[redacted]

Průběžné hodnocení zkušebního provozu informačního systému Digitálních podob osob využívajícím technologii „face recognition“

1. Úvod

Na základě rozkazu policejního prezidenta č. 194/2022, k zajištění zkušebního provozu informačního systému Digitálních podob osob (dále jen „**rozkaz**“) byl ke dni 22. srpna 2022 zahájen zkušební provoz informačního systému Digitálních podob osob (dále jen „**systém DPO**“). Částí druhou písm. a) rozkazu byl spravujícím orgánem systému DPO určen úřad služby kriminální policie a vyšetřování Policejního prezidia České republiky (dále jen „**úřad**“). V části třetí písm. a) bodu 3 a 4 bylo úřadu jakožto spravujícímu orgánu uloženo, aby provedl celkové vyhodnocení zkušebního provozu systému DPO a předložil policejnímu prezidentovi zprávu o stavu a průběhu zkušebního provozu, a to v termínu do 31. března 2023.

[redacted]

Obecným účelem zkušebního provozu informačního systému je připravit jej (a jeho současné i budoucí uživatele) na fungování v rámci ostrého provozu. To zahrnuje navržení a realizaci změn a nových funkcionalit, které umožní efektivnější práci se systémem a rozšíří možnosti jeho využití. Uvedené samozřejmě nevylučuje následný rozvoj v rámci ostrého provozu.

[redacted]

Předkládaný dokument shrnuje dosavadní průběh zkušebního provozu systému DPO, a to po stránce technické a provozní (funkčnost a využitelnost systému, statistické údaje, realizace změnových požadavků), uživatelské (praktické zkušenosti – provázanost s technickou stránkou) a též po stránce legislativní.

2. Legislativní rámec a popis systému

Při nastavování komplexního procesu, jakým systém sloužící k rozpoznávání tváří a čerpající z několika extrémně rozsáhlých zdrojových databází bezesporu je, je nutné, aby Policie České republiky (dále jen „**policie**“) respektovala celou škálu právních předpisů včetně ostatních pramenů a doporučujících norem.

Automatické rozpoznávání tváří (facial či face recognition) je specifickým druhem technologie pracující s biometrickými údaji[1], jejíž cílem je určit či ověřit totožnost jednotlivce pomocí fotografie jeho obličeje. Mezi tzv. „biometrické technologie" lze zařadit technologie na rozpoznávání otisků prstů, podpisu, DNA, oční duhovky a sítnice, hlasu, chůze, geometrie rukou a právě technologie rozpoznávání obličejů.[2] Zpracování biometrických údajů je ve smyslu čl. 9 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 a o zrušení směrnice 95/46/ES (dále jen „**obecné nařízení o ochraně osobních údajů**" nebo „**GDPR**") zpracováním tzv. zvláštních kategorií osobních údajů[3], tyto zvláštní kategorie osobních údajů obecně požívají větší míry právní ochrany než ostatní „standardní" osobní údaje.

Teorie rozeznává různé způsoby využití technologie automatického rozpoznávání tváří, mezi ty základní pak patří:

- Detekce (*Je na fotografii či záznamu obličej?)* – nástroj detekuje přítomnost obličeje na obrazu za pomocí umělé neurální sítě;

- Identifikace *(Čí obličej je na fotografii?)* – nástroj porovná zvolený obraz (např. vstupní fotografii obličeje) s obrazy v určené databázi (referenční databázi) a konstatuje shodu. Na tomto v zásadě jednoduchém principu hodlá fungovat informační systém Digitálních podob osob;

- Verifikace *(Shodují se tyto dva obličeje? Popř. v jaké míře?)* – nástroj v tomto případě porovná dva obrazy osoby a na základě určité míry citlivosti a pravděpodobnosti ověří, zda druhý obraz obsahuje shodnou osobu jako první obraz. Nástroj však k ověření nemusí nutně znát identitu osoby. Logicky zde dochází k definičnímu překryvu s předchozím bodem „Identifikace";

---

[1] Biometrickými údaji se ve smyslu čl. 4 odst. 14 obecného nařízení o ochraně osobních údajů rozumí osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.

[2] Blíže Biometrics Institute, 2021. Dostupné online z https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

[3] Článek 9 odst. 1 obecného nařízení o ochraně osobních údajů stanoví obecný zákaz zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby, s výjimkou případů uvedených v druhém odstavci.

Na řešenou situaci nicméně popsaný zákaz nedopadá, neboť zpracování osobních údajů probíhá v režimu „trestněprávní směrnice", tj. směrnice Evropského parlamentu a Rady (EU) 2016/680, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV, potažmo pak v režimu části první, hlavy III. zákona č. 110/2019 Sb., o zpracování osobních údajů.

[redacted]

- Klasifikace / Zařazení *(Co se mohu z obličeje dozvědět?)* – model je schopen z vyobrazení tváře extrahovat jednotlivé prvky a na základě těchto podmínit řadu vlastností zobrazené osoby jako věk, pohlaví, momentální emoční rozpoložení apod.[4]

Policie zaujala ve vztahu k úpravě soukromí jednotlivce opatrný a bezpečný přístup spočívající ve využití technologie pouze pro zpětnou identifikaci osob ze záznamu a jen pro zákonem stanovený okruh případů. Postupně hodlá do referenční databáze IS DPO zavádět jednotlivé zdrojové evidence, které jsou zmíněny níže.

Systém DPO využívající technologii automatického rozpoznávání obličejů (anglicky *„face recognition"*) je celostátní, automatizovaný systém provozovaný policií ve zkušebním provozu na základě § 66a zákona č. 273/2008 Sb., o Policii České republiky (dále jen „zákon o policii"), v datové síti intranet Ministerstva vnitra Hermes. Účelem systému DPO je poskytnutí podpůrného operativního nástroje napomáhajícího identifikaci zájmové osoby za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech. Z uvedeného tak vyplývá jednak skutečnost, že závěry předložené systémem není možné vnímat jako jednoznačné ztotožnění osoby, a jednak je jeho textací nastíněn okruh případů, kdy je možné systém DPO využívat.

Systém DPO je zjednodušeně řečeno tvořen referenční databází, softwarem sloužícím k automatickému rozpoznávání obličejů (algoritmus) a webovým grafickým uživatelským rozhraním pro nahrání vstupní fotografie a zobrazení výsledků. Referenční databáze může ze zákona (§ 66a odst. 1 zákona o policii) obsahovat fotografie z více externích zdrojových databází, konkrétně pak z:

- informačního systému evidence občanských průkazů,
- informačního systému evidence cestovních dokladů,
- informačního systému evidence diplomatických a služebních pasů,
- registru řidičů,
- centrálního registru řidičů, nebo
- informačního systému cizinců.

Dle právního výkladu spravujícího orgánu má Policie České republiky (dále jen „**policie**") navíc oprávnění k využití v IS DPO též fotografie [redacted]

[4] Blíže viz Leslie, D. (2020). Understanding bias in facial recognition technologies: an explainer.The Alan Turing Institute. Dostupné online z https://zenodo.org/record/4050457#.Yp8SXNpByHu

[5] Touto cestou se vydalo například Německo či Rakousko. Konkrétně rakouská obdoba FODAGEN s názvem EDE byla dlouho jediným zdrojem pro jejich GES (Gesichtserkennungsystem). Až v důsledku migrační krize přistoupili k využití rakouského informačního systému cizinců.

[redacted]

[redacted]

Úřad jakožto spravující orgán si za účelem plnění povinností v oblasti ochrany osobních údajů rovněž nastavil interní mechanismus vyžádání logů od provozovatele, na základě kterých bude provádět kontrolní činnost spočívající v ověřování oprávněnosti přístupů k osobním údajům v rámci IS DPO.

V případě zapracování některých požadavků a návrhů týkajících se technické či uživatelské stránky věci je úřad samozřejmě připraven odpovídajícím způsobem upravit též znění souvisejících podkladů, zejména pak samotný rozkaz, nastane-li taková potřeba.

3. Technická stránka

[redacted]

[redacted]

[redacted]

6 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

7 § 66a odst. 2 zákona č. 273/2008 Sb., o Policii České republiky.

8 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4. Žádosti a praktické aspekty

[redacted]

[redacted]

[redacted]

[redacted]

9 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

10 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

11 [redacted]

[redacted]

[redacted]

5. Shrnutí priorit, závěr

[redacted]

[redacted]

12 [redacted]