledování technologie rozpoznávání obličeje, jakmile bude zavedena (vedení logů a zpětná vazba pro přesnost a korektnost výsledků). Kromě toho zajistit, aby byla identifikována, měřena a zmírněna rizika, která jsou specifická pro některé

[83] Kromě posouzení rizik je součástí posouzení vlivu na ochranu osobních údajů také popis zpracování, jakož i posouzení nezbytnosti a přiměřenosti, jak již bylo popsáno ve výše uvedených krocích. V případě potřeby bude v posouzení vlivu na ochranu osobních údajů uveden podrobnější popis toků osobních údajů.

[84] Analýza rizik pro subjekty údajů by měla zahrnovat rizika související s místem pořízení snímku obličeje, který má být porovnáván (místní / na dálku), rizika týkající se zpracovatelů / dílčích zpracovatelů, jakož i rizika specifická pro strojové učení, pokud se použije (např. otrávení dat (data poisoning), příklady navržené tak, aby byly nesprávně vyhodnoceny (adversarial examples)).

systémy strojového učení a technologii rozpoznávání obličeje (např. otrávení dat (data poisoning), příklady navržené tak, aby byly nesprávně vyhodnoceny (adversarial examples), inverze modelu (model inversion), dovození bílé skříňky (white-box inference)). Vlastník procesu by měl rovněž stanovit vhodná ochranná opatření k zajištění toho, aby byly dodržovány požadavky na uchovávání biometrických údajů obsažených v datovém souboru pro účely přeškolení.

- Zdokumentovat systém využívající technologii rozpoznávání obličeje. To by mělo zahrnovat obecný popis systému využívajícího technologii rozpoznávání obličeje, podrobný popis prvků systému využívajícího technologii rozpoznávání obličeje a popis procesu jeho zavedení, podrobné informace o monitorování, fungování a kontrole systému využívajícího technologii rozpoznávání obličeje a podrobný popis jeho rizik a opatření k jejich zmírnění. Prvky obsažené v této dokumentaci budou zahrnovat hlavní prvky popisu systému využívajícího technologii rozpoznávání obličeje z předchozích fází (viz výše), které však budou rozšířeny o informace týkající se sledování výkonnosti a provádění změn v systému, včetně případných aktualizací verzí a/nebo přeškolení.
- Vytvořit uživatelské příručky vysvětlující technologii a případy použití. Ty musí jasným způsobem vysvětlit všechny scénáře a předpoklady, na jejichž základě bude technologie rozpoznávání obličeje používána.
- Vyškolit koncové uživatele o tom, jak tuto technologii používat. Tato školení musí vysvětlovat schopnosti a omezení technologie, aby uživatelé mohli pochopit okolnosti, za nichž je nutné ji použít, a případy, kdy může být tato technologie nepřesná. Tato školení rovněž pomohou zmírnit rizika spojená s neověřováním / nekritickým přijímáním výsledků algoritmů.
- Konzultovat s dozorovými úřady pro ochranu údajů podle čl. 28 odst. 1 písm. b) směrnice o prosazování práva. Poskytnout informace v souladu s článkem 13 směrnice o prosazování práva s cílem informovat subjekty údajů o zpracování a jejich právech. Tato oznámení se musí obracet na subjekty údajů vhodnou formou, aby byly schopny porozumět zpracování, a vysvětlovat základní prvky technologie, včetně míry přesnosti, datových souborů využitých ke školení a opatření přijatých s cílem zabránit diskriminaci a nízké přesnosti algoritmu.

4. DOPORUČENÍ PO ZAVEDENÍ TECHNOLOGIE ROZPOZNÁVÁNÍ OBLIČEJE

- Zajišťovat lidský zásah a dohled nad výsledky. Nikdy nepřijímejte žádné opatření týkající se jednotlivce pouze na základě výsledku technologie rozpoznávání obličeje (to by znamenalo porušení článku 11 směrnice o prosazování práva o automatizovaném individuálním rozhodování, které by mělo právní nebo jiné podobné účinky na subjekt údajů). Zajistěte, aby příslušník donucovacích orgánů přezkoumával výsledky technologie rozpoznávání obličeje. Rovněž zajistěte, aby se uživatelé z řad donucovacích orgánů vyhnuli předpojatosti automatizace tím, že budou zkoumat rozporuplné informace a kriticky zpochybňovat výsledky technologie. Za tímto účelem je důležité neustálé školení a zvyšování povědomí koncových uživatelů, nicméně vrcholné vedení by mělo zajistit dostatečné lidské zdroje pro výkon účinného dohledu. To znamená poskytnout každému agentovi dostatek času na kritické zpochybnění výsledků technologie. Zaznamenávejte, měřte a posuzujte, do jaké míry lidský dohled mění původní rozhodnutí technologie rozpoznávání obličeje.
- Sledovat rozklad modelu technologie rozpoznávání obličeje (zhoršení výkonnosti, model drift) po zavedení modelu do produkční fáze a zabývat se jím.
- Zavést proces pravidelného opětovného posuzování rizik a bezpečnostních opatření a pokaždé, když dojde ke změnám technologie nebo případu použití.
- Dokumentovat veškeré změny systému v průběhu jeho životního cyklu (např. aktualizace, přeškolení).

- Zavést proces, jakož i související technické schopnosti pro vyřizování žádostí subjektů údajů o přístup. Technická schopnost získávat údaje, pokud by bylo třeba je poskytnout subjektům údajů, musí být zavedena předtím, než přijde jakákoli žádost.
- Zajistit, aby byly zavedeny postupy pro případy porušení zabezpečení údajů. Dojde-li k porušení zabezpečení osobních údajů, včetně biometrických údajů, je pravděpodobné, že rizika budou vysoká. V tomto případě by si všichni dotčení uživatelé měli být vědomi příslušných postupů, které je třeba dodržet, pověřenec pro ochranu osobních údajů by měl být okamžitě informován a měly by být informovány i subjekty údajů.

PŘÍLOHA III – PRAKTICKÉ PŘÍKLADY

Existuje mnoho různých praktických nastavení a účelů použití rozpoznávání obličeje, například v kontrolovaném prostředí, jako jsou hraniční přechody, křížová kontrola s údaji z policejních databází nebo s osobními údaji, které subjekt údajů zjevně zveřejnil, kamerové záznamy naživo (rozpoznávání obličeje v přímém přenosu) atd. Rizika pro ochranu osobních údajů a dalších základních práv a svobod se tudíž v různých případech použití značně liší. Předkládané pokyny mají za cíl usnadnit posouzení nezbytnosti a přiměřenosti, které by mělo předcházet rozhodnutí o případném nasazení rozpoznávání obličeje, a poskytují orientační seznam možných použití technologie rozpoznávání obličeje v oblasti prosazování práva.

Předložené a posuzované scénáře vycházejí z **hypotetických** situací a mají ilustrovat určitá konkrétní využití technologie rozpoznávání obličeje a poskytnout pomoc při zvažování individuálních případů, jakož i pro stanovení celkového rámce. Tyto pokyny si nekladou za cíl být vyčerpávající a nejsou jimi dotčena žádná probíhající nebo budoucí řízení vedená vnitrostátním dozorovým úřadem v souvislosti s návrhem, experimentováním nebo zaváděním technologií rozpoznávání obličeje. Prezentace těchto scénářů by měla sloužit pouze jako příklad pokynů pro tvůrce politik, normotvůrce a donucovací orgány, které jsou již uvedeny v tomto dokumentu, při navrhování a plánování zavádění technologií rozpoznávání obličeje s cílem zajistit plný soulad s acquis EU v oblasti ochrany osobních údajů. V této souvislosti je třeba mít na paměti, že i v podobných situacích použití technologie rozpoznávání obličeje může přítomnost nebo nepřítomnost určitých prvků vést k odlišnému výsledku posouzení nezbytnosti a přiměřenosti.

1 SCÉNÁŘ 1

1.1. Popis

Systém automatizované hraniční kontroly, který umožňuje automatizovaný přechod hranic na základě ověření biometrického obrazu uloženého v elektronickém cestovním dokladu občanů EU a dalších cestujících procházejících hraničním přechodem a zjištění, že cestující je oprávněným držitelem dokladu.

Toto ověření/autentizace zahrnuje pouze rozpoznávání obličeje 1: 1 a provádí se v kontrolovaném prostředí (např. na letištních elektronických branách). Biometrické údaje cestujícího, který prochází hraničním přechodem, jsou zachyceny v okamžiku, kdy je výslovně vyzván, aby se podíval do kamery umístěné v elektronické bráně, a jsou porovnány s předloženým dokladem (cestovním pasem, průkazem totožnosti atd.), který je vydáván v souladu se zvláštními technickými požadavky.

Zároveň platí, že i když zpracování v takových případech v zásadě nespadá do oblasti působnosti směrnice o prosazování práva, může být výsledek ověření použit rovněž pro porovnávání (alfanumerických) údajů dané osoby s databázemi donucovacích orgánů v rámci ochrany hranic, a může tedy zahrnovat opatření s významným právním účinkem pro subjekt údajů, např. zatčení na základě záznamu v systému SIS. Za určitých okolností lze biometrické údaje použít také k vyhledávání shod v databázích donucovacích orgánů (v takovém případě by se v tomto kroku provedla identifikace 1: více).

Výsledek zpracování biometrických snímků má přímý dopad na subjekt údajů: pouze v případě úspěšného ověření umožňuje přechod hranice. V případě neúspěšné identifikace musí příslušníci pohraniční stráže provést druhou kontrolu, aby se ujistili, že subjekt údajů je skutečně jiná osoba než ta, která je vyobrazena v dokladu totožnosti.

V případě, že je nalezen záznam v systému SIS nebo vnitrostátní záznam, musí příslušníci pohraniční stráže provést druhé ověření a další nezbytné kontroly a poté přijmout veškerá nezbytná opatření, např. zadržet osobu, informovat příslušné orgány.

Zdroj informací:

- Typy subjektů údajů: ☒ všechny fyzické osoby překračující hranice
- Zdroj snímku: ☒ jiný (doklad totožnosti)
- Souvislost s trestnou činností: ☒ není nutná
- Způsob získávání informací: ☒ v kabině nebo v kontrolovaném prostředí
- Kontext – dopad na další základní práva: ano, konkrétně: ☒ právo na volný pohyb ☒ právo na azyl

Referenční databáze (s níž se porovnávají zachycené informace):

- Specifičnost: ☒ specifické databáze týkající se ochrany hranic

Algoritmus:

- Typ ověření: ☒ ověření 1: 1 (autentizace)

Výsledek:

- Dopad☒ přímý (subjektu údajů je povolen nebo odepřen vstup)
- Automatizované rozhodnutí: ☒ ano

1.2. Použitelný právní rámec

Od roku 2004 musí podle nařízení Rady (ES) č. 2252/2004[85] cestovní pasy a jiné cestovní doklady vydávané členskými státy obsahovat biometrický snímek obličeje uložený v elektronickém čipu zabudovaném v dokladu.

Schengenský hraniční kodex[86] stanoví požadavky na hraniční kontroly osob na vnějších hranicích. V případě občanů EU a dalších osob požívajících práva na volný pohyb podle práva Unie by minimální kontroly měly spočívat v ověření platnosti jejich cestovních dokladů, v případě potřeby s použitím technických prostředků. Schengenský hraniční kodex byl následně změněn nařízením (EU) 2017/2225[87], které zavedlo *mimo jiné* definice „elektronických bran“, „systému automatizované hraniční kontroly“ a „samoobslužného systému“, jakož i možnost zpracování biometrických údajů pro účely provádění hraničních kontrol.

Lze tedy předpokládat, že existuje jasný a předvídatelný právní základ, který povoluje tuto formu zpracování osobních údajů. Právní rámec je navíc přijat na úrovni Unie a je přímo použitelný v členských státech.

1.3. Nezbytnost a přiměřenost – účel/závažnost trestného činu

Ověření totožnosti občanů EU v rámci automatizované hraniční kontroly s využitím jejich biometrického snímku je součástí hraničních kontrol na vnějších hranicích EU. Proto přímo souvisí s bezpečností hranic a slouží účelu obecného zájmu, který uznává Unie. Kromě toho brány automatizované hraniční kontroly pomáhají urychlit odbavení cestujících a snižují riziko lidských chyb. Navíc je rozsah, míra a intenzita zásahu do základních práv v tomto scénáři mnohem omezenější ve srovnání s jinými formami rozpoznávání obličeje. Zpracování biometrických údajů však vytváří další

[85] NAŘÍZENÍ RADY (ES) č. 2252/2004 ze dne 13. prosince 2004 o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy.
[86] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/399 ze dne 9. března 2016, kterým se stanoví kodex Unie o pravidlech upravujících přeshraniční pohyb osob (Schengenský hraniční kodex).
[87] Nařízení Evropského parlamentu a Rady (EU) 2017/2225 ze dne 30. listopadu 2017, kterým se mění nařízení (EU) 2016/399, pokud jde o používání Systému vstupu/výstupu.

rizika pro subjekty údajů, která musí být řádně řešena a zmírněna příslušným orgánem, který zavádí a provozuje technologii rozpoznávání obličeje.

1.4. Závěr

Ověření totožnosti občanů EU v kontextu automatizované hraniční kontroly je nezbytným a přiměřeným opatřením, pokud jsou zavedeny vhodné záruky, zejména uplatňování zásad účelového omezení, kvality údajů, transparentnosti a vysoké úrovně bezpečnosti.

2 SCÉNÁŘ 2

2.1. Popis

Donucovací orgány zřídí systém identifikace obětí únosů dětí. Oprávněný policista může za přísných podmínek provést porovnání biometrických údajů dítěte, u něhož existuje podezření, že bylo uneseno, s databází obětí únosů dětí, a to výhradně za účelem identifikace nezletilých osob, které mohou odpovídat popisu pohřešovaného dítěte, kvůli němuž bylo zahájeno vyšetřování a po němž bylo vyhlášeno pátrání.

Dotčené zpracování by spočívalo v porovnání obličeje nebo snímku daného jednotlivce, který může odpovídat popisu pohřešovaného dítěte, se snímky uloženými v databázi. K takovému zpracování by docházelo ve zvláštních případech, a nikoli systematicky.

Databáze, s níž bude porovnání prováděno, je zaplněna fotografiemi pohřešovaných dětí, u nichž bylo nahlášeno podezření na únos dítěte, ohrožení jeho života nebo tělesné integrity, soudní orgán zahájil trestní vyšetřování a byl vydán záznam ohledně únosu dítěte. Údaje jsou shromažďovány v rámci postupů stanovených příslušným donucovacím orgánem, tj. policisty pověřenými výkonem úkolů justiční policie. Zaznamenávají se tyto kategorie osobních údajů:

- totožnost, přezdívka, pseudonym, příbuzenství, státní příslušnost, adresy, e-mailové adresy, telefonní čísla,
- datum a místo narození,
- informace o rodičovství,
- fotografie s technickými prvky umožňujícími použití zařízení pro rozpoznávání obličeje a jiné fotografie.

Výsledky porovnání musí být rovněž přezkoumány a ověřeny oprávněným příslušníkem, aby bylo možné podepřít předchozí důkazy o výsledky porovnání a vyloučit případné falešně pozitivní výsledky.

Obrázky a osobní údaje dětí mohou být uchovávány pouze po dobu trvání záznamu a musí být vymazány ihned po uzavření nebo zastavení trestního řízení v souladu s vnitrostátními postupy, v souvislosti s nimiž byly vloženy do databáze.

I když doba uchovávání biometrických údajů v databázi může být stanovena na poměrně dlouhou dobu a vymezena podle vnitrostátního práva, výkon práv subjektu údajů, zejména práva na opravu a výmaz, poskytuje dodatečnou záruku omezení zásahu do práva na ochranu osobních údajů dotčených subjektů údajů.

Zdroj informací:

- Typy subjektů údajů: ☒ děti

- Zdroj snímku ☒ jiné: předem neurčeno, domnělá oběť únosu dítěte
- Souvislost s trestnou činností ☒ není přímá časová ☒ není přímá geografická
- Způsob získávání informací: ☒ v kabině nebo v kontrolovaném prostředí
- Kontext: dopad na jiná základní práva☒ ano, konkrétně:☒ různé

Referenční databáze (s níž se porovnávají zachycené informace):

- Specifičnost ☒ zvláštní databáze

Algoritmus:

- Typ ověření: ☒ identifikace 1 : více

Výsledek:

- Dopad ☒ přímý
- Automatizované rozhodnutí: ☒ NE, povinný přezkum oprávněným úředníkem

Právní analýza:

- Použitelný právní rámec: ☒ zvláštní vnitrostátní právní předpisy pro toto zpracování (rychlé uznání)

2.2. Použitelný právní rámec

Vnitrostátní právní předpisy stanoví zvláštní právní rámec pro zřízení databáze, který určuje účely zpracování, jakož i kritéria pro zaplňování databáze, přístup k ní a její používání. Legislativní opatření nezbytná pro jeho provádění rovněž stanoví dobu uchovávání a odkazují na platné zásady neporušenosti a důvěrnosti. Legislativní opatření rovněž stanoví podmínky poskytování informací subjektu údajů a v tomto případě nositeli (nositelům) rodičovské zodpovědnosti, jakož i výkon práv subjektu údajů a jejich případné omezení. Při přípravě návrhu příslušného legislativního opatření bylo nutné konzultovat s vnitrostátním dozorovým úřadem.

2.3. Nezbytnost a přiměřenost – účel/závažnost trestného činu / počet osob, které nejsou zapojeny, ale jsou zpracováním dotčeny

Podmínky a záruky pro zpracování

Porovnání na základě rozpoznávání obličeje může oprávněný úředník provést pouze v krajním případě, pokud nejsou k dispozici žádné jiné, méně rušivé prostředky a pokud je to zcela nezbytné, například v případě pochybností o pravosti dokladu totožnosti cestující nezletilé osoby a/nebo po přezkoumání předchozích shromážděných důkazů a materiálů naznačujících možnou shodu s popisem pohřešovaného dítěte, v souvislosti s kterým probíhá trestní vyšetřování.

Je rovněž poskytnuta další záruka v podobě povinného přezkumu a ověření porovnání na základě rozpoznávání obličeje oprávněným úředníkem, aby bylo možné předchozí důkazy podepřít výsledky porovnání a vyloučit případné falešně pozitivní výsledky.

Sledovaný cíl

Zřízení databáze slouží důležitým účelům obecného veřejného zájmu, zejména předcházení, vyšetřování, odhalování nebo stíhání trestných činů nebo výkonu trestů a ochraně práv a svobod jiných osob. Zřízení databáze a předpokládané zpracování zjevně přispívají k identifikaci dětských obětí únosu, a proto je lze považovat za opatření vhodné k podpoře legitimního cíle, kterým je vyšetřování a stíhání takové trestné činnosti.

Účel a zaplnění databáze

Účely zpracování jsou jasně vymezeny zákonem a databáze se používá pouze pro účely identifikace pohřešovaných dětí, u nichž bylo nahlášeno podezření na únos dítěte a bylo zahájeno trestní vyšetřování pod dohledem soudního orgánu a v souvislosti s nimiž byl vydán záznam o únosu dítěte. Zákonem stanovené podmínky pro zaplnění databáze mají za cíl přísně omezit počet subjektů údajů a osobní údaje, které mají být do databáze zahrnuty. Nositel rodičovské zodpovědnosti za dítě musí být informován o prováděném zpracování a o podmínkách výkonu práv dítěte v souvislosti s biometrickým zpracováním zamýšleným pro účely identifikace nebo s osobními údaji dítěte uloženými v databázi.

2.4. Závěr

Vzhledem k nezbytnosti a přiměřenosti zamýšleného zpracování, jakož i k nejlepšímu zájmu dítěte při provádění takového zpracování osobních údajů a za předpokladu, že jsou zavedeny dostatečné záruky zejména pro zajištění výkonu práv subjektu údajů – zejména s ohledem na skutečnost, že mají být zpracovávány údaje dětí –, lze takové použití zpracování rozpoznávání obličeje považovat za pravděpodobně slučitelné s právem EU.

Kromě toho vzhledem k typu zpracování a použité technologii, která představuje vysoké riziko pro práva a svobody dotčeného subjektu údajů, se EDPB domnívá, že příprava návrhu legislativního opatření, který má přijmout vnitrostátní parlament, nebo návrhu regulačního opatření založeného na takovém legislativním opatření, jež souvisí se zpracováním, musí zahrnovat předchozí konzultaci s dozorovým úřadem, aby byla zajištěna soudržnost a soulad s platným právním rámcem, srov. čl. 28 odst. 2 směrnice o prosazování práva.

3 SCÉNÁŘ 3

3.1. Popis

V průběhu policejních zásahů při nepokojích a následných vyšetřování byla identifikována řada podezřelých osob, např. na základě předchozích vyšetřování s využitím uzavřeného televizního okruhu (CCTV) nebo svědků. Snímky těchto podezřelých se porovnávají se snímky osob, které byly zaznamenány na uzavřeném televizním okruhu nebo mobilních zařízeních na místě činu nebo v jeho okolí.

Za účelem získání podrobnějších důkazů o osobách podezřelých z účasti na nepokojích, které provázely demonstraci, vytváří policie databázi složenou z obrazového materiálu s volnou místní a časovou vazbou na nepokoje. Databáze zahrnuje soukromé záznamy, které policii předali občané, materiály z uzavřeného televizního okruhu veřejné dopravy, materiály z policejních kamerových systémů a materiály zveřejněné sdělovacími prostředky bez jakéhokoli zvláštního omezení nebo záruk. Zobrazování závažné trestné činnosti není nezbytným předpokladem pro shromažďování složek v databázi. Proto jsou v databázi uloženy i osoby, které se nepokojů neúčastnily, tedy významné procento místních obyvatel, kteří šli v době demonstrace náhodou kolem nebo se účastnili demonstrace, ale nikoliv nepokojů. Jedná se o tisíce videozáznamů a snímků.

Pomocí softwaru pro rozpoznávání obličejů se všem obličejům, které se v těchto souborech objeví, přiřadí jedinečný identifikátor obličeje. Obličeje jednotlivých podezřelých jsou pak automaticky porovnávány s těmito identifikátory obličeje. Databáze složená ze všech biometrických šablon v tisíci videozáznamech a obrazových souborech je uchovávána až do ukončení všech možných vyšetřování. Pozitivní shody řeší odpovědní úředníci, kteří pak rozhodují o dalších krocích. To může zahrnovat přiřazení spisu nalezeného v databázi k trestnímu spisu příslušné osoby, jakož i další opatření, jako je výslech nebo zatčení této osoby.

Vnitrostátní právo obsahuje obecné ustanovení, podle něhož je zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby přípustné, je-li to zcela nezbytné a jsou-li v této souvislosti stanoveny vhodné záruky pro práva a svobody dotčené osoby.

Zdroj informací:

- Typy subjektů údajů: ☒ všechny osoby
- Zdroj snímku: ☒ veřejně přístupné prostory ☒ soukromý subjekt ☒ jiné fyzické osoby ☒ jiný: sdělovací prostředky
- Souvislost s trestnou činností: ☒ neexistuje nevyhnutelně přímá geografická ani časová souvislost
- Způsob zachycování informací: ☒ na dálku
- Kontext – dopad na další základní práva: ano, konkrétně ☒ v souvislosti se svobodou shromažďování
- Dostupné další zdroje informací o subjektu údajů:
  ☒ jiné: není vyloučeno (např. použití bankomatů nebo návštěva obchodů), protože nelze kontrolovat motivy na fotografiích

Referenční databáze (s níž se porovnávají zachycené informace):

- Specifičnost: ☒ konkrétní databáze související s oblastí trestné činnosti

Algoritmus:

- Typ zpracování: ☒ identifikace 1: více

Výsledek:

- Dopad: ☒ přímý (např. subjekt údajů může být zatčen, vyslýchán)
- Automatické rozhodnutí: ☒ NE
- Doba uchovávání: do ukončení všech možných šetření

Právní analýza:

- Druh předchozího informování subjektu údajů: ☒ obecně na internetových stránkách donucovacího orgánu
- Použitelný právní rámec: ☒ směrnice o prosazování práva z větší části převzatá ve vnitrostátním právu ☒ obecný vnitrostátní právní předpis pro používání biometrických údajů ze strany donucovacích orgánů

3.2. Použitelný právní rámec

Jak bylo objasněno výše, v právních základech se pouze opakuje obecné ustanovení článku 10 směrnice o prosazování práva, a jejich znění není dostatečně jasné, aby jednotlivcům poskytlo dostatečné informace o podmínkách a okolnostech, za nichž jsou donucovací orgány oprávněny používat záznamy z uzavřeného televizního okruhu z veřejných prostor k vytvoření biometrické šablony jejich obličeje a porovnat ji s policejními databázemi, jinými dostupnými záznamy z uzavřeného televizního okruhu nebo soukromými záznamy atd. Právní rámec stanovený v tomto scénáři proto nesplňuje minimální požadavky na to, aby sloužil jako právní základ.

3.3. Nezbytnost a přiměřenost

V tomto případě zpracování vyvolává různé obavy ohledně zásad nezbytnosti a přiměřenosti, a to z několika důvodů:

Osoby nejsou podezřelé ze závažného trestného činu. Zobrazování závažné trestné činnosti není podmínkou pro použití souborů v databázi obsahující obrazový materiál. Rovněž přímá časová a geografická souvislost s trestným činem není podmínkou pro používání souborů v databázi. To vede k tomu, že je v biometrické databázi uchováváno po dobu potenciálně několika let, dokud nebudou ukončena všechna šetření, značné procento místního obyvatelstva.

Databáze místa činu se neomezuje na snímky splňující požadavky přiměřenosti, což vede k neomezenému množství snímků, které lze porovnávat. To je v rozporu se zásadou minimalizace údajů. Menší množství snímků by také umožnilo zvážit nealgoritmické a méně rušivé prostředky, např. „superrozpoznávače“.[88]

Vzhledem k tomu, že tento příklad pochází z okolí protestu, je také pravděpodobné, že snímky odhalují politické názory účastníků demonstrace, což je druhá zvláštní kategorie údajů, které mohou být v tomto scénáři dotčeny. V tomto scénáři není jasné, jak lze shromažďování těchto údajů zabránit a s jakými zárukami. Kromě toho, pokud se subjekty údajů dozvědí, že jejich účast na demonstraci vedla k jejich vložení do biometrické policejní databáze, může to mít vážné odrazující účinky na jejich budoucí výkon práva shromažďování.

Biometrické šablony v databázi lze také vzájemně porovnávat. Policie tak může nejen hledat konkrétní osobu ve všech jejich materiálech, ale také v průběhu několika dnů rekonstruovat vzorec chování dané osoby. Může rovněž shromažďovat další informace o osobách, jako jsou sociální kontakty a účast na politickém životě.

Zásah je dále zesílen skutečností, že údaje jsou zpracovávány bez vědomí subjektů údajů.

Vzhledem k tomu, že fotografie a videa jsou lidmi zaznamenávány neustále a že i všudypřítomné pokrytí uzavřeným televizním okruhem může být analyzováno za účelem získání biometrických údajů, může to vést k závažným odrazujícím účinkům.

Dalším důvodem ke znepokojení je rozsáhlé využívání soukromých fotografií a videí, včetně možného zneužití, jako je veřejné zostuzování. Vzhledem k tomu, že zneužití, jako je veřejné zostuzení, je riziko vlastní i trestnímu řízení obecně, je riziko podstatně vyšší, pokud jde o rozsah zpracovávaných údajů a počet zúčastněných osob, protože lidé mohou nahrát i materiály týkající se konkrétní osoby nebo skupiny osob, k nimž chovají averzi. Žádosti policie o zasílání fotografií a videí mohou vést k velmi nízkým omezením určujícím, který materiál mohou lidé poskytovat, zejména proto, že by to mohlo být možné anonymně nebo alespoň bez nutnosti dostavit se na policejní stanici a prokázat svou totožnost.

3.4. Závěr

V tomto příkladu neexistuje žádné zvláštní ustanovení, které by mohlo sloužit jako právní základ. I kdyby však existoval dostatečný právní základ, nebyly by splněny požadavky na nezbytnost a přiměřenost, což by vedlo k nepřiměřenému zásahu do práv subjektu údajů na respektování soukromého života a ochranu osobních údajů podle Listiny.

[88] Tj. lidé s mimořádnou schopností rozpoznávání obličeje. Srov. také: Face Recognition by Metropolitan Police Super-Recognisers (Rozpoznávání obličeje ze strany superrozpoznávačů metropolitní policie), 26. února 2016, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

4 SCÉNÁŘ 4

4.1. Popis

Policie zavede způsob identifikace podezřelých, kteří se dopustili závažného trestného činu zaznamenaného na uzavřeném televizním okruhu pomocí retrospektivní technologie rozpoznávání obličeje. Úředník manuálně vytřídí snímek (snímky) podezřelých z videomateriálu, který byl shromážděn na místě trestného činu nebo jinde v rámci předběžného vyšetřování, a poté zašle snímek (snímky) forenznímu oddělení. Forenzní oddělení použije technologii rozpoznávání obličeje k porovnávání těchto snímků s fotografiemi osob, které policie dříve shromáždila v databázi (tzv. popisná databáze, která se skládá z podezřelých a dříve odsouzených osob). Popisná databáze je pro tento postup – dočasně a v izolovaném prostředí – analyzována s využitím technologie rozpoznávání obličeje, aby bylo možné provést proces porovnávání. Aby se minimalizoval zásah do práv a zájmů osob, u kterých byla zjištěna shoda, má velmi omezený počet zaměstnanců forenzního oddělení povolení k provedení samotného postupu přiřazování, přístup k údajům je omezen na ty úředníky, kteří jsou pověřeni konkrétním spisem, a před předáním jakéhokoli výsledku vyšetřujícímu policistovi se provádí manuální kontrola výsledků. Biometrické údaje nejsou předávány mimo kontrolované izolované prostředí. Při vyšetřování se dále používá pouze výsledek a fotografie (nikoli biometrická šablona). Zaměstnanci absolvují zvláštní školení o pravidlech a postupech pro toto zpracování a veškeré zpracování osobních a biometrických údajů je ve vnitrostátních právních předpisech dostatečně specifikováno.

Zdroj informací:

- Typy subjektů údajů: ☒ podezřelé osoby identifikované na základě záznamů z uzavřeného televizního okruhu
- Zdroj snímku: ☒ veřejně přístupná místa ☒ internet
- Souvislost s trestnou činností: ☒ přímá časová souvislost
  ☒ přímá geografická
- Způsob zachycování informací: ☒ na dálku
- Kontext – dotčení dalších základních práv: ano, konkrétně: ☒ svoboda shromažďování
  ☒ svoboda projevu ☒ různé: __

Referenční databáze (s níž se porovnávají zachycené informace):

- Specifičnost: ☒ konkrétní databáze související s oblastí trestné činnosti

Algoritmus:

- Typ zpracování: ☒ identifikace 1 : více

Výsledek:

- Dopad: ☒ přímý (např. zatčení subjektu údajů, výslech)
- Automatické rozhodnutí: ☒ NE

Právní analýza:

- Použitelný právní rámec: ☒ zvláštní vnitrostátní právní předpis pro toto zpracování (rozpoznávání obličeje) pro daný příslušný orgán

4.2. Použitelný právní rámec

V tomto scénáři je ve vnitrostátních právních předpisech stanoveno, že biometrické údaje mohou být použity při provádění forenzní analýzy, je-li to zcela nezbytné pro dosažení účelu identifikace

podezřelých ze spáchání závažného trestného činu, přiřazením snímku v popisné databázi. Vnitrostátní právní předpis stanoví, které údaje mohou být zpracovávány, jakož i postupy pro zachování neporušenosti a důvěrnosti osobních údajů a postupy pro jejich zničení, a poskytují tak dostatečné záruky proti riziku zneužití a svévole.

4.3. Nezbytnost a přiměřenost

Používání rozpoznávání obličeje je zjevně časově účinnější než manuální přiřazování na forenzní úrovni. Manuální výběr snímků předem omezuje zásah do práv ve srovnání s porovnáváním veškerého videomateriálu s databází, a tím rozlišuje mezi lidmi a zaměřuje se pouze na osoby, které mají souvislost s cílem, tj. bojem proti závažné trestné činnosti. Je však stále důležité zvážit, zda nelze přiřazení provést manuálně v přiměřené době, v závislosti na daném případu. Omezení osob s přístupem k technologii a osobním údajům zmírňuje dopad na práva na soukromí a ochranu údajů. Stejný dopad má i to, pokud nebudou v průběhu vyšetřování biometrické šablony ukládány nebo používány později. Manuální kontrola výsledku rovněž znamená snížení rizika falešných pozitivních shod.

4.4. Závěr

Je důležité, aby vnitrostátní právní předpisy poskytovaly vhodný právní základ pro zpracování biometrických údajů, jakož i pro vnitrostátní databázi, s níž probíhá porovnávání. V tomto scénáři bylo zavedeno několik opatření s cílem omezit zásah do práv na ochranu údajů, jako jsou podmínky pro využívání technologie rozpoznávání obličeje stanovené v právním základu, počet osob s přístupem k technologii a biometrickým údajům, manuální kontroly atd. Technologie rozpoznávání obličeje významně zlepšuje účinnost vyšetřovací činnosti forenzního oddělení policie, je založena na právních předpisech umožňujících policii zpracovávat biometrické údaje, je-li to zcela nezbytné, a za těchto podmínek ji lze tedy považovat za legální zásah do práv jednotlivce.

5 SCÉNÁŘ 5

5.1. Popis

Biometrická identifikace na dálku znamená, že se totožnost osob zjišťuje pomocí biometrických identifikátorů (snímek obličeje, chůze, oční duhovky atd.) na dálku, ve veřejném prostoru a setrvale nebo průběžně jejich porovnáváním s (biometrickými) údaji uloženými v databázi[89]. Biometrická identifikace na dálku se provádí v reálném čase, pokud zachycování obrazového materiálu, porovnání a identifikace probíhají bez významného zpoždění.

Před každým nasazením dálkové biometrické identifikace v reálném čase policie v rámci vyšetřování sestaví seznam zájmových osob. Na tento seznam se zařadí snímky obličejů jednotlivců. Na základě zpravodajských informací, které naznačují, že se osoby budou nacházet v určité oblasti, například v nákupním centru nebo na veřejném prostranství, policie rozhodne, kdy, kde a na jak dlouho nasadí biometrickou identifikaci na dálku.

V den akce umístí na místo policejní dodávku jako řídicí středisko, v níž bude sedět vyšší policejní důstojník. V dodávce jsou umístěny monitory, na kterých se zobrazují záznamy z kamer uzavřeného televizního okruhu umístěných v okolí, a to buď instalovaných ad hoc, nebo připojených k videopřenosu z již nainstalovaných kamer. Když chodci procházejí kolem kamer, technologie izoluje

[89] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

snímky obličeje, převede je do podoby biometrické šablony a porovná je s biometrickými šablonami osob na seznamu zájmových osob.

Pokud je zjištěna potenciální shoda mezi seznamem zájmových osob a osobami, které procházejí kolem kamer, je příslušníkům v dodávce zasláno upozorněni a ti pak informují policisty v terénu, pokud došlo k pozitivní shodě, např. prostřednictvím rádiového zařízení. Policista na místě se pak rozhodne, zda zasáhne, přiblíží se k osobě nebo ji nakonec zadrží. Opatření přijatá policistou v terénu se zaznamenávají. V případě skryté kontroly jsou shromážděné informace (např. s kým je daná osoba v kontaktu, co má na sobě a kam jde) uloženy.

Vnitrostátní právní předpis, na který se odkazuje, obsahuje obecné ustanovení, podle něhož je zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby přípustné, je-li to zcela nezbytné a podléhá-li vhodným zárukám pro práva a svobody dotčené osoby.

Zdroj informací:

- Typy subjektů údajů: ☒ všechny osoby
- Zdroj snímku: ☒ veřejně přístupné prostory
- Souvislost s trestnou činností: ☒ neexistuje nevyhnutelně přímá geografická ani časová souvislost
- Způsob zachycování informací: ☒ na dálku
- Kontext – dopad na další základní práva: ano, konkrétně: ☒ svoboda shromažďování ☒ svoboda projevu ☒ různé
- Dostupné další zdroje informací o subjektu údajů:
  ☒ jiné: není vyloučeno (např. používání bankomatů nebo návštěva obchodů)

Referenční databáze (s níž se porovnávají zachycené informace):

- Specifičnost: ☒ konkrétní databáze související s oblastí trestné činnosti

Algoritmus:

- Typ zpracování: ☒ identifikace 1: více

Výsledek:

- Dopad: ☒ přímý (např. zatčení subjektu údajů, výslech)
- Automatické rozhodnutí: ☒ NE
- Doba uchovávání: do ukončení všech možných šetření

Právní analýza:

- Druh předchozího informování subjektu údajů: ☒ obecně na internetových stránkách donucovacího orgánu
- Použitelný právní rámec: ☒ směrnice o prosazování práva z větší části převzatá ve vnitrostátním právu ☒ obecný vnitrostátní právní předpis pro používání biometrických údajů ze strany donucovacích orgánů

5.2. Použitelný právní rámec

Právní základy, které pouze opakují obecné ustanovení článku 10 směrnice o prosazování práva, nejsou dostatečně jasné, pokud jde o jejich znění, aby jednotlivcům poskytly dostatečné informace o podmínkách a okolnostech, za nichž jsou donucovací orgány oprávněny používat záznamy z uzavřeného televizního okruhu z veřejných prostor k vytvoření biometrické šablony jejich obličeje a

porovnat ji s policejními databázemi. Právní rámec stanovený v tomto scénáři tedy nesplňuje minimální požadavky na to, aby sloužil jako právní základ.[90]

5.3. Nezbytnost a přiměřenost

Čím hlubší je zásah, tím vyšší je laťka nezbytnosti a přiměřenosti. Biometrická identifikace na dálku ve veřejných prostorách má několik dopadů na základní práva:

Scénáře zahrnují monitorování všech kolemjdoucích v příslušném veřejném prostoru. Má tedy závažný dopad na přiměřené očekávání obyvatel, že budou ve veřejných prostorách anonymní[91]. To je předpokladem pro mnoho aspektů demokratického procesu, jako je rozhodnutí vstoupit do občanského sdružení, navštívit shromáždění a setkat se s lidmi ze všech sociálních a kulturních prostředí, účastnit se politického protestu a navštěvovat místa všeho druhu. Koncepce anonymity na veřejných prostranstvích je nezbytná pro svobodné shromažďování a výměnu informací a idejí. Chrání pluralitu názorů, svobodu pokojného shromažďování a svobodu sdružování a ochranu menšin a podporuje zásadu oddělení pravomocí a zásadu brzd a protivah. Oslabení koncepce anonymity na veřejných prostranstvích může mít na občany závažný odrazující účinek. Mohou se zdržet určitého chování, které je v rámci svobodné a otevřené společnosti zcela v pořádku. To by ovlivnilo veřejný zájem, neboť demokratická společnost vyžaduje sebeurčení a účast jejích občanů v demokratickém procesu.

Pokud bude taková technologie použita, pouhá chůze po ulici, do metra nebo do pekařství v zasažené oblasti povede ke shromažďování osobních údajů, včetně biometrických, donucovacími orgány a v případě prvního scénáře také k porovnání s policejními databázemi. Situace, kdy by se totéž provádělo sejmutím otisků prstů, by byla zjevně nepřiměřená.

Počet dotčených subjektů údajů je mimořádně vysoký, neboť se to týká všech osob, které procházejí příslušnou veřejnou oblastí. Kromě toho by scénáře zahrnovaly automatizované hromadné zpracování biometrických údajů a také hromadné porovnávání biometrických údajů s policejními databázemi.

V evropské judikatuře je hromadné sledování zakázáno (např. ESLP ve věci S. a Marper proti Spojenému království považoval nerozlišující uchovávání biometrických údajů za „nepřiměřený zásah“ do práva na soukromí, protože jej nelze považovat za „nezbytný v demokratické společnosti“).

Biometrická identifikace na dálku je natolik náchylná k tomu, že bude využita k hromadnému sledování, že neexistují žádné spolehlivé prostředky pro její omezení. Zásadně se liší od sledování pomocí videokamer jako takového, protože případné použití videozáznamu bez biometrické identifikace je již silným zásahem, ale zároveň omezeným, zatímco v případě použití technologie rozpoznávání obličeje dojde ke změně kvality již tak rozšířeného systému sledování pomocí videokamer jako hlavního zdroje údajů. Kromě toho zejména s ohledem na naznačené odrazující účinky nebudou možná omezení v používání již existujících zařízení pro sledování pomocí videokamer viditelná, a tudíž nebudou pro veřejnost důvěryhodná.

Biometrická identifikace na dálku prováděná policejními orgány přistupuje ke každému jako k potenciálnímu podezřelému. V právním státě se však občané považují za počestné, dokud se

[90] V případech, kdy by vědecký projekt zaměřený na výzkum využití technologie rozpoznávání obličeje musel zpracovávat osobní údaje, ale toto zpracování by nespadalo do působnosti čl. 4 odst. 3 směrnice o prosazování práva nebo mimo oblast působnosti práva Unie, bylo by použitelné obecné nařízení o ochraně osobních údajů. V případě pilotních projektů, po nichž by následovaly operace v oblasti prosazování práva, by byla stále použitelná směrnice o prosazování práva.

[91] Odpověď EDPB poslancům EP týkající se aplikace pro rozpoznávání obličeje vyvinuté společností Clearview AI, 10. června 2020, ref.: OUT2020-0052.

neprokáže jejich pochybení. Tato zásada se částečně odráží i ve směrnici o prosazování práva, která zdůrazňuje potřebu co nejvíce rozlišovat mezi zacházením s odsouzenými nebo podezřelými z trestné činnosti, v jejichž případě musí mít donucovací orgány „*závažné důvody se domnívat, že spáchaly trestný čin nebo se jej chystají spáchat*“ (čl. 6 písm. a) směrnice o prosazování práva), a těmi, kteří nejsou odsouzeni nebo podezřelí z trestné činnosti.

Budou-li použity v dopravních uzlech nebo na veřejných prostranstvích, kde donucovací orgány využijí technologii schopnou jednoznačně identifikovat jednotlivou osobu a sledovat a analyzovat její pobyt a pohyb, bude možné odhalit až ty nejcitlivější informace o dané osobě (dokonce i sexuální preference, náboženství, zdravotní problémy). S tím je spojeno obrovské riziko neoprávněného přístupu k údajům a jejich neoprávněného použití.

Instalace systému, který umožňuje odhalit samotnou podstatu chování a vlastností jednotlivce, vede k silným odrazujícím účinkům. Nutí lidi pochybovat o tom, zda se mají připojit k určité manifestaci, a tím poškozuje demokratický proces. Za kritické by mohlo být považováno také setkání s určitým přítelem, o němž je známo, že má potíže s policií, nebo svébytné chování, a to vzhledem k tomu, že to vše by vedlo k přilákání pozornosti algoritmu systému, a tedy i donucovacích orgánů.

Není možné chránit zranitelné subjekty údajů, jako jsou děti. Kromě toho jsou dotčeny osoby, které mají profesionální zájem – a často příslušnou právní povinnost – na zachování důvěrnosti svých kontaktních osob, jako jsou novináři, advokáti a duchovní. Uvedený postup by mohl například vést k odhalení zdroje a novináře nebo ke skutečnosti, že se daná osoba radí s advokátem specializujícím se na obhajobu v trestním řízení. Problém se netýká pouze náhodných veřejných míst, kde se setkávají například novináři a jejich zdroje, ale přirozeně i veřejných prostor nezbytných k tomu, aby se v tomto ohledu obrátili na instituce nebo odborníky a získali k nim přístup.

Kromě toho může nepohodlí lidí spojené s technologií rozpoznávání obličeje vést k tomu, že změní své chování a začnou se vybývat místům, kde se tato technologie využívá, a tím se stáhnou ze společenského života a přestanou se účastnit kulturních akcí. V závislosti na rozsahu nasazení technologie rozpoznávání obličeje může být dopad na lidi natolik významný, že ovlivní jejich možnost žít důstojný život[92].

Proto je velmi pravděpodobné, že bude dotčena podstata – nedotknutelné jádro – práva na ochranu osobních údajů. Silné indicie (srov. oddíl 3.1.3.2 pokynů) jsou zejména tyto: ve velkém měřítku jsou automaticky zpracovávány jedinečné biologické znaky osob donucovacími orgány pomocí algoritmů založených na věrohodnosti s pouze omezenou možností vysvětlení výsledků. Omezení práva na soukromí a ochranu údajů jsou ukládána bez ohledu na individuální chování dané osoby nebo na okolnosti, které se jí týkají. Statisticky téměř všechny subjekty údajů dotčené tímto zásahem jsou jednotlivci, kteří dodržují právní předpisy. Existují pouze omezené možnosti poskytování informací subjektu údajů. Soudní přezkum bude ve většině případů možný pouze následně.

Spoléhání se na systém založený na věrohodnosti a s omezenou možností vysvětlení může vést k zastření odpovědnosti a nedostatečnosti opravných prostředků a může motivovat k nedbalosti.

Jakmile se takový systém, který lze použít i na stávající kamery v rámci uzavřeného televizního okruhu, zavede, může být s malým úsilím a bez toho, aby byl pro jednotlivce viditelný, zneužit a umožnit systematické a rychlé sestavování seznamů osob podle etnického původu, pohlaví, náboženství atd.

[92] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, strana 20.

Zásada zpracování osobních údajů podle předem stanovených kritérií, jako je místo pobytu osoby a trasa, po které cestuje, se již praktikuje[93] a může vést k diskriminaci.

Vzhledem k citlivosti, expresivnosti a množství zpracovávaných údajů jsou systémy pro rozpoznávání obličeje na dálku na veřejně přístupných místech náchylné ke zneužití, což může vést k nepříznivým dopadů na dotčené jednotlivce. Tyto údaje lze také snadno shromažďovat a zneužívat k nátlaku na klíčové aktéry v rámci zásady brzd a protivah, jako je politická opozice, úředníci a novináři.

Systémy využívající technologii rozpoznávání obličeje mají v neposlední řadě sklon vykazovat silnou předpojatost na základě rasy a pohlaví: falešně pozitivní výsledky neúměrně postihují osoby jiné barvy pleti a ženy[94], což vede k diskriminaci. Policejní opatření v návaznosti na falešně pozitivní výsledek, jako jsou prohlídky a zatýkání, tyto skupiny dále stigmatizují.

5.4. Závěr

Výše uvedené scénáře týkající se zpracování biometrických údajů na dálku ve veřejných prostorech pro účely identifikace nezajišťují spravedlivou rovnováhu mezi soupeřícími soukromými a veřejnými zájmy, a tudíž představují nepřiměřený zásah do práv subjektu údajů podle článků 7 a 8 Listiny.

6 SCÉNÁŘ 6

6.1. Popis

Soukromý subjekt poskytuje aplikaci, v níž se z internetu získávají snímky obličejů (scraping) a vytváří se z nich databáze. Uživatel, např. policie, pak může nahrát fotografii a aplikace se ji pomocí biometrické identifikace pokusí přiřadit ke snímkům obličeje nebo biometrickým šablonám ve své databázi.

Místní policejní útvar provádí vyšetřování trestného činu zachyceného na videozáznamu, ze kterého nelze identifikovat řadu potenciálních svědků a podezřelých prostřednictvím porovnání shromážděných informací s jakýmikoli interními databázemi nebo zpravodajskými informacemi. Jednotlivci nejsou na základě shromážděných informací zaregistrováni v žádné stávající policejní databázi. Policie se rozhodne použít výše popsaný nástroj, který poskytuje soukromá společnost, k identifikaci jednotlivců prostřednictvím biometrické identifikace.

Zdroj informací:

- Typy subjektů údajů: ☒ všichni občané (svědci) ☒ odsouzení ☒ podezřelí
- Zdroj snímku: ☒ videozáznam z veřejného prostranství nebo shromážděný jinde v rámci předběžného vyšetřování
- Souvislost s trestnou činností: ☒ není nutná
- Způsob zachycování informací: ☒ na dálku
- Kontext – dopad na další základní práva: ano, konkrétně: ☒ svoboda shromažďování ☒ svoboda projevu ☒ různé: __

[93] Srov. článek 6 směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti a článek 33 Nařízení Evropského parlamentu a Rady (EU) 2018/1240 ze dne 12. září 2018, kterým se zřizuje Evropský systém pro cestovní informace a povolení (ETIAS) a kterým se mění nařízení (EU) č. 1077/2011, (EU) č. 515/2014, (EU) 2016/399, (EU) 2016/1624 a (EU) 2017/2226.

[94] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

Referenční databáze (s níž se porovnávají zachycené informace):

- Specifičnost: ☒ databáze pro všeobecné účely zaplněná materiálem z internetu

Algoritmus:

- Typ zpracování: ☒ identifikace 1 : více

Výsledek:

- Dopad ☒ přímý (např. zatčení subjektu údajů, výslech, diskriminační chování)
- Automatické rozhodnutí: ☒ NE

Právní analýza:

- Typ předchozího informování subjektu údajů: ☒ ne

6.2. Použitelný právní rámec

Pokud soukromý subjekt poskytuje službu, která zahrnuje zpracování osobních údajů, pro které určuje účel a prostředky (v tomto případě „scraping“ snímků z internetu za účelem vytvoření databáze), musí mít tento soukromý subjekt právní základ pro toto zpracování. Kromě toho musí mít donucovací orgán, který se rozhodne využít tuto službu pro vlastní účely, právní základ pro zpracování, pro které určuje účel a prostředky. Aby mohl donucovací orgán zpracovávat biometrické údaje, musí existovat právní rámec, který stanoví cíl, osobní údaje, které mají být zpracovávány, účely zpracování a postupy pro zachování neporušenosti a důvěrnosti osobních údajů, jakož i postupy pro jejich zničení.

Tento scénář předpokládá hromadný sběr osobních údajů od jednotlivců, kteří si nejsou vědomi toho, že jsou jejich údaje shromažďovány. Takové zpracování by mohlo být zákonné pouze za velmi výjimečných okolností. V závislosti na tom, kde se databáze nachází, může použití takové služby znamenat předání osobních údajů a/nebo zvláštních kategorií osobních údajů mimo Evropskou unii (policií, např. „odesláním“ snímku obličeje na videozáznamu z průmyslové kamery nebo jinak shromážděných údajů), což vyžaduje zvláštní podmínky pro toto předání, viz článek 39 směrnice o prosazování práva.

V tomto scénáři neexistují žádná zvláštní pravidla, která by toto zpracování ze strany donucovacího orgánu umožňovala.

6.3. Nezbytnost a přiměřenost

Využívání služby ze strany donucovacího orgánu znamená, že osobní údaje jsou sdíleny se soukromým subjektem, který využívá databázi, v níž jsou osobní údaje shromažďovány neomezeně a hromadně. Mezi shromážděnými osobními údaji a cílem, který donucovací orgán sleduje, neexistuje žádná souvislost. Sdílení údajů donucovacím orgánem se soukromým subjektem rovněž znamená nedostatečnou kontrolu tohoto orgánu nad údaji, které soukromý subjekt zpracovává, a velké potíže pro subjekty údajů při výkonu jejich práv, protože si nebudou vědomy toho, že jsou jejich údaje tímto způsobem zpracovávány. To nastavuje velmi vysokou laťku pro situace, kdy by k takovému zpracování mohlo docházet. Je sporné, zda by jakýkoliv cíl splňoval požadavky stanovené ve směrnici, neboť jakékoli odchylky od práva na soukromí a ochranu údajů a jeho omezení jsou použitelné pouze tehdy, je-li to zcela nezbytné. Obecný zájem účinnosti v boji proti závažné trestné činnosti nemůže sám o sobě odůvodnit zpracování v případech, kdy je bez rozdílu shromažďováno takovéto obrovské množství údajů. Toto zpracování by proto nesplňovalo požadavky na nezbytnost a přiměřenost.

6.4. Závěr

Absence jasných, přesných a předvídatelných pravidel, která by splňovala požadavky článků 4 a 10 směrnice, a nedostatek důkazů, že dané zpracování je zcela nezbytné k dosažení zamýšlených cílů,

vede k závěru, že používání této aplikace by nesplňovalo požadavky na nezbytnost a přiměřenost a znamenalo by nepřiměřený zásah do práv subjektů údajů na respektování soukromého života a ochranu osobních údajů podle Listiny.