Wytyczne 05/2022 w sprawie wykorzystania technologii rozpoznawania twarzy w obszarze ścigania przestępstw

Wersja 2.0

Przyjęta 26 kwietnia 2023 r.

Historia wersji

Wersja 1.0	12 maja 2022 r.	Przyjęcie wytycznych do konsultacji publicznych
Wersja 2.0	26 kwietnia 2023 r.	Przyjęcie wytycznych po konsultacjach publicznych

Spis treści

Streszczenie 5

1 Wprowadzenie 8

2 Technologia 9

2.1 Jedna technologia biometryczna, dwie odrębne funkcje 9

2.2 Szerokie spektrum celów i zastosowań 11

2.3 Wiarygodność, dokładność i ryzyko dla osób, których dane dotyczą 13

3 Obowiązująca podstawa prawna 15

3.1 Ogólne ramy prawne – Karta praw podstawowych Unii Europejskiej i Konwencja o ochronie praw człowieka i podstawowych wolności (EKPC) 15

3.1.1 Zastosowanie Karty 15

3.1.2 Ingerencja w prawa określone w Karcie 16

3.1.3 Uzasadnienie ingerencji 16

3.2 Szczegółowe ramy prawne – dyrektywa o ochronie danych w sprawach karnych 21

3.2.1 Przetwarzanie szczególnych kategorii danych do celów ścigania przestępstw 21

3.2.2 Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie 24

3.2.3 Kategorie osób, których dane dotyczą 24

3.2.4 Prawa osoby, której dane dotyczą 25

3.2.5 Inne wymogi prawne i zabezpieczenia 29

4 Wniosek 32

5 Załączniki 33

Załącznik I – Szablon opisu scenariuszy 34

Załącznik II: Praktyczne wytyczne dotyczące zarządzania projektami FRT w organach ścigania 36

1. ROLE I OBOWIĄZKI 36

2. ROZPOCZĘCIE/PRZED ZAKUPEM SYSTEMU FRT 38

3. PODCZAS ZAKUPU I PRZED WDROŻENIEM FRT 40

4. ZALECENIA PO WDROŻENIU FRT 41

Załącznik III – PRAKTYCZNE PRZYKŁADY 42

1 Scenariusz 1 42

1.1. Opis 42

1.2. Obowiązująca podstawa prawna 43

1.3. Konieczność i proporcjonalność – cel/waga przestępstwa 44

1.4. Wniosek 44

2 Scenariusz 2 44

2.1. Opis 44
2.2. Obowiązująca podstawa prawna 45
2.3. Konieczność i proporcjonalność – cel / waga przestępstwa / liczba osób niezaangażowanych, ale na które przetwarzanie danych ma wpływ 45
2.4. Wniosek 46
3 Scenariusz 3 46
3.1. Opis 46
3.2. Obowiązująca podstawa prawna 48
3.3. Konieczność i proporcjonalność 48
3.4. Wniosek 49
4 Scenariusz 4 49
4.1. Opis 49
4.2. Obowiązująca podstawa prawna 50
4.3. Konieczność i proporcjonalność 50
4.4. Wniosek 50
5 Scenariusz 5 51
5.1. Opis 51
5.2. Obowiązująca podstawa prawna 52
5.3. Konieczność i proporcjonalność 52
5.4. Wniosek 55
6 Scenariusz 6 55
6.1. Opis 55
6.2. Obowiązująca podstawa prawna 56
6.3. Konieczność i proporcjonalność 56
6.4. Wniosek 56

STRESZCZENIE

Coraz więcej organów ścigania wykorzystuje lub zamierza wykorzystywać technologię rozpoznawania twarzy (FRT). Umożliwia ona **uwierzytelnienie** lub **identyfikację** osoby i można ją stosować na nagraniach wideo (np. CCTV) lub zdjęciach. Można ją wykorzystywać do różnych celów, w tym do wyszukiwania osób znajdujących się na policyjnych listach zagrożeń lub do monitorowania ruchów danej osoby w przestrzeni publicznej.

FRT opiera się na przetwarzaniu **danych biometrycznych**, a zatem obejmuje przetwarzanie szczególnych kategorii danych osobowych. FRT często wykorzystuje komponenty **sztucznej inteligencji** (AI) lub uczenia maszynowego. Umożliwia to przetwarzanie danych na dużą skalę, ale stwarza również ryzyko dyskryminacji i błędnych wyników. FRT może być wykorzystywana w kontrolowanych sytuacjach 1:1, ale również w przypadku ogromnych tłumów i ważnych węzłów transportowych.

FRT jest **narzędziem wrażliwym z punktu widzenia organów ścigania**. Organy ścigania są organami wykonawczymi i posiadają suwerenne uprawnienia. FRT może ingerować w prawa podstawowe – również wykraczać poza prawo do ochrony danych osobowych – i może wpływać na naszą społeczną i demokratyczną stabilność polityczną.

W odniesieniu do ochrony danych osobowych w kontekście ścigania przestępstw należy spełnić **wymogi dyrektywy o ochronie danych w sprawach karnych**. Pewne ramy dotyczące korzystania z FRT określono w dyrektywie o ochronie danych w sprawach karnych, w szczególności w art. 3 ust. 13 dyrektywy (termin „dane biometryczne"), art. 4 (zasady dotyczące przetwarzania danych osobowych), art. 8 (zgodność przetwarzania z prawem), art. 10 (przetwarzanie szczególnych kategorii danych osobowych) i art. 11 dyrektywy (zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach).

Zastosowanie FRT może mieć również wpływ na kilka innych praw podstawowych. Dlatego też **Karta praw podstawowych Unii Europejskiej** („Karta") ma zasadnicze znaczenie dla interpretacji dyrektywy o ochronie danych w sprawach karnych, w szczególności prawa do ochrony danych osobowych, o którym mowa w art. 8 Karty, ale także prawa do prywatności, o którym mowa w art. 7 Karty.

Akty prawne, które służą jako podstawa prawna do przetwarzania danych osobowych, bezpośrednio ingerują w prawa zagwarantowane w art. 7 i 8 Karty. W każdych okolicznościach samo przetwarzanie danych biometrycznych stanowi poważną ingerencję. Nie zależy to od wyniku, np. dopasowania pozytywnego. Wszelkie ograniczenia w korzystaniu z praw podstawowych i wolności muszą być przewidziane ustawą i szanować istotę tych praw i wolności.

Podstawa prawna musi być **wystarczająco jasna**, aby zapewnić obywatelom odpowiednie wskazanie warunków i okoliczności, w których organy są uprawnione do korzystania z wszelkich środków gromadzenia danych i tajnego nadzoru. Sama transpozycja do prawa krajowego klauzuli ogólnej zawartej w art. 10 dyrektywy o ochronie danych w sprawach karnych byłaby nieprecyzyjna i nieprzewidywalna.

Zanim prawodawca krajowy stworzy nową podstawę prawną dla jakiejkolwiek formy przetwarzania danych biometrycznych z wykorzystaniem rozpoznawania twarzy, należy **skonsultować** się z właściwym organem nadzorczym ds. ochrony danych.

Akty prawne muszą być **odpowiednie** do osiągnięcia uzasadnionych celów, do których dąży przedmiotowe prawodawstwo. **Cel interesu ogólnego**, mimo że ma on fundamentalne znaczenie, sam w sobie nie uzasadnia ograniczenia prawa podstawowego. Akty prawne powinny być **zróżnicowane** i

ukierunkowane na osoby nimi objęte z uwzględnieniem celu, np. zwalczania konkretnych poważnych przestępstw. Jeżeli akt obejmuje wszystkie osoby w sposób ogólny, bez takiego zróżnicowania, ograniczenia lub wyjątku, zwiększa on ingerencję. Zwiększa on również ingerencję, jeśli przetwarzaniem danych objęta jest znaczna część populacji.

Dane muszą być przetwarzane w sposób zapewniający stosowanie unijnych przepisów i zasad dotyczących ochrony danych oraz ich skuteczność. Każdorazowo **ocena konieczności i proporcjonalności** musi również określać i uwzględniać wszelkie możliwe konsekwencje dla innych praw podstawowych. Systematyczne przetwarzanie danych bez wiedzy osób, których dane dotyczą, może wywołać **ogólne poczucie ciągłego nadzoru**. Może to prowadzić do „efektu mrożącego" w odniesieniu do niektórych lub wszystkich odnośnych praw podstawowych, takich jak godność ludzka na mocy art. 1 Karty, wolność myśli, sumienia i wyznania na mocy art. 10 Karty, wolność wypowiedzi na mocy art. 11 Karty, a także wolność zgromadzeń i zrzeszania się na mocy art. 12 Karty.

Przetwarzanie szczególnych kategorii danych, takich jak dane biometryczne, można uznać za „**bezwzględnie niezbędne**" (art. 10 dyrektywy o ochronie danych w sprawach karnych) tylko wtedy, gdy ingerencja w ochronę danych osobowych i ograniczenia z tym związane sprowadzają się do tego, co jest absolutnie konieczne, tj. niezbędne, z wyłączeniem przetwarzania o charakterze ogólnym lub systematycznym.

Fakt, że fotografia została w **sposób oczywisty upubliczniona** przez osobę, której dane dotyczą (art. 10 dyrektywy o ochronie danych w sprawach karnych), nie oznacza, że związane z tym dane biometryczne, które można uzyskać z fotografii za pomocą określonych środków technicznych, zostały w sposób oczywisty upublicznione. Domyślne ustawienia usługi, np. publiczne udostępnianie wzorców lub brak możliwości wyboru, np. wzorce są upubliczniane bez możliwości zmiany tego ustawienia przez użytkownika, nie powinny być w żaden sposób interpretowane jako dane upubliczniane w sposób oczywisty.

W art. 11 dyrektywy o ochronie danych w sprawach karnych ustanawia się ramy dla **zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach**. Korzystanie z FRT wiąże się z wykorzystaniem szczególnych kategorii danych i może prowadzić do profilowania, w zależności od sposobu i celu stosowania FRT. W każdym przypadku, zgodnie z prawem Unii i art. 11 ust. 3 dyrektywy o ochronie danych w sprawach karnych, profilowanie skutkujące dyskryminacją osób fizycznych na podstawie danych osobowych szczególnych kategorii jest zabronione.

Artykuł 6 dyrektywy o ochronie danych w sprawach karnych dotyczy konieczności **rozróżniania poszczególnych kategorii osób, których dane dotyczą**. W odniesieniu do osób, których dane dotyczą, co do których brak jest dowodów mogących sugerować, że ich zachowanie może mieć związek, chociażby pośredni i daleki, ze zgodnym z prawem celem określonym w dyrektywie o ochronie danych w sprawach karnych, najprawdopodobniej nie ma uzasadnienia dla ingerencji.

Zasada minimalizacji danych (art. 4 ust. 1 lit. e) dyrektywy o ochronie danych w sprawach karnych) wymaga również, aby wszelkie materiały wideo niemające znaczenia dla celu przetwarzania przed wdrożeniem były zawsze usuwane lub anonimizowane (np. poprzez rozmycie bez możliwości odzyskania danych).

Administrator musi dokładnie rozważyć, w jaki sposób (lub czy może) spełnić wymogi dotyczące **praw osoby, której dane dotyczą**, przed rozpoczęciem jakiegokolwiek przetwarzania FRT, ponieważ stosowanie FRT często wiąże się z przetwarzaniem szczególnych kategorii danych osobowych bez widocznej interakcji z osobą, której dane dotyczą.

Skuteczne wykonywanie praw osoby, której dane dotyczą, zależy od tego, czy administrator wypełnia swoje **obowiązki informacyjne** (art. 13 dyrektywy o ochronie danych w sprawach karnych). Oceniając, czy istnieje „konkretny przypadek" zgodnie z art. 13 ust. 2 dyrektywy o ochronie danych w sprawach karnych, należy wziąć pod uwagę kilka czynników, w tym to, czy dane osobowe są gromadzone bez wiedzy osoby, której dane dotyczą, ponieważ byłby to jedyny sposób, aby osoby, których dane dotyczą, mogły skutecznie wykonywać przysługujące im prawa. Jeżeli decyzje podejmowane są wyłącznie na podstawie zastosowania FRT, osoby, których dane dotyczą, muszą zostać poinformowane o funkcjach zautomatyzowanego podejmowania decyzji.

W odniesieniu do **wniosków o udzielenie dostępu**, gdy dane biometryczne są przechowywane i powiązane z tożsamością również za pomocą danych alfanumerycznych, zgodnie z zasadą minimalizacji danych, właściwy organ powinien mieć możliwość potwierdzenia wniosku o udzielenie dostępu na podstawie wyników wyszukiwania tych danych alfanumerycznych i bez dalszego przetwarzania danych biometrycznych innych osób (tj. poprzez wyszukiwanie za pomocą FRT w bazie danych).

Dla osób, których dane dotyczą, ryzyko jest szczególnie poważne, jeśli w policyjnej bazie danych przechowywane są niedokładne (nieprawidłowe) dane lub są one udostępniane innym podmiotom. Administrator musi odpowiednio **skorygować** przechowywane dane i systemy FRT (zob. również motyw 47 dyrektywy o ochronie danych w sprawach karnych).

Prawo do **ograniczenia** staje się szczególnie ważne, jeśli chodzi o technologię rozpoznawania twarzy (opartą na algorytmie (algorytmach), a tym samym nigdy niewykazującą ostatecznego wyniku) w sytuacjach, w których gromadzone są duże ilości danych, a dokładność i jakość identyfikacji może się różnić.

Ocena skutków dla ochrony danych przed zastosowaniem FRT jest obowiązkowym wymogiem, por. art. 27 dyrektywy o ochronie danych w sprawach karnych. EROD zaleca podanie wyników takich ocen lub co najmniej głównych ustaleń i wniosków zawartych w ocenie skutków dla ochrony danych do wiadomości publicznej jako środek wspierający zaufanie i przejrzystość.

Większość przypadków wdrażania i wykorzystywania FRT wiąże się z nieodłącznym wysokim ryzykiem naruszenia praw i wolności osób, których dane dotyczą. W związku z tym organ wdrażający FRT powinien **skonsultować** się z właściwym organem nadzorczym przed wdrożeniem systemu.

Biorąc pod uwagę unikalny charakter danych biometrycznych, organ wdrażający lub wykorzystujący FRT powinien zwrócić szczególną uwagę na **bezpieczeństwo przetwarzania danych**, zgodnie z art. 29 dyrektywy o ochronie danych w sprawach karnych. W szczególności organ ścigania powinien zapewnić zgodność systemu z odpowiednimi normami i wdrożyć środki ochrony wzorców biometrycznych. Zasady ochrony danych i zabezpieczenia muszą być wbudowane w technologię przed rozpoczęciem przetwarzania danych osobowych. W związku z tym nawet jeżeli organ ścigania zamierza zastosować i wykorzystać narzędzia FRT od zewnętrznych dostawców, musi zapewnić, np. w drodze postępowania o udzielenie zamówienia, aby stosowane były wyłącznie narzędzia FRT oparte na zasadach **uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych**.

Ewidencjonowanie (zob. art. 25 dyrektywy o ochronie danych w sprawach karnych) stanowi ważne zabezpieczenie weryfikacji zgodności z prawem przetwarzania, zarówno wewnętrznie (tj. monitorowanie własnej działalności danego administratora/podmiotu przetwarzającego), jak i przez zewnętrzne organy nadzorcze. W kontekście systemów rozpoznawania twarzy zaleca się również ewidencjonowanie zmian w referencyjnej bazie danych oraz prób identyfikacji lub weryfikacji, w tym użytkownika, wyniku i wskaźnika zaufania. Ewidencjonowanie jest jednak tylko jednym z podstawowych elementów ogólnej **zasady rozliczalności** (zob. art. 4 ust. 4 dyrektywy o ochronie

danych w sprawach karnych). Administrator musi być w stanie wykazać zgodność przetwarzania z podstawowymi zasadami ochrony danych określonymi w art. 4 ust. 1–3 dyrektywy o ochronie danych w sprawach karnych.

Europejska Rada Ochrony Danych przypomina wspólny apel EIOD i EROD **o zakazanie** niektórych rodzajów przetwarzania w odniesieniu do (1) zdalnej identyfikacji biometrycznej osób fizycznych w publicznie dostępnych przestrzeniach, (2) wspieranych przez sztuczną inteligencję systemów rozpoznawania twarzy dzielących osoby fizyczne w oparciu o ich dane biometryczne na grupy ze względu na pochodzenie etniczne, płeć, poglądy polityczne lub orientację seksualną lub z innych względów, które stanowią podstawę zakazu dyskryminacji, (3) wykorzystania rozpoznawania twarzy lub podobnych technologii w celu wykrywania emocji osoby fizycznej oraz (4) przetwarzania danych osobowych w kontekście ścigania przestępstw, które opierałoby się na bazie danych utworzonej poprzez gromadzenie danych osobowych na masową skalę i w sposób niekontrolowany, np. poprzez pozyskiwanie (ang. scraping) zdjęć i obrazów twarzy dostępnych online.

Głównym zabezpieczeniem praw podstawowych, o których mowa, jest **skuteczny nadzór** ze strony właściwych organy nadzorczych ds. ochrony danych. W związku z tym państwa członkowskie muszą zapewnić, aby zasoby organów nadzorczych były odpowiednie i wystarczające, co pozwoli im wypełniać ich mandat.

Niniejsze wytyczne **skierowane są do prawodawców** na szczeblu unijnym i krajowym, a także do organów ścigania i ich funkcjonariuszy wdrażających i korzystających z systemów FRT. Wytyczne skierowane są do osób fizycznych w zakresie, w jakim są one zainteresowane ogólnie lub jako osoby, których dane dotyczą, w szczególności w odniesieniu do praw osób, których dane dotyczą.

Celem wytycznych jest informowanie o niektórych właściwościach FRT i mających zastosowanie ramach prawnych w kontekście ścigania przestępstw (w szczególności dyrektywy o ochronie danych w sprawach karnych).

- Ponadto stanowią one **narzędzie wspierające pierwszą klasyfikację wrażliwości danego przypadku użycia** (załącznik I).
- Zawierają one również **praktyczne wytyczne dla organów ścigania, które chcą zamówić i uruchomić system FRT** (załącznik II).
- W wytycznych przedstawiono również kilka typowych **przypadków użycia i wymieniono szereg istotnych okoliczności**, zwłaszcza w odniesieniu do analizy konieczności i proporcjonalności (załącznik III).

1 WPROWADZENIE

1. Technologia rozpoznawania twarzy (FRT) może być wykorzystywana do automatycznego rozpoznawania osób fizycznych na podstawie ich twarzy. FRT często opiera się na sztucznej inteligencji, takiej jak technologie uczenia maszynowego. Aplikacje FRT są w coraz większym stopniu testowane i wykorzystywane w różnych obszarach, począwszy od indywidualnych zastosowań, a skończywszy na organizacjach prywatnych i administracji publicznej. Organy ścigania również spodziewają się korzyści ze stosowania FRT. Technologia ta oferuje rozwiązania dla stosunkowo nowych wyzwań, takich jak dochodzenia obejmujące dużą ilość przechwyconych dowodów, ale także dla znanych problemów, w szczególności związanych z niedoborem personelu do zadań obserwacyjnych i poszukiwawczych.

2. Wzrost zainteresowania FRT w dużej mierze wynika z wydajności i skalowalności FRT. Wiążą się z tym pewne niedogodności charakterystyczne dla tej technologii i jej zastosowania – również na dużą skalę. Podczas gdy mogą istnieć tysiące zbiorów danych osobowych, które można analizować po wciśnięciu jednego przycisku, już niewielkie skutki algorytmicznej dyskryminacji lub błędnej identyfikacji mogą spowodować, że wiele osób odczuje poważne konsekwencje w swoim postępowaniu i codziennym życiu. Sama wielkość przetwarzania danych osobowych, a w szczególności danych biometrycznych, jest kolejnym kluczowym elementem FRT, ponieważ przetwarzanie danych osobowych stanowi ingerencję w podstawowe prawo do ochrony danych osobowych zgodnie z art. 8 Karty praw podstawowych Unii Europejskiej (Karta).

3. Stosowanie FRT przez organy ścigania będzie miało – i do pewnego stopnia już ma — istotne konsekwencje dla poszczególnych osób i grup osób, w tym mniejszości. Konsekwencje te będą miały również znaczący wpływ na sposób, w jaki żyjemy razem oraz na naszą społeczną i demokratyczną stabilność polityczną, w której doceniamy duże znaczenie pluralizmu i opozycji politycznej. Prawo do ochrony danych osobowych jest często kluczem do zagwarantowania innych praw podstawowych. Stosowanie FRT może w znacznym stopniu kolidować z prawami podstawowymi w stopniu wykraczającym poza prawo do ochrony danych osobowych.

4. W związku z tym EROD uważa, że ważne jest, aby przyczynić się do ciągłej integracji FRT w obszarze ścigania przestępstw objętym dyrektywą o ochronie danych w sprawach karnych[1], a także krajowymi przepisami transponującymi tę dyrektywę i przedstawić niniejsze wytyczne. Wytyczne mają na celu dostarczenie istotnych informacji prawodawcom na szczeblu unijnym i krajowym, a także organom ścigania i ich funkcjonariuszom podczas wdrażania i korzystania z systemów FRT. Zakres wytycznych ogranicza się do FRT. Inne formy przetwarzania danych osobowych przez organy ścigania na podstawie danych biometrycznych, zwłaszcza jeżeli są przetwarzane zdalnie, mogą jednak wiązać się z podobnymi lub dodatkowymi zagrożeniami dla osób fizycznych, grup i społeczeństwa. W zależności od okoliczności, niektóre aspekty tych wytycznych mogą służyć jako przydatne źródło informacji również w tych przypadkach. Wreszcie, wytyczne zawierają ważne informacje dla osób fizycznych, które są zainteresowane tematem ogólnie lub jako osoby, których dane dotyczą, w szczególności w odniesieniu do praw osób, których dane dotyczą.

5. Wytyczne składają się z głównego dokumentu i trzech załączników. W głównym dokumencie przedstawiono technologię i obowiązujące ramy prawne. Szablon pomocny w określeniu niektórych głównych aspektów klasyfikacji stopnia ingerencji w prawa podstawowe w danym obszarze zastosowania można znaleźć w załączniku I. Organy ścigania, które chcą zamówić i uruchomić system FRT, mogą znaleźć praktyczne wskazówki w załączniku II. W zależności od obszaru zastosowania FRT, różne względy mogą być istotne. Zestaw hipotetycznych scenariuszy i odpowiednich rozważań można znaleźć w załączniku III.

2 TECHNOLOGIA

2.1 Jedna technologia biometryczna, dwie odrębne funkcje

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

6. Rozpoznawanie twarzy to technologia oparta na prawdopodobieństwie, dzięki której możliwe jest automatyczne rozpoznawanie osób na podstawie ich twarzy w celu ich uwierzytelnienia lub identyfikacji.

7. FRT należy do szerszej kategorii technologii biometrycznej. Biometria obejmuje wszystkie zautomatyzowane procesy wykorzystywane do rozpoznawania osoby poprzez kwantyfikację cech fizycznych, fizjologicznych lub behawioralnych (odciski palców, struktura tęczówki, głos, chód, układ naczyń krwionośnych itp.) Cechy te definiuje się jako „dane biometryczne", ponieważ umożliwiają one lub potwierdzają jednoznaczną identyfikację danej osoby.

8. Tak jest w przypadku ludzkich twarzy, a dokładniej ich technicznego przetwarzania za pomocą urządzeń do rozpoznawania twarzy: dzięki obrazowi twarzy (zdjęcie lub wideo) zwanemu „próbką" biometryczną, możliwe jest wyodrębnienie cyfrowej reprezentacji wyraźnych cech tej twarzy (nazywa się to „wzorcem").

9. Wzorzec biometryczny jest cyfrową reprezentacją unikalnych cech, które zostały wyodrębnione z próbki biometrycznej i mogą być przechowywane w bazie danych biometrycznych[2]. Wzorzec ten ma być unikalny i specyficzny dla każdej osoby i z zasady nie zmienia się z upływem czasu[3]. Na etapie rozpoznawania urządzenie porównuje ten wzorzec z innymi wzorcami uprzednio wyprodukowanymi lub obliczonymi bezpośrednio z próbek biometrycznych, takimi jak twarze znalezione na obrazie, zdjęciu lub nagraniu wideo. „Rozpoznawanie twarzy" jest zatem procesem dwuetapowym: zebranie obrazu twarzy i jego przekształcenie we wzorzec, a następnie rozpoznanie tej twarzy poprzez porównanie odpowiedniego wzorca z jednym lub kilkoma innymi wzorcami.

10. Podobnie jak w przypadku każdego procesu biometrycznego, rozpoznawanie twarzy może pełnić dwie odrębne funkcje:

    - **uwierzytelnianie** osoby, które ma na celu sprawdzenie, czy dana osoba jest tym, za kogo się podaje. W takim przypadku system porówna wcześniej zapisany wzorzec lub próbkę biometryczną (np. przechowywaną na karcie elektronicznej lub paszporcie biometrycznym) z pojedynczą twarzą, taką jak twarz osoby pojawiającej się w punkcie kontrolnym, w celu zweryfikowania, czy jest to jedna i ta sama osoba. W związku z tym funkcja ta opiera się na porównaniu dwóch wzorców. Proces ten nazywa się również **weryfikacją** 1 do 1;

    - **identyfikacja** osoby w celu znalezienia osoby wśród grupy osób w określonym obszarze, na określonym obrazie lub w bazie danych. W takim przypadku system musi przetworzyć każdą uchwyconą twarz, aby wygenerować wzorzec biometryczny, a następnie sprawdzić, czy pasuje on do osoby znanej systemowi. Funkcjonalność ta opiera się zatem na porównaniu jednego wzorca z bazą danych wzorców lub próbek (wzorzec bazowy). Nazywa się to również identyfikacją 1 do wielu. Na przykład, system może powiązać zapis danych osobowych (nazwisko, imię) z twarzą, jeśli porównanie zostanie dokonane z bazą danych zdjęć powiązanych z nazwiskami i imionami. Proces ten może również polegać na podążaniu za osobą w tłumie, bez konieczności powiązania jej z tożsamością cywilną.

11. W obu przypadkach stosowane techniki rozpoznawania twarzy opierają się na szacunkowym dopasowaniu między wzorcami: wzorcem porównywanym a bazowym. Z tego punktu widzenia są one oparte na prawdopodobieństwie: porównanie określa wyższe lub niższe prawdopodobieństwo, że

[2] Wytyczne dotyczące rozpoznawania twarzy, Komitet Konsultacyjny Konwencji nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, Rada Europy, czerwiec 2021 r.

[3] Może to zależeć od rodzaju biometrii oraz wieku osoby, której dane dotyczą.

dana osoba jest rzeczywiście osobą, która ma zostać uwierzytelniona lub zidentyfikowana; jeśli prawdopodobieństwo to przekroczy określony próg w systemie, zdefiniowany przez użytkownika lub twórcę systemu, system przyjmie, że istnieje zgodność.

12. Chociaż obie funkcje – uwierzytelnianie i identyfikacja – są odrębne, obie dotyczą przetwarzania danych biometrycznych związanych ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, a zatem stanowią przetwarzanie danych osobowych, a w szczególności przetwarzanie szczególnych kategorii danych osobowych.

13. Rozpoznawanie twarzy jest częścią szerszego spektrum technik przetwarzania obrazu wideo. Niektóre kamery wideo mogą filmować ludzi w określonym obszarze, w szczególności ich twarze, ale nie mogą być używane jako takie do automatycznego rozpoznawania osób. To samo dotyczy zwykłej fotografii: aparat fotograficzny nie jest systemem rozpoznawania twarzy, ponieważ zdjęcia osób muszą być przetwarzane w określony sposób w celu wyodrębnienia danych biometrycznych.

14. Samo wykrywanie twarzy za pomocą tzw. inteligentnych kamer również niekoniecznie stanowi system rozpoznawania twarzy. Chociaż techniki cyfrowe służące do wykrywania nietypowych zachowań lub zdarzeń związanych z przemocą lub do rozpoznawania emocji na twarzy, a nawet sylwetek, również budzą istotne wątpliwości pod względem etyki i skuteczności, nie można ich uznać za systemy biometryczne przetwarzające szczególne kategorie danych osobowych, pod warunkiem, że nie mają one na celu jednoznacznej identyfikacji osoby, a przetwarzanie danych osobowych nie obejmuje innych szczególnych kategorii danych osobowych. Powyższe przykłady nie są całkowicie niezwiązane z funkcją rozpoznawania twarzy i nadal podlegają zasadom ochrony danych osobowych[4]. Ponadto ten rodzaj systemu wykrywania może być używany w połączeniu z innymi systemami mającymi na celu identyfikację osoby, a tym samym może zostać uznany za technologię rozpoznawania twarzy.

15. W przeciwieństwie np. do systemów wychwytywania i przetwarzania wideo, które wymagają instalacji urządzeń fizycznych, rozpoznawanie twarzy jest funkcją oprogramowania, którą można wdrożyć w ramach istniejących systemów (kamery, bazy danych obrazów itp.). Taka funkcjonalność może być zatem połączona lub zintegrowana z wieloma systemami i powiązana z innymi funkcjami. Taka integracja z już istniejącą infrastrukturą wymaga szczególnej uwagi, ponieważ wiąże się z nieodłącznym ryzykiem wynikającym z faktu, że technologia rozpoznawania twarzy może być niewidoczna i łatwa do ukrycia[5].

2.2 Szerokie spektrum celów i zastosowań

16. Poza zakresem niniejszych wytycznych i poza zakresem dyrektywy o ochronie danych w sprawach karnych rozpoznawanie twarzy może być wykorzystywane do wielu różnych celów, zarówno do celów komercyjnych, jak i do rozwiązywania problemów związanych z bezpieczeństwem publicznym lub ściganiem przestępstw. Może być stosowane do różnych celów: w bezpośredniej relacji między użytkownikiem a usługą (dostęp do aplikacji), w celu uzyskania dostępu do określonego miejsca (fizyczne filtrowanie) lub bez żadnych szczególnych ograniczeń w przestrzeni publicznej (rozpoznawanie twarzy na żywo). Może być stosowane do każdej osoby, której dane dotyczą: klienta usługi, pracownika, zwykłego obserwatora, osoby poszukiwanej lub osoby zaangażowanej w postępowanie prawne lub administracyjne itp. Niektóre zastosowania są już powszechne i szeroko stosowane; inne są w tym momencie na etapie eksperymentalnym lub spekulacyjnym. Chociaż

[4] Artykuł 10 dyrektywy o ochronie danych w sprawach karnych (lub art. 9 RODO) ma jednak zastosowanie do systemów, które wykorzystuje się do kategoryzowania osób fizycznych na podstawie ich danych biometrycznych w grupy według pochodzenia etnicznego, a także orientacji politycznej lub seksualnej lub innych szczególnych kategorii danych osobowych.

[5] Na przykład w kamerach noszonych na ciele, które coraz częściej wykorzystuje się w praktyce.

niniejsze wytyczne nie będą dotyczyć wszystkich takich zastosowań i aplikacji, EROD przypomina, że mogą one być wdrażane tylko wtedy, gdy są zgodne z obowiązującymi ramami prawnymi, w szczególności z RODO i odpowiednimi przepisami krajowymi[6]. Nawet w kontekście dyrektywy o ochronie danych w sprawach karnych, poza funkcjami uwierzytelniania lub identyfikacji, dane przetwarzane przy użyciu technologii rozpoznawania twarzy mogą być dalej przetwarzane również do innych celów, takich jak kategoryzacja.

17. W szczególności można rozważyć skalę potencjalnych zastosowań w zależności od stopnia kontroli, jaką ludzie mają nad swoimi danymi osobowymi, skutecznych środków, jakimi dysponują w celu sprawowania takiej kontroli oraz ich prawa do inicjatywy w zakresie uruchamiania tej technologii i korzystania z niej, konsekwencji dla nich (w przypadku rozpoznania lub nierozpoznania) oraz skali przeprowadzanego przetwarzania. Rozpoznawanie twarzy w oparciu o wzorzec przechowywany na urządzeniu osobistym (karcie elektronicznej, smartfonie itp.) należącym do danej osoby, wykorzystywane do uwierzytelniania i ściśle osobistego użytku za pośrednictwem dedykowanego interfejsu, nie stwarza takiego samego ryzyka, jak na przykład wykorzystanie do celów identyfikacji, w niekontrolowanym środowisku, bez aktywnego zaangażowania osób, których dane dotyczą, gdzie wzorzec każdej twarzy wchodzącej do obszaru monitorowania jest porównywany z wzorcami z szerokiego przekroju populacji przechowywanymi w bazie danych. Pomiędzy tymi dwoma skrajnościami znajduje się bardzo zróżnicowane spektrum zastosowań i związanych z tym kwestii dotyczących ochrony danych osobowych.

18. W celu dalszego zilustrowania kontekstu, w jakim technologie rozpoznawania twarzy są obecnie omawiane lub wdrażane, zarówno w celu uwierzytelniania, jak i identyfikacji, EROD uważa za istotne przytoczenie szeregu przykładów. Poniższe przykłady mają charakter wyłącznie opisowy i nie powinny być traktowane jako jakakolwiek wstępna ocena ich zgodności z dorobkiem prawnym UE w dziedzinie ochrony danych.

Przykłady uwierzytelniania za pomocą rozpoznawania twarzy

19. Uwierzytelnianie może być zaprojektowane tak, aby użytkownicy mieli nad nim pełną kontrolę, na przykład w celu umożliwienia dostępu do usług lub aplikacji wyłącznie w warunkach domowych. W związku z tym jest ono szeroko stosowane przez właścicieli smartfonów do odblokowywania urządzeń zamiast uwierzytelniania hasłem.

20. Uwierzytelnianie za pomocą rozpoznawania twarzy może być również wykorzystywane do sprawdzania tożsamości osoby, która chce skorzystać z publicznych lub prywatnych usług osób trzecich. Takie procesy oferują zatem możliwość tworzenia tożsamości cyfrowej za pomocą aplikacji mobilnej (smartfona, tabletu itp.), którą można następnie wykorzystać do uzyskiwania dostępu do usług administracyjnych online.

21. Ponadto uwierzytelnianie za pomocą rozpoznawania twarzy może mieć na celu kontrolowanie fizycznego dostępu do jednej lub kilku z góry określonych lokalizacji, takich jak wejścia do budynków lub przekroczenia określonych przejść granicznych. Funkcja ta jest np. wdrażana w ramach niektórych operacji przetwarzania danych do celów przekraczania granicy, w ramach których twarz osoby znajdującej się na przejściu granicznym jest porównywana z twarzą przechowywaną w jej dokumencie tożsamości (paszporcie lub bezpiecznym dokumencie pobytowym).

Przykłady identyfikacji za pomocą rozpoznawania twarzy

[6] Zobacz również wytyczne EROD 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo przyjęte 29 stycznia 2020 r. w celu uzyskania dalszych wskazówek.

22. Identyfikację można stosować na wiele, nawet bardziej zróżnicowanych sposobów. Obejmuje ona między innymi zastosowania wymienione poniżej, które są obecnie stosowane na terytorium UE, są w fazie eksperymentalnej lub są w fazie planowania:

- przeszukiwanie, w bazie fotografii, tożsamości niezidentyfikowanej osoby (ofiary, podejrzanego itp.);
- monitorowanie ruchów danej osoby w przestrzeni publicznej. Twarz danej osoby jest porównywana z wzorcami biometrycznymi osób, które podróżują lub podróżowały w monitorowanym obszarze, na przykład w przypadku pozostawienia bagażu lub po popełnieniu przestępstwa;
- rekonstrukcja podróży danej osoby i jej późniejszych interakcji z innymi osobami, poprzez opóźnione porównanie tych samych elementów w celu zidentyfikowania na przykład jej kontaktów;
- zdalna identyfikacja biometryczna osób poszukiwanych w przestrzeni publicznej. Wszystkie twarze zarejestrowane na żywo przez kamery wideo są sprawdzane w czasie rzeczywistym w bazie danych prowadzonej przez siły bezpieczeństwa;
- automatyczne rozpoznawanie osób na obrazie w celu zidentyfikowania, na przykład, ich relacji w sieci społecznościowej, która z niej korzysta. Obraz jest porównywany z wzorcami wszystkich osób w sieci, które wyraziły zgodę na wykorzystanie tej funkcji, aby sugerować imienną identyfikację tych relacji;
- dostęp do usług, korzystanie z niektórych bankomatów z funkcją rozpoznawania twarzy klientów: twarz uchwycona przez kamerę jest porównywana do obrazów twarzy przechowywanych w bazie danych banku;
- śledzenie podróży pasażera na określonym etapie podróży. Obliczany w czasie rzeczywistym wzorzec każdej osoby odprawiającej się przy bramkach znajdujących się na określonych etapach podróży (punkty odbioru bagażu, bramki wejścia na pokład itp.) jest porównywany z wzorcami osób wcześniej zarejestrowanych w systemie.

23. Oprócz wykorzystania FRT w dziedzinie ścigania przestępstw, szeroki zakres zaobserwowanych zastosowań z pewnością wymaga kompleksowej debaty i podejścia politycznego w celu zapewnienia spójności i zgodności z dorobkiem prawnym UE w dziedzinie ochrony danych.

2.3 Wiarygodność, dokładność i ryzyko dla osób, których dane dotyczą

24. Jak w przypadku każdej technologii, rozpoznawanie twarzy może również wiązać się z wyzwaniami związanymi z jej wdrażaniem, w szczególności jeśli chodzi o jej niezawodność i skuteczność w zakresie uwierzytelniania lub identyfikacji, a także ogólną kwestię jakości i prawidłowości danych „źródłowych" oraz wyników przetwarzania technologii rozpoznawania twarzy.

25. Takie wyzwania technologiczne wiążą się ze szczególnym ryzykiem dla osób, których dane dotyczą, co jest tym bardziej znaczące lub groźne w obszarze ścigania przestępstw, biorąc pod uwagę możliwe skutki dla osób, których dane dotyczą, zarówno prawne, jak i inne, które w podobny sposób mogą mieć na te osoby istotny wpływ. W tym kontekście warto również podkreślić, że stosowanie FRT ex post nie jest samo w sobie bezpieczniejsze, ponieważ osoby fizyczne mogą być monitorowane przez cały czas i

w różnych miejscach. W związku z tym wykorzystanie tej technologii ex post wiąże się również z określonymi zagrożeniami, które należy oceniać indywidualnie dla każdego przypadku[7].

26. Jak wskazała Agencja Praw Podstawowych Unii Europejskiej w swoim sprawozdaniu z 2019 r., „określenie niezbędnego poziomu dokładności oprogramowania do rozpoznawania twarzy stanowi wyzwanie: istnieje wiele różnych sposobów oceny dokładności, również w zależności od zadania, celu i kontekstu jego użycia. Stosując tę technologię w miejscach odwiedzanych przez miliony osób – takich jak stacje kolejowe lub porty lotnicze – stosunkowo niewielki odsetek błędów (np. 0,01%)[8] nadal oznacza, że setki osób są błędnie oznaczone. Ponadto niektóre kategorie osób mogą być bardziej narażone na błędne dopasowanie niż inne, jak opisano w sekcji 3. Istnieją różne sposoby obliczania i interpretowania poziomów błędu, dlatego należy zachować ostrożność. Ponadto, jeżeli chodzi o dokładność i błędy, pytania dotyczące tego, jak łatwo można oszukać system, na przykład przez fałszywe wizerunki twarzy (zwane „spoofingiem"), są istotne zwłaszcza do celów ścigania przestępstw"[9].

27. W tym kontekście EROD uważa, że ważne jest przypomnienie, że FRT, niezależnie od tego, czy jest wykorzystywana do celów uwierzytelniania czy identyfikacji, nie zapewnia ostatecznego wyniku, ale opiera się na prawdopodobieństwie, że dwie twarze lub obrazy twarzy odpowiadają tej samej osobie[10]. Wynik ten ulega dalszemu pogorszeniu, gdy jakość próbki biometrycznej wprowadzanej do rozpoznawania twarzy jest niska. Nieostrość obrazów źródłowych, niska rozdzielczość kamery, ruch i słabe oświetlenie mogą przyczyniać się do niskiej jakości. Inne aspekty mające znaczący wpływ na wyniki to rozpowszechnienie i spoofing, np. gdy przestępcy próbują uniknąć przechodzenia obok kamer lub oszukać FRT. Liczne badania ujawniły również, że takie wyniki statystyczne z przetwarzania algorytmicznego mogą również być obarczone błędem, w szczególności wynikającym z jakości danych źródłowych, a także trenowania baz danych lub innych czynników, takich jak wybór lokalizacji wdrożenia. Ponadto należy również podkreślić wpływ technologii rozpoznawania twarzy na inne prawa podstawowe, takie jak poszanowanie życia prywatnego i rodzinnego, wolność wypowiedzi i informacji, wolność zgromadzeń i zrzeszania się itp.

28. Niezbędne jest zatem uwzględnienie niezawodności i dokładności technologii rozpoznawania twarzy jako kryteriów oceny zgodności z kluczowymi zasadami ochrony danych, zgodnie z art. 4 dyrektywy o ochronie danych w sprawach karnych, w szczególności jeśli chodzi o rzetelność i dokładność.

29. EROD zwraca uwagę na fakt, że wysokiej jakości dane są niezbędne dla wysokiej jakości algorytmów, a także podkreśla potrzebę, aby administratorzy, w ramach obowiązku rozliczalności, przeprowadzali regularną i systematyczną ocenę przetwarzania algorytmicznego w celu zapewnienia w szczególności dokładności, rzetelności i wiarygodności wyników takiego przetwarzania danych osobowych. Dane osobowe wykorzystywane do celów oceny, szkolenia i dalszego rozwoju systemów FRT mogą być przetwarzane wyłącznie na podstawie wystarczającej podstawy prawnej i zgodnie ze wspólnymi zasadami ochrony danych.

[7] Zobacz przykłady przedstawione w załączniku III.

[8] Ten wskaźnik dokładności wynika z cytowanego raportu i odzwierciedla wskaźnik znacznie lepszy niż obecna skuteczność algorytmów w zastosowaniach FRT.

[9] Technologia rozpoznawania twarzy: kwestie praw podstawowych w kontekście ściganie przestępstw, Agencja Praw Podstawowych Unii Europejskiej, 21 listopada 2019 r.

[10] Prawdopodobieństwo to określa się jako „wskaźnik zaufania".

3 OBOWIĄZUJĄCA PODSTAWA PRAWNA

30. Korzystanie z technologii rozpoznawania twarzy jest nierozerwalnie związane z przetwarzaniem danych osobowych, w tym szczególnych kategorii danych. Ponadto ma bezpośredni lub pośredni wpływ na szereg praw podstawowych zapisanych w Karcie praw podstawowych Unii Europejskiej. Jest to szczególnie istotne w obszarze ścigania przestępstw i wymiaru sprawiedliwości w sprawach karnych. W związku z tym wszelkie wykorzystanie technologii rozpoznawania twarzy powinno odbywać się w ścisłej zgodności z obowiązującymi ramami prawnymi.

31. Poniższe informacje mają posłużyć do analizy przyszłych aktów prawnych i administracyjnych, a także wdrażania istniejących przepisów w poszczególnych przypadkach, które obejmują FRT. Znaczenie poszczególnych wymogów różni się w zależności od konkretnych okoliczności. Ponieważ nie można przewidzieć wszystkich przyszłych okoliczności, uznaje się, że stanowią one jedynie wsparcie i nie należy ich traktować jako wyczerpującego wykazu.

3.1 Ogólne ramy prawne – Karta praw podstawowych Unii Europejskiej i Konwencja o ochronie praw człowieka i podstawowych wolności (EKPC)

3.1.1 Zastosowanie Karty

32. Karta praw podstawowych Unii Europejskiej (zwana dalej „Kartą") jest skierowana do instytucji, organów i jednostek organizacyjnych Unii oraz do państw członkowskich w zakresie, w jakim stosują one prawo Unii.

33. Uregulowanie przetwarzania danych biometrycznych na potrzeby ścigania przestępstw zgodnie z art. 1 ust. 1 dyrektywy o ochronie danych w sprawach karnych nieuchronnie rodzi pytanie o zgodność z prawami podstawowymi, w szczególności poszanowania życia prywatnego i komunikacji na mocy art. 7 Karty oraz prawa do ochrony danych osobowych na mocy art. 8 Karty.

34. Gromadzenie i analiza nagrań wideo osób fizycznych, w tym ich twarzy, obejmuje przetwarzanie danych osobowych. Techniczne przetwarzanie obrazu obejmuje również przetwarzanie określonych biometrycznych. Techniczne przetwarzanie danych dotyczących twarzy osoby fizycznej w odniesieniu do czasu i miejsca pozwala na formułowanie wniosków dotyczących życia prywatnego danych osób. Wnioski te mogą dotyczyć pochodzenia rasowego lub etnicznego, zdrowia, religii, nawyków życia codziennego, stałych lub tymczasowych miejsc zamieszkania, codziennego lub innego przemieszczania się, wykonywanych czynności, relacji społecznych tych osób oraz środowisk społecznych, w których przebywają. Szeroki zakres informacji, które mogą zostać ujawnione w wyniku zastosowania FRT, wyraźnie wskazuje na możliwy wpływ na prawo do ochrony danych osobowych określone w art. 8 Karty, ale także na prawo do prywatności określone w art. 7 Karty.

35. W takich okolicznościach nie można również wykluczyć, że gromadzenie, analiza i dalsze przetwarzanie przedmiotowych danych biometrycznych (twarzy) może mieć wpływ na swobodę działania ludzi, nawet jeśli działanie to byłoby w pełni zgodne z zasadami wolnego i otwartego społeczeństwa. Może to mieć również poważny wpływ na korzystanie z ich praw podstawowych, takich jak prawo do wolności myśli, sumienia i religii, prawo do pokojowych zgromadzeń i wolności zrzeszania się na mocy art. 1, 10, 11 i 12 Karty. Przetwarzanie takie wiąże się również z innymi rodzajami ryzyka, takimi jak ryzyko niewłaściwego wykorzystania danych osobowych gromadzonych przez właściwe organy w wyniku niezgodnego z prawem dostępu do danych osobowych i ich wykorzystania, naruszenia bezpieczeństwa itp. Ryzyko często zależy od przetwarzania i jego okoliczności, takich jak ryzyko

nieuprawnionego dostępu i wykorzystania przez funkcjonariuszy policji lub inne nieupoważnione strony. Niektóre rodzaje ryzyka są jednak po prostu nieodłącznie związane z unikalnym charakterem danych biometrycznych. W przeciwieństwie do adresu lub numeru telefonu, osoba, której dane dotyczą, nie może zmienić swoich unikalnych cech, takich jak twarz lub tęczówka. W przypadku nieuprawnionego dostępu lub przypadkowej publikacji danych biometrycznych prowadziłoby to do naruszenia bezpieczeństwa danych podczas ich wykorzystywania jako haseł lub kluczy kryptograficznych lub mogłoby zostać wykorzystane do dalszych nieuprawnionych działań nadzorczych ze szkodą dla osoby, której dane dotyczą.

3.1.2 Ingerencja w prawa określone w Karcie

36. W każdych okolicznościach samo przetwarzanie danych biometrycznych stanowi poważną ingerencję. Nie zależy to od wyniku, np. dopasowania pozytywnego. Przetwarzanie danych stanowi ingerencję, nawet jeśli wzorzec biometryczny zostanie natychmiast usunięty po zestawieniu z policyjną bazą danych i nie przyniesie żadnego trafienia.

37. Ingerencja w prawa podstawowe osób, których dane dotyczą, może wynikać z aktu prawnego, którego celem lub skutkiem jest ograniczenie danego prawa podstawowego[11]. Może ono również wynikać z działania organu publicznego mającego ten sam cel lub taki sam skutek lub nawet podmiotu prywatnego, któremu na mocy prawa powierzono sprawowanie władzy publicznej i wykonywanie uprawnień publicznych.

38. Akt prawny, który stanowi podstawę prawną przetwarzania danych osobowych, bezpośrednio wpływa na prawa zagwarantowane w art. 7 i 8 Karty[12].

39. Wykorzystanie danych biometrycznych, a w szczególności FRT, w wielu przypadkach narusza również prawo do godności ludzkiej zagwarantowane w art. 1 Karty. Godność ludzka oznacza, że jednostki nie mogą być traktowane jak zwykłe przedmioty. FRT przetwarza egzystencjalne i wysoce osobiste cechy, rysy twarzy, w formę nadającą się do odczytu maszynowego w celu wykorzystania jej jako ludzkiej tablicy rejestracyjnej lub dowodu osobistego, tym samym uprzedmiotawiając twarz.

40. Takie przetwarzanie może również naruszać inne prawa podstawowe, takie jak prawa wynikające z art. 10, 11 i 12 Karty, o ile „efekt mrożący" jest zamierzony lub wynika z odpowiedniego nadzoru wideo prowadzonego przez organy ścigania.

41. Ponadto należy również dokładnie rozważyć potencjalne zagrożenia wynikające z korzystania z technologii rozpoznawania twarzy przez organy ścigania w odniesieniu do prawa do rzetelnego procesu sądowego i domniemania niewinności zgodnie z art. 47 i 48 Karty. Wynik zastosowania FRT, np. dopasowanie, może nie tylko prowadzić do objęcia danej osoby dalszymi czynnościami policyjnymi, ale także stanowić decydujący dowód w postępowaniu sądowym. Wady FRT, takie jak możliwa stronniczość, dyskryminacja lub błędna identyfikacja („wynik fałszywie dodatni") mogą zatem prowadzić do poważnych konsekwencji również w postępowaniu karnym. Co więcej, w ocenie dowodów wynik zastosowania FRT może być faworyzowany, nawet jeśli istnieją dowody z nim sprzeczne („stronniczość wynikająca z automatyzacji").

3.1.3 Uzasadnienie ingerencji

42. Zgodnie z art. 52 ust. 1 Karty, wszelkie ograniczenia w korzystaniu z praw podstawowych i wolności uznanych w Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z

[11] TSUE, C-219/91 – Ter Voort, RoC 1992 I-05485, pkt 36f; TSUE, C-200/96 – Metronome, SalC 1998 I-1953, pkt 28.

[12] TSUE, C-594/12, pkt 36; TSUE, C-291/12, pkt 23 i nast.

zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię Europejską lub potrzebom ochrony praw i wolności innych osób.

3.1.3.1 Przewidziane ustawą

43. Artykuł 52 ust. 1 Karty ustanawia wymóg szczególnej podstawy prawnej. Ta podstawa prawna musi mieć wystarczająco jasne brzmienie, aby przekazać obywatelom odpowiednią wskazówkę co do warunków i okoliczności, w jakich organy są uprawnione do stosowania wszelkich środków gromadzenia danych i tajnego nadzoru[13]. Musi ona wskazywać z rozsądną jasnością zakres i sposób wykonywania przyznanego władzom publicznym uznania, tak by zapewnić jednostkom minimalny stopień ochrony, do którego są uprawnione pod rządami prawa w społeczeństwie demokratycznym[14]. Ponadto zgodność z prawem wymaga odpowiednich gwarancji w celu zapewnienia poszanowania w szczególności prawa jednostki w świetle art. 8 Karty. Zasady te mają również zastosowanie do przetwarzania danych osobowych do celów oceny, szkolenia i dalszego rozwoju systemów FRT.

44. Biorąc pod uwagę, że dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej stanowią szczególne kategorie danych wymienionych w art. 10 dyrektywy o ochronie danych w sprawach karnych, różne zastosowania FRT w większości przypadków wymagałyby specjalnego prawa precyzyjnie opisującego zastosowanie i warunki jej wykorzystania. Obejmuje to w szczególności rodzaje przestępstw oraz, w stosownych przypadkach, odpowiednią wagę tych przestępstw, w celu, między innymi, skutecznego wykluczenia drobnej przestępczości[15].

3.1.3.2 Istota podstawowego prawa do prywatności i ochrony danych osobowych, o którym mowa w art. 7 i 8 Karty praw podstawowych

45. Ograniczenia praw podstawowych w każdej sytuacji nadal muszą zapewniać poszanowanie istoty danego prawa. Istota odnosi się do samego rdzenia danego prawa podstawowego[16]. Należy szanować godność ludzką, nawet jeśli dane prawo jest ograniczone[17].

46. Oznakami możliwego naruszenia nienaruszalnego rdzenia są:

- przepis, który nakłada ograniczenia niezależnie od indywidualnego zachowania danej osoby lub wyjątkowych okoliczności[18];
- odwołanie się do sądów nie jest możliwe ani utrudnione[19];
- przed poważnym ograniczeniem nie bierze się pod uwagę okoliczności danej osoby[20];
- w odniesieniu do praw wynikających z art. 7 i 8 Karty: oprócz szerokiego zbioru metadanych komunikacyjnych, uzyskanie wiedzy o treści komunikacji elektronicznej może naruszać istotę tych praw[21];
- w odniesieniu do praw wynikających z art. 7, 8 i 11 Karty: przepisy nakładające na dostawców dostępu do usług internetowej komunikacji publicznej i na dostawców usług hostingowych

[13] ETPC, Shimovolos przeciwko Rosji, pkt 68; Vukota-Bojić przeciwko Szwajcarii.
[14] ETPC, Piechowicz przeciwko Polsce, pkt 212.
[15] Zob. np. wyroki TSUE w sprawach C-817/19 Ligue des droits humains, pkt. 151 f, C-207/16 Ministerio Fiscal, pkt 56.
[16] TSUE C-279/09, RoC 2010 I-13849, pkt 60.
[17] Wyjaśnienia dotyczące Karty praw podstawowych, Tytuł I, Wyjaśnienie odnoszące się do artykułu 1, Dz.U. C 303 z 14.12.2007, s. 17–35.
[18] TSUE C-601/15, pkt 52.
[19] TSUE C-400/10, RoC 2010 I-08965, pkt 55.
[20] TSUE C-408/03, RoC 2006 I-02647, pkt 68.
[21] TSUE, 203/15, Tele2 Sverige, pkt 101 w odniesieniu do TSUE - C-293/12 i C-594/12, pkt 39.

obowiązek uogólnionego i niezróżnicowanego zatrzymywania między innymi danych osobowych dotyczących tych usług[22];

- w odniesieniu do praw wynikających z art. 8 Karty: brak podstawowych zasad ochrony danych i bezpieczeństwa danych również może naruszać istotę tego prawa[23].

3.1.3.3 Cel zgodny z prawem

47. Jak już wyjaśniono w punkcie 3.1.3., ograniczenia praw podstawowych muszą rzeczywiście odpowiadać celom interesu ogólnego uznawanym przez Unię Europejską lub potrzebom ochrony praw i wolności innych osób.

48. Unia uznaje zarówno cele wymienione w art. 3 Traktatu o Unii Europejskiej, jak i inne interesy chronione postanowieniami szczególnymi Traktatów[24], tj. – między innymi – przestrzeń wolności, bezpieczeństwa i sprawiedliwości, zapobieganie przestępczości i jej zwalczanie. W stosunkach z resztą świata Unia powinna nadal przyczyniać się do pokoju i bezpieczeństwa oraz ochrony praw człowieka.

49. Potrzeba ochrony praw i wolności innych osób odnosi się do praw osób, które są chronione przez prawo Unii lub jej państw członkowskich. Oceny takiej należy dokonywać, przestrzegając konieczności pogodzenia wymogów związanych z ochroną poszczególnych praw oraz zapewnienia sprawiedliwej równowagi między nimi [25].

3.1.3.4 Analiza niezbędności i proporcjonalności

50. W przypadku ingerencji w prawa podstawowe, zakres uprawnień dyskrecjonalnych prawodawcy krajowego i unijnego może okazać się ograniczony. Zależy to od kilku czynników, w tym między innymi obszaru, którego kontrola ta dotyczy, natury prawa gwarantowanego przez Kartę, charakteru i wagi tej ingerencji oraz jej celu[26]. Akty prawne muszą być odpowiednie do osiągnięcia uzasadnionych celów, do których dąży przedmiotowe prawodawstwo. Ponadto akt ten nie może wykraczać poza to, co jest niezbędne do osiągnięcia tych celów[27]. Cel interesu ogólnego, mimo że ma on fundamentalne znaczenie, sam w sobie nie uzasadnia ograniczenia prawa podstawowego[28].

51. Zgodnie z utrwalonym orzecznictwem TSUE odstępstwa i ograniczenia w odniesieniu do ochrony danych osobowych muszą być stosowane wyłącznie w zakresie, w jakim jest to absolutnie niezbędne[29]. Oznacza to również, że nie istnieją mniej inwazyjne środki służące osiągnięciu tego celu. Należy dokładnie zidentyfikować i ocenić możliwe alternatywy, takie jak – w zależności od danego celu – dodatkowy personel, częstsze interwencje policji lub dodatkowe oświetlenie ulic. Akty prawne powinny być zróżnicowane i ukierunkowane na osoby nimi objęte z uwzględnieniem celu, np. zwalczania poważnych przestępstw. Jeżeli akt obejmuje wszystkie osoby w sposób ogólny, bez takiego

---

[22] TSUE C-512/18, La Quadrature du Net, pkt 209 i nast.

[23] TSUE - C-594/12, pkt. 40.

[24] Wyjaśnienia dotyczące Karty praw podstawowych, Tytuł I, Wyjaśnienie do art. 52, Dz.U. C 303 z 14.12.2007, s. 17–35.

[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta art. 52 Rn. 31–32.

[26] TSUE – C-594/12, pkt 47 z następującymi źródłami: zob. analogicznie, w odniesieniu do art. 8 EKPC, wyrok ETPC w sprawie S. i Marper przeciwko Zjednoczonemu Królestwu [wielka izba], nr 30562/04 i 30566/04, § 102, ETPC 2008-V.

[27] TSUE – C-594/12, pkt 46 z następującymi źródłami: Sprawa C-343/09 Afton Chemical EU:C:2010:419, pkt 45; Volker und Markus Schecke i Eifert EU:C:2010:662, pkt 74; sprawy C-581/10 i C-629/10 Nelson i in. EU:C:2012:657, pkt 71; sprawa C-283/11 Sky Österreich EU:C:2013:28, pkt 50; oraz sprawa C-101/12 Schaible EU:C:2013:661, pkt 29.

[28] TSUE – C-594/12, pkt. 51.

[29] TSUE – C-594/12, pkt 52, z następującymi źródłami: sprawa C-473/12 IPI EU:C:2013:715, pkt 39 i przytoczone tam orzecznictwo.

zróżnicowania, ograniczenia lub wyjątku, zwiększa on ingerencję[30]. Zwiększa on również ingerencję, jeśli przetwarzaniem danych objęta jest znaczna część populacji[31].

52. Ochrona danych osobowych wynikająca z wyraźnego obowiązku określonego w art. 8 ust. 1 Karty jest szczególnie ważna dla prawa do poszanowania życia prywatnego zapisanego w art. 7 Karty[32]. Przepisy muszą zawierać jasne i dokładne reguły dotyczące zakresu i sposobu stosowania rozpatrywanych środków, a także ustanawiać zabezpieczenia służące temu, aby osoby, których dane zostały przetworzone, miały wystarczające gwarancje rzeczywistej ochrony ich danych osobowych przed ryzykiem nadużyć oraz ich bezprawnym udostępnianiem i wykorzystywaniem[33]. Potrzeba takich zabezpieczeń jest tym większa, gdy dane osobowe przetwarzane są automatycznie i istnieje znaczne ryzyko bezprawnego uzyskania dostępu do nich[34]. Ponadto wewnętrzne lub zewnętrzne, np. sądowe, zezwolenie na wdrożenie FRT może również stanowić formę zabezpieczenia i może okazać się konieczne w niektórych przypadkach poważnej ingerencji[35].

53. Ustanowione reguły muszą być dostosowane do konkretnej sytuacji, np. ilości przetwarzanych danych, charakteru danych[36] i ryzyka nieuprawnionego dostępu do danych. Wymaga to ustanowienia reguł, które w szczególności wyraźnie i dokładnie rozwiązywałyby problem ochrony i bezpieczeństwa tych danych w taki sposób, aby zapewnić ich integralność i poufność[37].

54. W odniesieniu do relacji między administratorem a podmiotem przetwarzającym podmiotom przetwarzającym nie powinno się zezwalać na uwzględnianie wyłącznie względów ekonomicznych przy określaniu poziomu bezpieczeństwa, jaki stosują do danych osobowych; mogłoby to stanowić zagrożenie dla zapewnienia wystarczająco wysokiego poziomu ochrony[38].

55. Akt prawny musi określać przesłanki merytoryczne i proceduralne oraz obiektywne kryteria, na podstawie których można określić granice dostępu właściwych organów do danych oraz ich późniejsze wykorzystanie. W celu zapobiegania, wykrywania i ścigania karnego, przestępstwa musiałyby zostać uznane za wystarczająco poważne, aby uzasadnić zakres i wagę ingerencji w prawa podstawowe ustanowione w art. 7 i 8 Karty[39].

56. Dane muszą być przetwarzane w sposób zapewniający stosowanie i skuteczność unijnych przepisów o ochronie danych; w szczególności tych przewidzianych w art. 8 Karty, który stanowi, że zgodność z wymogami ochrony i bezpieczeństwa podlega kontroli niezależnego organu. W takiej sytuacji istotne może być położenie geograficzne miejsca przetwarzania danych[40].

---

[30] TSUE – C-594/12, pkt 57.
[31] TSUE – C-594/12, pkt 56.
[32] TSUE – C-594/12, pkt 53.
[33] TSUE – C-594/12, pkt 54, wraz z następującymi źródłami: zob. analogicznie, w odniesieniu do art. 8 EKPC, wyrok ETPC z dnia 1 lipca 2008 r. w sprawie Liberty i in. przeciwko Zjednoczonemu Królestwu, skarga nr 58243/00, §§ 62 i 63; wyrok w sprawie Rotaru przeciwko Rumunii, §§ 57–59; a także wyrok w sprawie S. i Marper przeciwko Zjednoczonemu Królestwu, § 99.
[34] TSUE – C-594/12, pkt 55, z następującymi źródłami: zob. analogicznie, w odniesieniu do art. 8 EKPC, wyrok w sprawie S. i Marper przeciwko Zjednoczonemu Królestwu, § 103; a także wyrok z dnia 18 kwietnia 2013 r. w sprawie M.K. przeciwko Francji, skarga nr 19522/09, § 35.
[35] ETPC, Szabó i Vissy przeciwko Węgrom, pkt 73–77.
[36] Zobacz również zaostrzone wymogi dotyczące środków technicznych i organizacyjnych podczas przetwarzania szczególnych kategorii danych, art. 29 ust. 1 dyrektywy o ochronie danych w sprawach karnych.
[37] TSUE – C-594/12, pkt 66.
[38] TSUE – C-594/12, pkt 67.
[39] TSUE – C-594/12, pkt 60 i 61.
[40] TSUE– C-594/12, pkt 68.

57. W odniesieniu do poszczególnych etapów przetwarzania danych osobowych należy dokonać rozróżnienia między kategoriami danych w zależności od użyteczności danych w stosunku do zakładanego celu lub w zależności od zainteresowanych osób[41]. Określenie warunków przetwarzania, na przykład określenie okresu przechowywania, musi opierać się na obiektywnych kryteriach w celu zapewnienia, aby ingerencja była ograniczona do tego, co jest bezwzględnie niezbędne[42].

58. Każdorazowo przy ocenie niezbędności i proporcjonalności należy zidentyfikować i rozważyć wszystkie implikacje, które wchodzą w zakres innych praw podstawowych, takich jak godność ludzka zgodnie z art. 1 Karty, wolność myśli, sumienia i religii zgodnie z art. 10 Karty, wolność wypowiedzi zgodnie z art. 11 Karty, a także wolność zgromadzeń i zrzeszania się zgodnie z art. 12 Karty.

59. Ponadto za kwestię krytyczną należy uznać to, że jeśli dane są systematycznie przetwarzane bez wiedzy osób, których dane dotyczą, może to wywoływać ogólne poczucie ciągłego nadzoru[43]. Może to prowadzić do powstania „efektu mrożącego" w odniesieniu do niektórych lub wszystkich praw podstawowych.

60. Aby ułatwić i zoperacjonalizować ocenę niezbędności i proporcjonalności aktów prawnych dotyczących rozpoznawania twarzy w obszarze ścigania przestępstw, prawodawcy krajowi i unijni mogliby skorzystać z dostępnych praktycznych narzędzi zaprojektowanych specjalnie do tego zadania. W szczególności można wykorzystać zestaw narzędzi dotyczących niezbędności i proporcjonalności[44] zapewniony przez Europejskiego Inspektora Ochrony Danych.

3.1.3.5 Artykuł 52 ust. 3, art. 53 Karty (poziom ochrony, również w odniesieniu do Konwencji o ochronie praw człowieka i podstawowych wolności)

61. Zgodnie z art. 52 ust. 3 i art. 53 Karty znaczenie i zakres tych praw Karty, które odpowiadają prawom zagwarantowanym w EKPC, muszą być takie same jak te określone w EKPC. O ile w szczególności dla art. 7 Karty można znaleźć odpowiednik w EKPC, nie jest tak w przypadku art. 8 Karty[45]. Artykuł 52 ust. 3 Karty nie stoi na przeszkodzie temu, aby prawo Unii przyznawało szerszą ochronę. Ponieważ EKPC nie stanowi aktu prawnego formalnie obowiązującego w porządku prawnym Unii, przepisy Unii należy przyjmować w świetle praw podstawowych zagwarantowanych w Karcie[46].

62. Zgodnie z art. 8 EKPC władza publiczna nie może ingerować w korzystanie z prawa do poszanowania życia prywatnego i rodzinnego, chyba że jest to przewidziane przez ustawę i konieczne w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób.

63. EKPC wyznacza również standardy w odniesieniu do sposobu, w jaki można wprowadzać ograniczenia. Jednym z podstawowych wymogów, oprócz praworządności, jest przewidywalność. Aby spełnić

[41] TSUE – C-594/12, pkt 63.
[42] TSUE – C-594/12, pkt 64.
[43] TSUE – C-594/12, pkt 37.
[44] Europejski Inspektor Ochrony Danych: „Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit" [„Zestaw narzędzi w zakresie oceny konieczności środków ograniczających podstawowe prawo do ochrony danych osobowych"]: Zestaw narzędzi (11.4.2017); Europejski Inspektor Ochrony Danych: „EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data" [„Wytyczne EIOD w sprawie oceny proporcjonalności środków ograniczających prawa podstawowe do prywatności i ochrony danych osobowych"] (19.12.2019).
[45] TSUE – C-203/15 - Tele2 Sverige, pkt 129.
[46] TSUE – C-311/18, pkt. 99.

wymóg przewidywalności, przepisy muszą być sformułowane na tyle jasno, aby wskazywać wszystkim w sposób wystarczający, w jakich okolicznościach i na jakich warunkach upoważnia on organy publiczne do stosowania środków[47]. Wymóg ten został uznany przez TSUE i unijne prawo o ochronie danych (zob. sekcja 3.2.1.1).

64. Ponadto, określając prawa wynikające z art. 8 EKPC, należy również w pełni przestrzegać postanowień Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[48]. Należy jednak wziąć pod uwagę, że przepisy te stanowią jedynie minimalny standard w świetle obowiązującego prawa Unii.

3.2 Szczegółowe ramy prawne – dyrektywa o ochronie danych w sprawach karnych

65. W dyrektywie o ochronie danych w sprawach karnych przewidziano pewne ramy dotyczące stosowania FRT. Po pierwsze, w art. 3 ust. 13 dyrektywy o ochronie danych w sprawach karnych zdefiniowano termin „dane biometryczne”[49]. Szczegółowe informacje można znaleźć w sekcji 2.1 powyżej. Po drugie, art. 8 ust. 2 wyjaśnia, że aby jakiekolwiek przetwarzanie było zgodne z prawem, musi ono – oprócz tego, że jest niezbędne do celów określonych w art. 1 ust. 1 dyrektywy o ochronie danych w sprawach karnych – być uregulowane w prawie krajowym, które określa co najmniej powody przetwarzania, dane osobowe mające podlegać przetwarzaniu oraz cele przetwarzania. Kolejne przepisy o szczególnym znaczeniu w odniesieniu do danych biometrycznych zawarto w art. 10 i 11 dyrektywy o ochronie danych w sprawach karnych. Artykuł 10 należy odczytywać w związku z art. 8 dyrektywy o ochronie danych w sprawach karnych[50]. Należy zawsze przestrzegać zasad przetwarzania danych osobowych określonych w art. 4 dyrektywy o ochronie danych w sprawach karnych i kierować się nimi przy ocenie ewentualnego przetwarzania danych biometrycznych za pośrednictwem FRT.

3.2.1 Przetwarzanie szczególnych kategorii danych do celów ścigania przestępstw

66. Zgodnie z art. 10 dyrektywy o ochronie danych w sprawach karnych przetwarzanie szczególnych kategorii danych, takich jak dane biometryczne, jest dozwolone jeżeli jest bezwzględnie niezbędne i podlega odpowiednim zabezpieczeniom w odniesieniu do praw i wolności osoby, której dane dotyczą. Przy czym takie przetwarzanie jest dozwolone tylko pod warunkiem, że jest dopuszczone prawem Unii lub prawem państwa członkowskiego i jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, albo też dotyczy danych w sposób oczywisty upublicznionych przez samą osobę, której dane dotyczą. Ta ogólna klauzula podkreśla wrażliwość przetwarzania szczególnych kategorii danych.

3.2.1.1 Dopuszczone prawem Unii lub prawem państwa członkowskiego

67. W odniesieniu do niezbędnego rodzaju aktu prawnego, motyw 33 dyrektywy o ochronie danych w sprawach karnych stanowi, że „[j]eżeli w niniejszej dyrektywie jest mowa o prawie państwa członkowskiego, podstawie prawnej lub akcie prawnym, niekoniecznie wymaga to przyjęcia aktu

[47] Europejski Trybunał Praw Człowieka, wyrok w sprawie COPLAND przeciwko ZJEDNOCZONEMU KRÓLESTWU, 03/04/2007, skarga nr 62617/00, pkt 46.
[48] ETS nr 108.
[49] Artykuł 3 ust. 13 dyrektywy o ochronie danych w sprawach karnych: „Dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby fizycznej, takie jak wizerunek twarzy lub dane daktyloskopijne.
[50] WP258, opinia dotycząca niektórych głównych zagadnień dyrektywy o ochronie danych w sprawach karnych (UE 2016/680), s. 7.

prawnego przez parlament, z zastrzeżeniem wymogów wynikających z porządku konstytucyjnego danego państwa członkowskiego”[51].

68. Zgodnie z art. 52 ust. 1 Karty, wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w niniejszej Karcie muszą być „przewidziane ustawą”. Powyższe zdanie przywołuje wyrażenie „przewidziane przez ustawę” pochodzące z art. 8 ust. 2 EKPC, które oznacza nie tylko przestrzeganie prawa właściwego, lecz także odnosi się do jakości tego prawa, wymagając od niego zgodności z zasadą praworządności.

69. Motyw 33 dyrektywy o ochronie danych w sprawach karnych stanowi ponadto, że „[t]akie prawo państwa członkowskiego, podstawa prawna lub akt prawny powinny jednak być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka. Prawo państwa członkowskiego regulujące przetwarzanie danych osobowych w ramach zakresu zastosowania niniejszej dyrektywy powinno co najmniej określać cele ogólne, dane osobowe mające podlegać przetwarzaniu, cele przetwarzania oraz procedury pozwalające chronić integralność i poufność danych osobowych oraz procedury niszczenia tych danych”.

70. Prawo krajowe musi mieć wystarczająco jasne brzmienie, aby przekazać osobom, których dane dotyczą, wskazówkę co do okoliczności i warunków, w których administratorzy danych są uprawnieni do stosowania takich środków. Obejmuje to możliwe warunki wstępne przetwarzania, takie jak określone rodzaje dowodów, a także konieczność uzyskania zgody sądowej lub wewnętrznej. Odpowiednie przepisy mogą być neutralne pod względem technologicznym, o ile w wystarczającym stopniu uwzględniają specyficzne ryzyko i cechy przetwarzania danych osobowych przez systemy FRT. Zgodnie z dyrektywą o ochronie danych w sprawach karnych oraz orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej (TSUE) i Europejskiego Trybunału Praw Człowieka (ETPC) istotne jest, aby akty prawne, których celem jest zapewnienie podstawy prawnej środka rozpoznawania twarzy, były przewidywalne dla osób, których dane dotyczą.

71. Akt prawny nie może być powoływany jako akt zezwalający na przetwarzanie danych biometrycznych za pomocą FRT do celów ścigania przestępstw, jeżeli stanowi on zwykłą transpozycję ogólnej klauzuli zawartej w art. 10 dyrektywy o ochronie danych w sprawach karnych.

72. Oprócz danych biometrycznych, art. 10 dyrektywy o ochronie danych w sprawach karnych reguluje przetwarzanie innych szczególnych kategorii danych, takich jak orientacja seksualna, poglądy polityczne i przekonania religijne, obejmując tym samym szeroki zakres przetwarzania. Ponadto taki przepis nie zawierałby szczegółowych wymogów określających okoliczności i warunki, w jakich organy ścigania byłyby uprawnione do korzystania z technologii rozpoznawania twarzy. Ze względu na odniesienie do innych rodzajów danych oraz wyraźną potrzebę wprowadzenia specjalnych zabezpieczeń bez dalszych specyfikacji, przepisy krajowe transponujące art. 10 dyrektywy o ochronie danych w sprawach karnych do prawa krajowego – o podobnie ogólnym i abstrakcyjnym brzmieniu – nie mogą być powoływane jako podstawa prawna dla przetwarzania danych biometrycznych obejmujących rozpoznawanie twarzy, ponieważ nie byłyby precyzyjne i przewidywalne. Zgodnie z art. 28 ust. 2 lub art. 46 ust. 1 lit. c) dyrektywy o ochronie danych w sprawach karnych, zanim prawodawca stworzy nową podstawę prawną dla jakiejkolwiek formy przetwarzania danych

[51] Rodzaj rozważanych aktów prawnych musi być zgodny z prawem Unii lub prawem krajowym. W zależności od stopnia ingerencji ograniczenia, na poziomie krajowym może być wymagany szczególny akt prawny, uwzględniający poziom normy.

biometrycznych z wykorzystaniem rozpoznawania twarzy, powinien skonsultować się z krajowym organem nadzorczym ds. ochrony danych.

3.2.1.2 Bezwzględna niezbędność

73. Przetwarzanie można uznać za „bezwzględnie niezbędne" tylko wtedy, gdy ingerencja w ochronę danych osobowych i jej ograniczenie są zredukowane do tego, co jest absolutnie konieczne[52]. Dodanie terminu „bezwzględnie" oznacza, że zamiarem prawodawcy było, aby przetwarzanie szczególnych kategorii danych odbywało się wyłącznie w warunkach jeszcze bardziej rygorystycznych niż warunki konieczności (zob. powyżej, pkt 3.1.3.4). Wymóg ten należy interpretować jako niezbędny. Ogranicza on margines swobody oceny przysługujący organowi ścigania w ramach testu niezbędności do absolutnego minimum. Zgodnie z utrwalonym orzecznictwem TSUE, warunek „bezwzględnej niezbędności" jest również ściśle powiązany z wymogiem stosowania obiektywnych kryteriów umożliwiających określenie okoliczności i warunków, w których możliwe jest przetwarzanie danych, tym samym wykluczając jakiekolwiek przetwarzanie o charakterze ogólnym lub systematycznym[53].

3.2.1.3 W sposób oczywisty upublicznione

74. Oceniając, czy przetwarzanie odnosi się do danych, które są w sposób oczywisty upubliczniane przez osobę, której dane dotyczą, należy przypomnieć, że fotografia jako taka nie jest powszechnie uznawana za dane biometryczne[54]. W związku z tym fakt, że fotografia została w sposób oczywisty upubliczniona przez osobę, której dane dotyczą, nie oznacza, że powiązane dane biometryczne, które można z niej pobrać przy użyciu określonych środków technicznych, uznaje się za w sposób oczywisty upublicznione.

75. Tak jak w przypadku danych osobowych w ujęciu ogólnym, aby dane biometryczne były postrzegane jako w oczywisty sposób upublicznione przez osobę, której dane dotyczą, osoba ta musi celowo udostępnić wzorzec biometryczny (a nie tylko wizerunek twarzy) za pomocą otwartego źródła. Jeżeli osoba trzecia ujawnia dane biometryczne, nie można uznać, że dane zostały w sposób oczywisty upublicznione przez osobę, której dane dotyczą.

76. Ponadto nie wystarczy interpretacja zachowania osoby, której dane dotyczą, aby uznać, że dane biometryczne zostały w sposób oczywisty upublicznione. Na przykład w przypadku sieci społecznościowych lub platform internetowych EROD uważa, że fakt, że osoba, której dane dotyczą, nie uruchomiła lub nie ustanowiła szczególnych cech prywatności, nie jest wystarczająca, aby uznać, że ta osoba, której dane dotyczą, w sposób oczywisty upubliczniła swoje dane osobowe oraz że dane te (np. fotografie) mogą być przetwarzane we wzorcach biometrycznych i wykorzystywane do celów identyfikacji bez zgody osoby, której dane dotyczą. Ogólnie rzecz biorąc, domyślne ustawienia usługi, np. publiczne udostępnianie wzorców lub brak możliwości wyboru, np. wzorce są upubliczniane bez możliwości zmiany tego ustawienia przez użytkownika, nie powinny być w żaden sposób interpretowane jako dane w sposób oczywisty upubliczniane.

[52] Spójne orzecznictwo dotyczące podstawowego prawa do poszanowania życia prywatnego, zob. sprawa TSUE C-73/07 pkt 56 (Satakunnan Markkinapörssi i Satamedia); TSUE, sprawy C-92/09 i C-93/09 pkt 77 (Schecke i Eifert); TSUE – C-594/12, pkt 52 (Digital Rights); TSUE, sprawa C-362/14, pkt 92 (Schrems).
[53] TSUE, sprawa C-623/17, pkt 78.
[54] Por. motyw 51 RODO: „[p]rzetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją „danych biometrycznych" tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości."

3.2.2 Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie

77. Zgodnie z art. 11 ust. 1 dyrektywy o ochronie danych w sprawach karnych państwa członkowskie zapewniają, by decyzje, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i mają niekorzystne skutki prawne dla osoby, której dane dotyczą, lub poważnie na nią wpływają, były zakazane. W ramach odstępstwa od tego ogólnego zakazu takie przetwarzanie może być możliwe wyłącznie wtedy, gdy dopuszcza je prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator i które przewiduje odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą, a przynajmniej prawo do uzyskania interwencji ludzkiej ze strony administratora. Może być stosowane jedynie w sposób restrykcyjny. Próg ten ma zastosowanie do zwykłych (tj. nie szczególnych) kategorii danych osobowych. Do wyłączenia na podstawie art. 11 ust. 2 dyrektywy o ochronie danych w sprawach karnych stosuje się jeszcze wyższy próg i bardziej restrykcyjne zastosowanie. Zgodnie z tym artykułem decyzje, o których mowa w ust. 1, nie mogą opierać się na danych osobowych szczególnych kategorii, tj. w szczególności na danych biometrycznych w celu jednoznacznej identyfikacji osoby fizycznej. Wyłączenie można zastosować tylko wtedy, gdy istnieją właściwe środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą. Wyłączenie to należy odczytywać jako uzupełnienie art. 10 dyrektywy o ochronie danych w sprawach karnych i w świetle jego przesłanek.

78. W zależności od systemu FRT, nawet interwencja ludzka podczas oceny wyników FRT sama w sobie nie stanowi wystarczającej gwarancji poszanowania praw osób fizycznych, a w szczególności prawa do ochrony danych osobowych, biorąc pod uwagę możliwą stronniczość i błędy, które mogą wynikać z samego przetwarzania. Ponadto interwencję ludzką można uznać za zabezpieczenie tylko wtedy, gdy osoba interweniująca jest w stanie podważyć wyniki FRT podczas takiej interwencji. Kluczowe jest umożliwienie danej osobie zrozumienia systemu FRT i jego ograniczeń, a także właściwej interpretacji jego wyników. Konieczne jest również ustanowienie miejsca pracy i organizacji, które będą przeciwdziałać skutkom błędu automatyzacji i pozwolą uniknąć bezkrytycznej akceptacji wyników, np. z powodu presji czasu, uciążliwych procedur, potencjalnie szkodliwego wpływu na karierę itp.

79. Zgodnie z art. 11 ust. 3 dyrektywy o ochronie danych w sprawach karnych profilowanie skutkujące dyskryminacją osób fizycznych na podstawie danych osobowych szczególnych kategorii, takich jak dane biometryczne, jest zabronione zgodnie z prawem Unii. Zgodnie z art. 3 ust. 4 dyrektywy o ochronie danych w sprawach karnych „profilowanie” oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. Rozważając, czy przewiduje się właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, należy pamiętać, że korzystanie z FRT może prowadzić do profilowania, w zależności od sposobu i celu, w jakim FRT jest stosowane. W każdym przypadku, zgodnie z prawem Unii i art. 11 ust. 3 dyrektywy o ochronie danych w sprawach karnych, profilowanie skutkujące dyskryminacją osób fizycznych na podstawie szczególnych kategorii danych osobowych jest zabronione.

3.2.3 Kategorie osób, których dane dotyczą

80. Artykuł 6 dyrektywy o ochronie danych w sprawach karnych dotyczy konieczności rozróżniania między poszczególnymi kategoriami osób, których dane dotyczą. Rozróżnienie to należy wprowadzić w stosownych przypadkach i w miarę możliwości. Musi wykazywać wpływ na sposób przetwarzania danych. Z przykładów podanych w art. 6 dyrektywy o ochronie danych w sprawach karnych można

wywnioskować, że co do zasady przetwarzanie danych osobowych musi spełniać kryteria niezbędności i proporcjonalności również w odniesieniu do kategorii osób, których dane dotyczą[55]. Ponadto można z tego wywnioskować, że w odniesieniu do osób, których dane dotyczą, co do których brak jest dowodów mogących sugerować, że ich zachowanie może mieć związek, chociażby pośredni i daleki, ze zgodnym z prawem celem przewidzianym w dyrektywie o ochronie danych w sprawach karnych, najprawdopodobniej nie ma uzasadnienia dla ingerencji[56]. Jeżeli rozróżnienie zgodnie z art. 6 dyrektywy o ochronie danych w sprawach karnych nie ma zastosowania lub nie jest możliwe, przy ocenie niezbędności i proporcjonalności ingerencji należy dokładnie rozważyć zastosowanie wyjątku od zasady określonej w art. 6 dyrektywy o ochronie danych w sprawach karnych. Rozróżnienie między różnymi kategoriami osób, których dane dotyczą, wydaje się być niezbędnym wymogiem, jeśli chodzi o przetwarzanie danych osobowych obejmujące rozpoznawanie twarzy, biorąc również pod uwagę możliwe wyniki fałszywie dodatnie lub fałszywie ujemne, które mogą mieć istotny wpływ na osoby, których dane dotyczą, a także podczas dochodzenia.

81. Jak wspomniano, przy wdrażaniu prawa Unii należy przestrzegać postanowień Karty praw podstawowych Unii Europejskiej, por. art. 52 Karty. Ramy i kryteria przewidziane w dyrektywie o ochronie danych w sprawach karnych należy zatem odczytywać w świetle Karty. Akty prawne UE i jej państw członkowskich nie mogą nie spełniać tego wymogu i muszą zapewniać pełną skuteczność Karty.

3.2.4 Prawa osoby, której dane dotyczą

82. Europejska Rada Ochrony Danych przedstawiła już wytyczne dotyczące praw osób, których dane dotyczą, wynikające z RODO w różnych aspektach[57]. Dyrektywa o ochronie danych w sprawach karnych przewiduje podobne prawa osób, których dane dotyczą, a ogólne wytyczne w tym zakresie zostały przedstawione w opinii Grupy Roboczej Art. 29, którą zatwierdziła Europejska Rada Ochrony Danych[58]. W określonych okolicznościach dyrektywa o ochronie danych w sprawach karnych dopuszcza pewne ograniczenia tych praw. Parametry dotyczące takich ograniczeń zostaną omówione bardziej szczegółowo w sekcji 3.2.4.6. „Uzasadnione ograniczenia praw osób, których dane dotyczą".

83. Podczas gdy wszystkie prawa osób, których dane dotyczą, wymienione w rozdziale III dyrektywy o ochronie danych w sprawach karnych, mają oczywiście zastosowanie również do przetwarzania danych osobowych za pomocą technologii rozpoznawania twarzy (FRT), w poniższym rozdziale omówione zostaną niektóre prawa i aspekty, które mogą być szczególnie interesujące, aby zapewnić wytyczne w tym zakresie. Ponadto niniejszy rozdział i jego analiza opierają się na założeniu, że przedmiotowe przetwarzanie FRT spełniło wymogi prawne opisane w poprzednim rozdziale.

84. Biorąc pod uwagę charakter przetwarzania danych osobowych za pośrednictwem FRT (przetwarzanie szczególnych kategorii danych osobowych często bez widocznej interakcji z osobą, której dane dotyczą), administrator musi dokładnie zastanowić się, w jaki sposób (lub czy jest w stanie) spełnić wymogi dyrektywy o ochronie danych w sprawach karnych przed rozpoczęciem przetwarzania FRT. W szczególności poprzez staranną analizę:

- tego, kim są osoby, których dane dotyczą (często jest to więcej niż jedna osoba, która jest głównym celem przetwarzania),

[55] Por. również TSUE – C-594/12, pkt 56–59.
[56] Por. również TSUE – C-594/12, pkt 58.
[57] Zob. np. 1/2022 Wytyczne EROD dotyczące praw osób, których dane dotyczą – prawo dostępu oraz 3/2019 Wytyczne EROD dotyczące przetwarzania danych osobowych przez urządzenia wideo.
[58] WP258, opinia dotycząca niektórych głównych zagadnień dyrektywy o ochronie danych w sprawach karnych (UE 2016/680).

- sposobu, w jaki osoby, których dane dotyczą, są informowane o przetwarzaniu za pomocą FRT (zob. sekcja 3.2.4.1),

- sposobu, w jaki osoby, których dane dotyczą, mogą wykonywać przysługujące im prawa (w tym przypadku zachowanie zarówno prawa do informacji i dostępu, jak i prawa do sprostowania lub ograniczenia może być szczególnie trudne w sytuacji, gdy FRT jest wykorzystywana do wszystkich rodzajów weryfikacji, z wyłączeniem weryfikacji 1 do 1 przy bezpośrednim kontakcie z osobą, której dane dotyczą).

3.2.4.1 Udostępnianie praw i informacji osobom, których dane dotyczą, w zwięzłej, zrozumiałej i łatwo dostępnej formie

85. Stosowanie FRT wiąże się z wyzwaniami w zakresie zapewnienia, aby osoby, których dane dotyczą, były świadome tego, że ich dane biometryczne są przetwarzane. Jest to szczególnie trudne, jeśli organ ścigania analizuje za pośrednictwem FRT materiał wideo, który pochodzi od osoby trzeciej lub jest przez nią udostępniany, ponieważ organ ścigania ma niewielką możliwość powiadomienia osoby, której dane dotyczą, w momencie gromadzenia danych (np. za pomocą odpowiedniego komunikatu na miejscu), a w większości przypadków nie ma takiej możliwości. Wszelkie materiały wideo niemające znaczenia dla dochodzenia (lub celu ich przetwarzania) powinny być zawsze usuwane lub anonimizowane (np. poprzez zamazanie bez możliwości odzyskania danych z mocą wsteczną) przed rozpoczęciem przetwarzania danych biometrycznych, aby uniknąć ryzyka naruszenia zasady minimalizacji określonej w art. 4 ust. 1 lit. e) dyrektywy o ochronie danych w sprawach karnych oraz obowiązków informacyjnych określonych w art. 13 ust. 2 dyrektywy o ochronie danych w sprawach karnych. Obowiązkiem administratora danych jest ocena, jakie informacje byłyby istotne dla osoby, której dane dotyczą, przy wykonywaniu jej praw i zapewnienie dostarczenia niezbędnych informacji. Skuteczne wykonywanie praw osoby, której dane dotyczą, zależy od tego, czy administrator danych wypełnia swoje obowiązki informacyjne.

86. Artykuł 13 ust. 1 dyrektywy o ochronie danych w sprawach karnych określa, jakie minimalne informacje należy ogólnie przekazać osobie, której dane dotyczą. Informacje te mogą być przekazywane za pośrednictwem strony internetowej administratora, w formie drukowanej (np. ulotki dostępnej na żądanie) lub w inny sposób łatwo dostępny dla osoby, której dane dotyczą. Administrator danych musi w każdym przypadku zapewnić skuteczne przekazywanie informacji w odniesieniu do co najmniej następujących elementów:

- imię i nazwisko oraz dane kontaktowe administratora, w tym inspektora ochrony danych,

- cel przetwarzania oraz fakt, że dane są przetwarzane za pośrednictwem FRT,

- prawo do złożenia skargi do organu nadzorczego oraz dane kontaktowe takiego organu,

- prawo do żądania dostępu do danych osobowych, ich sprostowania lub usunięcia oraz ograniczenia przetwarzania danych osobowych.

87. Ponadto w konkretnych przypadkach określonych w prawie krajowym, które powinny być zgodne z art. 13 ust. 2 dyrektywy o ochronie danych w sprawach karnych[59], jak na przykład przetwarzanie FRT, osobie, której dane dotyczą, należy przekazać bezpośrednio następujące informacje:

- podstawa prawna przetwarzania,

[59] Np. art. 56 ust. 1 niemieckiej federalnej ustawy o ochronie danych, w którym określono między innymi, jakie informacje należy przekazywać osobom, których dane dotyczą, w ramach operacji tajnych.

- dalsze informacje, gdy dane osobowe zostały zgromadzone bez wiedzy osoby, której dane dotyczą,
- okres przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteria służące określeniu tego okresu,
- w stosownych przypadkach kategorie odbiorców danych osobowych (w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych).

88. Podczas gdy art. 13 ust. 1 dyrektywy o ochronie danych w sprawach karnych dotyczy ogólnych informacji udostępnianych publicznie, art. 13 ust. 2 dyrektywy o ochronie danych w sprawach karnych dotyczy dodatkowych informacji, które należy przekazać konkretnej osobie, której dane dotyczą, w szczególnych przypadkach, na przykład gdy dane są zbierane bezpośrednio od osoby, której dane dotyczą, lub pośrednio bez wiedzy osoby, której dane dotyczą[60]. Nie ma jasnej definicji tego, co należy rozumieć przez „konkretne przypadki" w art. 13 ust. 2 dyrektywy o ochronie danych w sprawach karnych. Odnosi się to jednak do sytuacji, w których osoby, których dane dotyczą, muszą być świadome przetwarzania dotyczącego ich konkretnie i otrzymać odpowiednie informacje w celu skutecznego wykonywania przysługujących im praw. Europejska Rada Ochrony Danych uważa, że oceniając, czy istnieje „konkretny przypadek", należy wziąć pod uwagę kilka czynników, w tym to, czy dane osobowe są gromadzone bez wiedzy osoby, której dane dotyczą, ponieważ byłby to jedyny sposób, aby umożliwić osobom, których dane dotyczą, skuteczne korzystanie z przysługujących im praw. Innymi przykładami „konkretnych przypadków" mogą być sytuacje, w których dane osobowe są dalej przetwarzane w ramach procedury międzynarodowej współpracy w sprawach karnych lub w sytuacji przetwarzania danych osobowych w ramach tajnych operacji określonych w prawie krajowym. Ponadto z motywu 38 dyrektywy o ochronie danych w sprawach karnych wynika, że jeśli podejmowanie decyzji odbywa się wyłącznie na podstawie FRT, wówczas osoby, których dane dotyczą, muszą zostać poinformowane o cechach zautomatyzowanego podejmowania decyzji. Wskazywałoby to również, że jest to konkretny przypadek, w którym osobie, której dane dotyczą, należy udzielić dodatkowych informacji zgodnie z art. 13 ust. 2 dyrektywy o ochronie danych w sprawach karnych[61].

89. Wreszcie należy zauważyć, że zgodnie z art. 13 ust. 3 dyrektywy o ochronie danych w sprawach karnych, państwa członkowskie mogą przyjąć akty prawne, które ograniczają obowiązek udzielania informacji w konkretnych przypadkach dla określonych celów. Ma to zastosowanie w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów osoby, której dane dotyczą.

3.2.4.2 Prawo dostępu

90. Ogólnie rzecz biorąc, osoba, której dane dotyczą, ma prawo do otrzymania odpowiedzi pozytywnej lub negatywnej dotyczącej każdego przetwarzania jej danych osobowych oraz, w przypadku odpowiedzi pozytywnej, dostępu do danych osobowych jako takich, a także dodatkowych informacji wymienionych w art. 14 dyrektywy o ochronie danych w sprawach karnych. W przypadku FRT, gdy dane biometryczne są przechowywane i powiązane z tożsamością również za pomocą danych alfanumerycznych, właściwy organ powinien mieć możliwość potwierdzenia wniosku o dostęp na

[60] WP258, opinia dotycząca niektórych głównych zagadnień dyrektywy o ochronie danych w sprawach karnych (UE 2016/680), s. 17–18.

[61] Należy zwrócić uwagę na różnicę między „udostępnione osobie, której dane dotyczą" w art. 13 ust. 1 dyrektywy o ochronie danych w sprawach karnych a „przekazane osobie, której dane dotyczą" w art. 13 ust. 2 dyrektywy o ochronie danych w sprawach karnych. W art. 13 ust. 2 dyrektywy o ochronie danych w sprawach karnych administrator musi zapewnić, aby informacje docierały do osoby, której dane dotyczą, w przypadku gdy informacje opublikowane na stronie internetowej nie będą wystarczające.

podstawie wyszukiwania tych danych alfanumerycznych, bez konieczności dalszego przetwarzania danych biometrycznych innych osób (tj. poprzez wyszukiwanie w bazie danych za pomocą FRT). Należy przestrzegać zasady minimalizacji danych i nie należy przechowywać więcej danych niż jest to niezbędne w odniesieniu do celu przetwarzania.

3.2.4.3 Prawo do sprostowania danych osobowych

91. Ponieważ FRT nie zapewnia absolutnej dokładności, szczególnie ważne jest, aby administratorzy byli ostrożni w przypadku wniosków o sprostowanie danych osobowych. Sytuacja taka może mieć również miejsce, gdy osoba, której dane dotyczą, została umieszczona w niewłaściwej kategorii na podstawie FRT, np. niesłusznie umieszczona w kategorii podejrzanych na podstawie wstępnego założenia co do sposobu działania w nagraniu wideo. Dla osób, których dane dotyczą, ryzyko jest szczególnie poważne, jeśli w policyjnej bazie danych przechowywane są takie niedokładne (nieprawidłowe) dane lub są one udostępniane innym podmiotom. Administrator musi odpowiednio skorygować przechowywane dane i systemy FRT, zob. motyw 47 dyrektywy o ochronie danych w sprawach karnych.

3.2.4.4 Prawo do usunięcia danych

92. Przetwarzanie FRT w większości przypadków – jeśli nie jest wykorzystywane do weryfikacji/uwierzytelnienia 1 do 1 – oznacza przetwarzanie dużej liczby danych biometrycznych osób, których dane dotyczą. Dlatego ważne jest, aby administrator wcześniej rozważył, gdzie leżą granice jego celu i konieczności, tak aby wniosek o usunięcie danych zgodnie z art. 16 dyrektywy o ochronie danych w sprawach karnych mógł zostać rozpatrzony bez zbędnej zwłoki (ponieważ administrator musi między innymi usunąć dane osobowe, które są przetwarzane w zakresie wykraczającym poza to, na co pozwalają obowiązujące przepisy wynikające z art. 4, 8 i 10 dyrektywy o ochronie danych w sprawach karnych).

3.2.4.5 Prawa do ograniczenia przetwarzania

93. W przypadku gdy osoba, której dane dotyczą, kwestionuje prawidłowość danych i nie można stwierdzić ich prawidłowości (lub gdy dane osobowe muszą zostać zachowane do celów przyszłych dowodów), administrator ma obowiązek ograniczyć dane osobowe tej osoby, której dane dotyczą, zgodnie z art. 16 dyrektywy o ochronie danych w sprawach karnych. Staje się to szczególnie ważne, jeśli chodzi o technologię rozpoznawania twarzy (opartą na algorytmie (algorytmach), a tym samym nigdy niepokazującą ostatecznego wyniku) w sytuacjach, w których gromadzone są duże ilości danych, a dokładność i jakość identyfikacji może się różnić. W przypadku niskiej jakości materiałów wideo (np. z miejsca przestępstwa) wzrasta ryzyko wystąpienia wyników fałszywie dodatnich. Ponadto jeżeli wizerunki twarzy znajdujące się na liście obserwacyjnej nie są regularnie aktualizowane, zwiększa to również ryzyko wystąpienia wyników fałszywie dodatnich lub fałszywie ujemnych. W konkretnych przypadkach, gdy nie można usunąć danych ze względu na fakt, że uzasadnione przesłanki sugerują, że usunięcie mogłoby wpłynąć na uprawnione interesy osoby, której dane dotyczą, zgromadzone dane należy ograniczyć i przetwarzać tylko w celu, który zapobiegł ich usunięciu (zob. motyw 47 dyrektywy o ochronie danych w sprawach karnych).

3.2.4.6 Uzasadnione ograniczenia praw osób, których dane dotyczą

94. Jeśli chodzi o obowiązki informacyjne administratora i prawo dostępu osób, których dane dotyczą, ograniczenia są dozwolone tylko wtedy, gdy są określone w prawie, które z kolei musi stanowić środek konieczny i proporcjonalny w społeczeństwie demokratycznym, z należytym uwzględnieniem uzasadnionych interesów danej osoby fizycznej (zob. art. 13 ust. 3, art. 13 ust. 4, art. 15 i art. 16 ust. 4 dyrektywy o ochronie danych w sprawach karnych). W przypadku wykorzystywania FRT do celów ścigania przestępstw można oczekiwać, że będą one wykorzystywane w okolicznościach, w których informowanie osoby, której dane dotyczą, lub umożliwienie dostępu do danych byłoby szkodliwe dla

zamierzonego celu. Dotyczy to na przykład policyjnego śledztwa lub w celu ochrony bezpieczeństwa narodowego lub publicznego.

95. Prawo dostępu nie oznacza automatycznego dostępu do wszystkich informacji, np. w przypadku spraw karnych, w których występują dane osobowe. Realnym przykładem sytuacji, w których można dopuścić ograniczenia prawa, może być śledztwo.

3.2.4.7 Wykonywanie praw za pośrednictwem organu nadzorczego

96. W przypadkach, w których istnieją uzasadnione ograniczenia w wykonywaniu praw zgodnie z rozdziałem III dyrektywy o ochronie danych w sprawach karnych, osoba, której dane dotyczą, może zwrócić się do organu ochrony danych o wykonanie przysługujących jej praw w jej imieniu i sprawdzenie zgodności przetwarzania przez administratora z prawem. Na administratorze spoczywa obowiązek poinformowania osoby, której dane dotyczą, o możliwości skorzystania z przysługujących jej praw w taki sposób (zob. art. 17 dyrektywy o ochronie danych w sprawach karnych i art. 46 ust. 1 lit. g) dyrektywy o ochronie danych w sprawach karnych). W przypadku FRT oznacza to, że administrator musi zapewnić odpowiednie środki, aby taki wniosek mógł zostać rozpatrzony, np. poprzez umożliwienie przeszukania nagranego materiału, pod warunkiem, że osoba, której dane dotyczą, dostarczy wystarczających informacji w celu zlokalizowania jej danych osobowych.

3.2.5 Inne wymogi prawne i zabezpieczenia

3.2.5.1 Artykuł 27 Ocena skutków dla ochrony danych

97. Przed zastosowaniem FRT należy obowiązkowo przeprowadzić ocenę skutków dla ochrony danych, ponieważ ten rodzaj przetwarzania, w szczególności przy korzystaniu z nowych technologii, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania, z dużym prawdopodobieństwem może skutkować dużym zagrożeniem dla praw i wolności osób fizycznych. Biorąc pod uwagę, że korzystanie z FRT wiąże się z systematycznym automatycznym przetwarzaniem szczególnych kategorii danych, można założyć, że w takich przypadkach administrator będzie co do zasady zobowiązany do przeprowadzenia oceny skutków dla ochrony danych. Ocena skutków dla ochrony danych powinna zawierać co najmniej ogólny opis planowanych operacji przetwarzania, ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów, ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą, środki planowane w celu zaradzenia takiemu ryzyku, zabezpieczenia, środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać zgodność z prawem. EROD zaleca podanie wyników takich ocen lub co najmniej głównych ustaleń i wniosków zawartych w ocenie skutków dla ochrony danych do wiadomości publicznej jako środek wspierający zaufanie i przejrzystość[62].

3.2.5.2 Artykuł 28 Uprzednie konsultacje z organem nadzorczym

98. Zgodnie z art. 28 dyrektywy o ochronie danych w sprawach karnych, administrator lub podmiot przetwarzający musi skonsultować się z organem nadzorczym przed rozpoczęciem przetwarzania, jeżeli: a) ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu jego ograniczenia; lub b) odnośny rodzaj przetwarzania – zwłaszcza z użyciem nowych technologii, mechanizmów lub procedur – stwarza poważne ryzyko naruszenia praw i wolności osób, których dane dotyczą. Jak już wyjaśniono w sekcji 2.3 niniejszych wytycznych, EROD uważa, że większość przypadków wdrażania i stosowania FRT wiąże się z nieodłącznym wysokim ryzykiem naruszenia praw i wolności osób, których dane dotyczą. W

[62] Więcej informacji można znaleźć w dokumencie WP248 rev.01 Ocena skutków dla ochrony danych, wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko".

związku z tym, oprócz oceny skutków dla ochrony danych, organ wdrażający FRT powinien skonsultować się z właściwym organem nadzorczym przed wdrożeniem systemu.

3.2.5.3 Artykuł 29 Bezpieczeństwo przetwarzania

99. Unikalny charakter danych biometrycznych uniemożliwia ich zmianę przez osobę, której dane dotyczą, w przypadku ich ujawnienia, np. w wyniku naruszenia ochrony danych. W związku z tym właściwy organ, wdrażający lub stosujący FRT powinien zwracać szczególną uwagę na bezpieczeństwo przetwarzania, zgodnie z art. 29 dyrektywy o ochronie danych w sprawach karnych. W szczególności organ ścigania powinien zapewnić zgodność systemu z odpowiednimi normami i wdrożyć zabezpieczenia techniczne wzorców biometrycznych[63]. Obowiązek ten jest jeszcze bardziej istotny, jeśli organ ścigania korzysta z usług zewnętrznego dostawcy usług (podmiotu przetwarzającego dane).

3.2.5.4 Artykuł 20 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

100. Uwzględnienie ochrony danych w fazie projektowania i domyślna ochrona danych, zgodnie z art. 20 dyrektywy o ochronie danych w sprawach karnych, mają na celu zapewnienie, aby zasady i zabezpieczenia w zakresie ochrony danych, takie jak minimalizacja danych i ograniczenie ich przechowywania, były wbudowane w technologię poprzez odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, nawet przed rozpoczęciem przetwarzania danych osobowych i były stosowane w całym cyklu ich życia. Biorąc pod uwagę nieodłączne wysokie ryzyko dla praw i wolności osób fizycznych, przy wyborze takich środków nie należy kierować się wyłącznie względami ekonomicznymi[64], ale dążyć do wdrożenia najnowocześniejszych technologii ochrony danych. Podobnie, jeśli organ ścigania zamierza stosować i wykorzystywać FRT od zewnętrznych dostawców, musi zapewnić, na przykład poprzez procedurę udzielania zamówień, aby wdrażane były wyłącznie FRT oparte na zasadach ochrony danych w fazie projektowania i domyślnej ochrony danych[65]. Oznacza to również, że przejrzystość funkcjonowania FRT nie jest ograniczona roszczeniami dotyczącymi tajemnic handlowych lub praw własności intelektualnej.

3.2.5.5 Artykuł 25 Ewidencja czynności

101. Dyrektywa o ochronie danych w sprawach karnych przewiduje różne metody wykazania przez administratora lub podmiot przetwarzający zgodności przetwarzania z prawem oraz zapewnienia integralności i bezpieczeństwa danych. W tym względzie bardzo przydatnym narzędziem i ważnym zabezpieczeniem służącym do weryfikacji zgodności przetwarzania z prawem, zarówno wewnętrznie (tj. samokontroli), jak i przez zewnętrzne organy nadzorcze, takie jak organy ochrony danych, jest ewidencja systemowa. Zgodnie z art. 25 dyrektywy o ochronie danych w sprawach karnych należy ewidencjonować przynajmniej następujące operacje przetwarzania prowadzone w zautomatyzowanych systemach przetwarzania: zbieranie, modyfikowanie, przeglądanie, ujawnianie wraz z przekazywaniem, łączenie i usuwanie. Ponadto ewidencja przeglądania i ujawniania pozwala ustalić zasadność, datę i godzinę takich operacji oraz w miarę możliwości tożsamość osoby, która przeglądała lub ujawniła dane osobowe, oraz tożsamość odbiorców takich danych osobowych. Ponadto w kontekście systemów rozpoznawania twarzy zaleca się ewidencjonowanie następujących

[63] Zobacz na przykład: ISO/IEC 24745 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Ochrona informacji biometrycznych.

[64] Zobacz motyw 53 dyrektywy o ochronie danych w sprawach karnych.

[65] Więcej informacji można znaleźć w wytycznych EROD dotyczących uwzględnienia ochrony danych w fazie projektowania i domyślnej ochrony danych https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

dodatkowych operacji przetwarzania danych (częściowo wykraczających poza zakres art. 25 dyrektywy o ochronie danych w sprawach karnych):

- zmiany referencyjnej bazy danych (dodanie, usunięcie lub aktualizacja). W ewidencji należy przechowywać kopię odpowiedniego (dodanego, usuniętego lub zaktualizowanego) obrazu, jeśli w inny sposób nie można zweryfikować zgodności z prawem lub wyniku operacji przetwarzania;
- próby identyfikacji lub weryfikacji, w tym wynik i poziom zaufania. Należy stosować zasadę ścisłej minimalizacji, tak aby w ewidencji przechowywany był tylko identyfikator obrazu z referencyjnej bazy danych, zamiast obrazu referencyjnego. Należy unikać ewidencjonowania wejściowych danych biometrycznych, chyba że istnieje taka konieczność (np. tylko w przypadkach dopasowania);
- identyfikator użytkownika, który zwrócił się o przeprowadzenie próby identyfikacji lub weryfikacji;
- wszelkie dane osobowe przechowywane w ewidencji systemów podlegają ścisłym ograniczeniom celu (np. audyty) i nie powinny być wykorzystywane do innych celów (np. do dalszego rozpoznawania lub dalszej weryfikacji, z wykorzystaniem obrazu, który został usunięty z referencyjnych baz danych). W celu zapewnienia integralności ewidencji należy stosować środki ochrony, przy czym wysoce zalecane jest stosowanie automatycznych systemów monitorowania w celu wykrywania nadużyć w ewidencji. W przypadku ewidencji referencyjnej bazy danych środki ochrony powinny być równoważne z referencyjną bazą danych, w odniesieniu do przechowywania obrazów twarzy. Należy również wdrożyć automatyczne procesy zapewniające egzekwowanie okresu przechowywania danych ewidencjonowanych.

3.2.5.6 Artykuł 4 ust. 4 Rozliczalność

102. Administrator musi być w stanie wykazać zgodność przetwarzania z zasadami określonymi w art. 4 ust. 1–3, por. art. 4 ust. 4 dyrektywy o ochronie danych w sprawach karnych. W tym względzie kluczowe znaczenie ma systematyczna i aktualna dokumentacja systemu (w tym aktualizacje, uaktualnienia i szkolenia algorytmiczne), środki techniczne i organizacyjne (w tym monitorowanie wydajności systemu i potencjalna interwencja ludzka) oraz przetwarzanie danych osobowych. Aby wykazać zgodność przetwarzania z prawem, szczególnie ważnym elementem jest ewidencjonowanie zgodnie z art. 25 dyrektywy o ochronie danych w sprawach karnych (por. sekcja 3.2.5.5). Zasada rozliczalności odnosi się nie tylko do systemu i przetwarzania, ale także do dokumentacji gwarancji proceduralnych, takich jak oceny niezbędności i proporcjonalności, oceny skutków dla ochrony danych, a także konsultacji wewnętrznych (np. zatwierdzenie projektu przez kierownictwo lub wewnętrzne decyzje w sprawie wartości wskaźnika zaufania) i konsultacji zewnętrznych (np. organ ochrony danych). Załącznik II zawiera szereg elementów w tym zakresie.

3.2.5.7 Artykuł 47 Skuteczny nadzór

103. Skuteczny nadzór ze strony właściwych organów ochrony danych jest jednym z najważniejszych zabezpieczeń podstawowych praw i wolności osób fizycznych, wobec których stosowane są FRT. Jednocześnie zapewnienie każdemu organowi ochrony danych niezbędnych zasobów kadrowych, technicznych i finansowych, pomieszczeń i infrastruktury jest warunkiem koniecznym skutecznego wypełniania przez nie ich zadań i wykonywania ich uprawnień[66]. Jeszcze ważniejsze niż liczba dostępnych pracowników są umiejętności ekspertów, którzy powinni posiadać wiedzę z bardzo szerokiego zakresu zagadnień – od śledztw i współpracy policyjnej po analizę dużych zbiorów danych i sztuczną inteligencję. W związku z tym państwa członkowskie powinny zapewnić organom nadzorczym

[66] Zobacz komunikat Komisji „Pierwsze sprawozdanie dotyczące stosowania i funkcjonowania dyrektywy (UE) 2016/680 o ochronie danych w sprawach karnych”, COM(2022) 364 final, s. 3.4.1.

odpowiednie i wystarczające zasoby, aby umożliwić im wypełnianie ich mandatu w zakresie ochrony praw osób, których dane dotyczą, oraz uważnie śledzić wszelkie zmiany w tym zakresie[67].

4 WNIOSKI

104. Korzystanie z technologii rozpoznawania twarzy jest nierozerwalnie związane z przetwarzaniem znacznych ilości danych osobowych, w tym szczególnych kategorii danych. Twarz oraz, bardziej ogólnie, dane biometryczne są trwale i nieodwołalnie powiązane z tożsamością danej osoby. W związku z tym korzystanie z technologii rozpoznawania twarzy ma bezpośredni lub pośredni wpływ na szereg podstawowych praw i wolności zapisanych w Karcie praw podstawowych Unii Europejskiej, które mogą wykraczać poza ochronę prywatności i danych, takich jak godność człowieka, swoboda przemieszczania się, wolność zgromadzania się i inne. Jest to szczególnie istotne w obszarze ścigania przestępstw i wymiaru sprawiedliwości w sprawach karnych.

105. EIOD rozumie potrzebę korzystania przez organy ścigania z najlepszych możliwych narzędzi do szybkiej identyfikacji sprawców aktów terrorystycznych i innych poważnych przestępstw. Narzędzia takie należy jednak stosować w ścisłej zgodności z obowiązującymi ramami prawnymi i tylko w przypadkach, gdy spełniają one wymogi konieczności i proporcjonalności określone w art. 52 ust. 1 Karty. Co więcej, choć nowoczesne technologie mogą być częścią rozwiązania, w żadnym wypadku nie są „cudownym środkiem".

106. Istnieją pewne przypadki użycia technologii rozpoznawania twarzy, które stwarzają niedopuszczalnie wysokie ryzyko dla osób fizycznych i społeczeństwa (ang. „red lines"). Z tych powodów EROD i EIOD opowiedzieli się za tym, aby wprowadzić ich ogólny zakaz[68].

107. W szczególności zdalna identyfikacja biometryczna osób fizycznych w przestrzeniach publicznych stwarza wysokie ryzyko ingerencji w życie prywatne osób fizycznych i nie ma dla takiej praktyki miejsca w demokratycznym społeczeństwie, ponieważ ze swej natury pociąga za sobą masową inwigilację. W tym samym duchu EROD uważa, że systemy rozpoznawania twarzy wspierane przez sztuczną inteligencję dzielących osoby fizyczne w oparciu o ich dane biometryczne na grupy ze względu na pochodzenie etniczne, płeć, orientację polityczną lub seksualną za niezgodne z Kartą. Ponadto EROD jest przekonana, że wykorzystanie technologii rozpoznawania twarzy lub podobnych technologii do wyciągania wniosków na temat emocji osoby fizycznej jest wysoce niepożądane i powinno być zakazane, ewentualnie z kilkoma należycie uzasadnionymi wyjątkami. Ponadto EROD uważa, że przetwarzanie danych osobowych w kontekście egzekwowania prawa, które opierałoby się na bazie danych wypełnionej poprzez gromadzenie danych osobowych na masową skalę i w sposób niekontrolowany, np. poprzez „scraping" fotografii i wizerunków twarzy dostępnych online, w szczególności udostępnianych za pośrednictwem sieci społecznościowych, samo w sobie nie spełniałoby rygorystycznego wymogu „bezwzględnej niezbędności" określonego w prawie Unii.

[67] Zobacz wkład EROD w sporządzoną przez Komisję Europejską ocenę dyrektywy o ochronie danych w sprawach karnych na podstawie art. 62 ust. 14., https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

[68] Zobacz opinia EROD-EIOD nr 5/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji).https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

5 ZAŁĄCZNIKI

Załącznik I: Wzór wsparcia

Załącznik II: Praktyczne wytyczne dotyczące zarządzania projektami FRT w organach ścigania

Załącznik III: Praktyczne przykłady

ZAŁĄCZNIK I – SZABLON OPISU SCENARIUSZY

(Z zestawem informacji o aspektach poruszanych w scenariuszu)

Opis przetwarzania:

- Opis przetwarzania, kontekst (związek z przestępstwem), cel

Źródło informacji:

- Rodzaje osób, których dane dotyczą: ☐ wszyscy obywatele ☐ skazani ☐ podejrzani ☐ dzieci ☐ inne osoby, których dane dotyczą wymagające szczególnej opieki
- Źródło obrazu: ☐ przestrzeń publiczna ☐ internet ☐ podmiot prywatny ☐ inne osoby fizyczne ☐ inne .....
- Związek z przestępczością: ☐ bezpośredni związek czasowy ☐ brak bezpośredniego związku czasowego ☐ bezpośredni związek geograficzny ☐ brak bezpośredniego związku geograficznego ☐ Nie koniecznie
- Sposób przechwytywania informacji: ☐ zdalnie ☐ w kabinie lub w kontrolowanym środowisku
- Kontekst – wpływ na inne prawa podstawowe:
  ☐ Nie
  Tak, mianowicie ☐ wolność zgromadzeń
  ☐ wolność słowa
  ☐ różne:.....
- Możliwości uzyskania dodatkowych źródeł informacji na temat osoby, której dane dotyczą:
  ☐ dokument tożsamości☐ korzystanie z publicznych sieci telefonicznych
  ☐ tablica rejestracyjna pojazdu
  ☐ inne .....

Referencyjna baza danych (z którą porównywane są przechwycone informacje):

- Specyfika: ☐ ogólne bazy danych ☐ szczególne bazy danych związane z obszarem przestępczości
- Opis sposobu tworzenia referencyjnych baz danych (i podstawa prawna)
- Zmiana celu bazy danych (np. głównym celem było bezpieczeństwo własności prywatnej):
  ☐ TAK
  ☐ NIE

Algorytm:

- Rodzaj przetwarzania: ☐ weryfikacja 1 do 1 (uwierzytelnienie) ☐ identyfikacja 1 do wielu
- Uwagi dotyczące dokładności
- Zabezpieczenia techniczne

Wyniki:

- Oddziaływanie ☐ Bezpośrednie (np. osoba, której dane dotyczą, może zostać zatrzymana, przesłuchana, zachowanie dyskryminujące)

  ☐ Brak bezpośredniego oddziaływania (wykorzystywane do modeli statystycznych, brak poważnych działań prawnych przeciwko osobom, których dane dotyczą)

- Zautomatyzowana decyzja: ☐ TAK ☐ NIE
- Czas przechowywania

Analiza prawna:

- Analiza konieczności i proporcjonalności – cel / poważny charakter przestępstwa / liczba osób niezaangażowanych, ale dotkniętych przetwarzaniem danych
- Rodzaj informacji przekazanych wcześniej osobie, której dane dotyczą: ☐ Przy wjeździe do określonego obszaru

  ☐ Ogólnie na stronie internetowej organu ścigania

  ☐ Na stronie internetowej organu ścigania w odniesieniu do konkretnego przetwarzania

  ☐ Inne .....
- Obowiązujące ramy prawne:

  ☐ Dyrektywa o ochronie danych w sprawach karnych w większości skopiowana do prawa krajowego

  ☐ Ogólne przepisy prawa krajowego dotyczące wykorzystywania danych biometrycznych przez ograny ścigania

  ☐ Szczególne przepisy prawa krajowego dotyczące tego przetwarzania (rozpoznawanie twarzy) przez właściwy organ

  ☐ Szczególne przepisy krajowe dotyczące tego przetwarzania (zautomatyzowana decyzja)

Wniosek:

Ogólne rozważania dotyczące tego, czy opisane przetwarzanie jest prawdopodobnie zgodne z prawem UE (i kilka wskazówek dotyczących wymogów prawnych)

ZAŁĄCZNIK II: PRAKTYCZNE WYTYCZNE DOTYCZĄCE ZARZĄDZANIA PROJEKTAMI FRT W ORGANACH ŚCIGANIA

Niniejszy załącznik zawiera dodatkowe praktyczne wskazówki dla organów ścigania planujących rozpoczęcie projektu obejmującego technologię rozpoznawania twarzy („FRT"). Zawiera on więcej informacji na temat środków organizacyjnych i technicznych, które należy wziąć pod uwagę podczas wdrażania projektu i nie powinien być traktowany jako wyczerpująca lista kroków/środków, które należy podjąć. Jego treść należy również rozpatrywać w powiązaniu z wytycznymi EROD nr 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo[69] oraz wszelkimi rozporządzeniami UE/EOG oraz wytycznymi EROD dotyczącymi korzystania z technologii sztucznej inteligencji.

Niniejszy załącznik zawiera wytyczne oparte na założeniu, że organy ścigania będą zamawiać FRT (jako produkty gotowe). Jeśli organ ścigania planuje rozwijać (dalej szkolić) FRT, wówczas obowiązują dodatkowe wymagania dotyczące wyboru niezbędnych zbiorów danych szkoleniowych, walidacyjnych i testowych, które będą wykorzystywane podczas rozwoju, oraz ról/środków dla środowiska rozwoju. Podobnie, gotowy produkt może wymagać dalszych dostosowań do zamierzonego zastosowania, w którym to przypadku należy spełnić wyżej wymienione wymagania dotyczące wyboru zbiorów danych testowych, walidacyjnych i szkoleniowych.

Sama przynależność do tego samego organu ścigania nie zapewnia pełnego dostępu do danych biometrycznych. Podobnie jak w przypadku wszelkich innych kategorii danych osobowych, dane biometryczne zebrane w jakimkolwiek celu związanym ze ściganiem przestępstw na podstawie określonej podstawy prawnej nie mogą być wykorzystywane bez odpowiedniej podstawy prawnej dla innego celu związanego ze ściganiem przestępstw (art. 4 ust. 2 dyrektywy (UE) 2016/680). Ponadto rozwijanie/szkolenie narzędzia FRT jest uważane za inny cel i należy ocenić, czy przetwarzanie danych biometrycznych w celu pomiaru wydajności/szkolenia technologii, aby uniknąć wpływu niskiej wydajności technologii na osoby, których dane dotyczą, jest konieczne i proporcjonalne, biorąc pod uwagę pierwotny cel przetwarzania.

1. ROLE I OBOWIĄZKI

Jeżeli organ ścigania korzysta z FRT w celu wykonywania swoich zadań wchodzących w zakres dyrektywy o ochronie danych w sprawach karnych (zapobieganie przestępstwom, prowadzenie dochodzeń w ich sprawie, wykrywanie ich i ściganie itp., zgodnie z art. 3 dyrektywy o ochronie danych w sprawach karnych), można go uznać za administratora FRT. Organy ścigania składają się jednak z kilku jednostek/wydziałów, które mogą być zaangażowane w przetwarzanie danych, albo poprzez określenie procesu stosowania FRT, albo poprzez stosowanie go w praktyce. Ze względu na specyfikę tej technologii może zaistnieć potrzeba zaangażowania różnych jednostek w celu wsparcia pomiaru jej wydajności lub dalszego jej szkolenia.

Projekt związany z FRT może wymagać zaangażowania kilku zainteresowanych stron[70] w ramach organów ścigania:

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

[70] Poniższe role wskazują różne zainteresowane strony i ich obowiązki w ramach projektu związanego z FRT. Chociaż język użyty do opisania ról w tym załączniku nie ma charakteru wiążącego, każdy organ ścigania musi

- Kierownictwo najwyższego szczebla – zatwierdzenie projektu po wyważeniu ryzyka i potencjalnych korzyści.
- Inspektor ochrony danych lub dział prawny organu ścigania – pomoc w ocenie zgodności z prawem wdrożenia określonego projektu FRT; pomoc w przeprowadzeniu oceny skutków dla ochrony danych; zapewnienie poszanowania i wykonywania praw osób, których dane dotyczą.
- Właściciel procesu – konkretna jednostka działająca w ramach właściwego organu ścigania w celu opracowania projektu, decydująca o szczegółach projektu FRT, w tym o wymaganiach dotyczących wydajności systemu; decydująca o odpowiedniej miarach sprawiedliwości; ustalająca poziom ufności[71]; ustalająca dopuszczalne progi błędu; identyfikująca potencjalne zagrożenia, jakie projekt FRT stwarza dla praw i wolności osób fizycznych (poprzez konsultacje również z inspektorem ochrony danych i działem IT AI lub Data Science (patrz poniżej)) oraz przedstawiająca je najwyższemu kierownictwu. Właściciel procesu skonsultuje się również z administratorem referencyjnej bazy danych, przed podjęciem decyzji w sprawie szczegółów projektu FRT, aby zrozumieć zarówno cel wykorzystania referencyjnej bazy danych, jak i jej szczegóły techniczne. W przypadku ponownego szkolenia zamówionego FRT, właściciel procesu będzie również odpowiedzialny za wybór zestawu danych szkoleniowych. Jako jednostka, której zadaniem jest opracowanie i podjęcie decyzji w sprawie szczegółów projektu, właściciel procesu jest odpowiedzialny za przeprowadzenie oceny skutków dla ochrony danych.
- Departament IT AI lub Data Science – pomoc w przeprowadzaniu oceny skutków dla ochrony danych; wyjaśnienie dostępnych wskaźników do pomiaru wydajności systemu, sprawiedliwości[72] i potencjalnych błędów; wdrożenie technologii i zabezpieczeń technicznych, aby zapobiec nieuprawnionemu dostępowi do zgromadzonych danych, cyberatakom itp. W przypadku ponownego przeszkolenia zamówionego FRT dział IT AI lub Data Science szkoli system na podstawie zbioru danych szkoleniowych dostarczonego przez właściciela procesu. Dział ten będzie również odpowiedzialny za określenie środków mających na celu ograniczenie ryzyka zidentyfikowanego wspólnie przez właścicieli procesów (np. ryzyko związane ze sztuczną inteligencją, takie jak ataki na wnioskowanie modelowe).
- Użytkownicy końcowi (tacy jak funkcjonariusze policji w terenie lub w laboratoriach kryminalistycznych) – przeprowadzenie porównania z bazą danych; krytyczny przegląd wyników z uwzględnieniem wcześniejszych dowodów i przekazanie właścicielowi procesu informacji zwrotnej na temat wyników fałszywie dodatnich i oznak możliwej dyskryminacji.
- Menedżer referencyjnej bazy danych – specjalna jednostka w ramach właściwego organu ścigania odpowiedzialna za gromadzenie i zarządzanie referencyjną bazą danych, czyli bazą danych, z którą porównywane będą wizerunki, w tym za usuwanie wizerunków twarzy po upływie określonego okresu przechowywania. Taka baza danych może zostać utworzona specjalnie na potrzeby planowanego projektu FRT lub może istnieć wcześniej, do zgodnych celów. Menedżer referencyjnej bazy danych jest odpowiedzialny za określenie, kiedy i w jakich okolicznościach wizerunki twarzy mogą być przechowywane, a także za ustalenie wymagań dotyczących przechowywania danych (według czasu lub innych kryteriów).

Ponieważ większość przypadków wdrażania i wykorzystywania FRT wiąże się z nieodłącznym wysokim ryzykiem dla praw i wolności osób, których dane dotyczą, organ nadzorczy ds. ochrony danych

zdefiniować i przypisać podobne role zgodnie ze swoją organizacją. Może się zdarzyć, że jednostka pełni więcej niż jedną rolę, na przykład właściciela procesu i administratora referencyjnej bazy danych lub właściciela procesu i działu IT AI i/lub Data Science (w sytuacji, gdy jednostka właściciela procesu posiada całą niezbędną wiedzę techniczną).

[71] Poziom ufności to poziom ufności predykcji (dopasowania) w formie prawdopodobieństwa. Np. porównanie dwóch wzorców daje 90% pewności, że należą one do tej samej osoby. Poziom ufności różni się od wydajności FRT, jednak wpływa na wydajność. Im wyższy próg ufności, tym mniej wyników fałszywie dodatnich i więcej wyników fałszywie ujemnych FRT.

[72] Sprawiedliwość można zdefiniować jako brak niesprawiedliwej, niezgodnej z prawem dyskryminacji, takiej jak uprzedzenia ze względu na płeć lub rasę.

powinien być również zaangażowany w uprzednie konsultacje wymagane na mocy art. 28 dyrektywy o ochronie danych w sprawach karnych.

2. ROZPOCZĘCIE/PRZED ZAKUPEM SYSTEMU FRT

Właściciel procesu w organie ścigania powinien najpierw dokładnie zrozumieć procesy prowadzące do wykorzystania FRT (przypadki użycia) i upewnić się, że istnieje podstawa prawna pozwalająca na uzasadnienie planowanego przypadku użycia. Na tej podstawie powinni:

- Formalnie opisać przypadek użycia. Należy opisać problem do rozwiązania i sposób, w jaki FRT zapewni rozwiązanie, a także przegląd procesu (zadania), w którym FRT zostanie zastosowana. W tym względzie organy ścigania powinny dokumentować co najmniej[73]:
  - kategorie danych osobowych rejestrowanych w procesie;
  - założenia i konkretne cele, do których FRT będą wykorzystywane, w tym potencjalne konsekwencje dla osoby, której dane dotyczą, w przypadku dopasowania;
  - kiedy i w jaki sposób gromadzone będą wizerunki twarzy (w tym informacje o kontekście tego gromadzenia, np. przy bramce na lotnisku, nagrania z kamer bezpieczeństwa przed sklepem, w którym popełniono przestępstwo itp. oraz kategorie osób, których dane dotyczą, a których dane biometryczne będą przetwarzane);
  - baza danych, z którą porównywane będą wizerunki (referencyjna baza danych), a także informacje o sposobie jej utworzenia, rozmiarze i jakości zawartych w niej danych biometrycznych;
  - podmioty organów ścigania, które będą upoważnione do korzystania z systemu FRT i działania na jego podstawie w kontekście ścigania przestępstw (ich profile i prawa dostępu muszą zostać zdefiniowane przez właściciela procesu);
  - przewidywany okres przechowywania wprowadzonych danych lub moment, który określi koniec tego okresu (taki jak zamknięcie lub zakończenie postępowania karnego zgodnie z krajowym prawem procesowym, dla którego zostały one pierwotnie zebrane), a także wszelkie późniejsze działania (usunięcie tych danych, anonimizacja i wykorzystanie do celów statystycznych lub badawczych itp.);
  - wdrożenie i dostępność ewidencji i prowadzonych rejestrów;
  - wskaźniki wydajności (np. dokładność, precyzja, wycofanie, wynik F1) i ich minimalne akceptowalne progi[74];
  - szacunek, ile osób będzie objętych systemem FRT w jakim okresie / przy jakiej okazji.
- Przeprowadzić ocenę niezbędności i proporcjonalności[75]. Fakt, że istnieje taka technologia, nie powinien być czynnikiem decydującym o jej stosowaniu. Właściciel procesu musi najpierw ocenić, czy istnieje odpowiednia podstawa prawna dla planowanego przetwarzania. W tym celu należy skonsultować się z inspektorem ochrony danych i ze służbą prawną. Czynnikiem zachęcającym do

[73] Załącznik I zawiera wykaz elementów, które pomagają administratorowi opisać przypadek użycia FRT.

[74] Istnieją różne wskaźniki do oceny wydajności systemu FRT. Każdy wskaźnik dostarcza innego obrazu wyników systemu, przy czym jego skuteczność w dostarczaniu prawidłowego obrazu funkcjonowania systemu FRT zależy od przypadku użycia FRT. W przypadku gdy celem jest osiągnięcie wysokiego odsetka poprawnych dopasowań twarzy, można zastosować wskaźniki takie jak precyzja i przywołanie. Wskaźniki te nie mierzą jednak tego, jak FRT radzi sobie z przykładami negatywnymi (ile z nich zostało nieprawidłowo dopasowanych przez system). Właściciel procesu, wspierany przez dział IT AI i Data Science, powinien być w stanie określić wymagania dotyczące wydajności i wyrazić je za pomocą najbardziej odpowiednich wskaźników zgodnie z przypadkiem użycia FRT.

[75] Można rozważyć dalsze kroki w celu zapewnienia konieczności dostosowania i korzystania z systemu, dlatego podczas oceny niezbędności i proporcjonalności można również nieznacznie zmienić opis przypadku użycia.

wdrożenia FRT powinien być fakt, że jest to konieczne i proporcjonalne w odniesieniu do konkretnie określonego problemu organów ścigania. Należy to ocenić w zależności od celu / powagi przestępstwa / liczby osób niezaangażowanych, ale objętych systemem FRT. W celu oceny zgodności z prawem należy wziąć pod uwagę co najmniej: dyrektywę o ochronie danych osobowych w sprawach karnych[76], RODO[77] [78], wszelkie istniejące ramy prawne dotyczące sztucznej inteligencji[79] i wszystkie towarzyszące im wytyczne organów nadzorczych ds. ochrony danych (takie jak wytyczne EROD 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo[80]). Te akty prawne UE powinny być zawsze zgodne z obowiązującymi wymogami krajowymi, zwłaszcza w dziedzinie prawa karnego procesowego. Ocena proporcjonalności powinna określać podstawowe prawa osób, których dane dotyczą, które mogą zostać naruszone (poza prywatnością i ochroną danych). Powinna również opisywać i uwzględniać wszelkie ograniczenia (lub ich brak) nałożone w przypadku użycia na system FRT. Na przykład, czy system będzie działał w sposób ciągły czy tymczasowy i czy będzie ograniczony do określonego obszaru geograficznego.

- Przeprowadzić ocenę skutków dla ochrony danych[81]. Należy przeprowadzić ocenę skutków dla ochrony danych, ponieważ wdrożenie FRT w obszarze ścigania przestępstw może skutkować wysokim ryzykiem dla praw i wolności osób fizycznych[82]. Ocena skutków dla ochrony danych powinna zawierać w szczególności: ogólny opis planowanych operacji przetwarzania[83], ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą[84], środki planowane w celu rozwiązania takiego ryzyka, zabezpieczenia, środki i mechanizmy bezpieczeństwa mające

[76] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar.

[77] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

[78] W przypadkach, w których projekt naukowy mający na celu badanie wykorzystania FRT wymagałby przetwarzania danych osobowych, ale takie przetwarzanie nie podlegałoby art. 4 ust. 3 dyrektywy o ochronie danych w sprawach karnych, zasadniczo zastosowanie miałoby RODO (art. 9 ust. 2 dyrektywy o ochronie danych w sprawach karnych). Dyrektywa o ochronie danych w sprawach karnych nadal miałaby zastosowanie w przypadku projektów pilotażowych, po których nastąpiłyby działania organów ścigania.

[79] Na przykład złożono wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY USTANAWIAJĄCEGO ZHARMONIZOWANE PRZEPISY DOTYCZĄCE SZTUCZNEJ INTELIGENCJI (AKT W SPRAWIE SZTUCZNEJ INTELIGENCJI) I ZMIENIAJĄCEGO NIEKTÓRE AKTY USTAWODAWCZE UNII, jednak nie został on jeszcze ustanowiony jako rozporządzenie.

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

[81] Dalsze wytyczne dotyczące ocen skutków dla ochrony danych można znaleźć w dokumencie: Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko dla celów rozporządzenia 2016/679, WP 248 rev.01, dostępne pod adresem: https://ec.europa.eu/newsroom/article29/items/611236 oraz w zestawie narzędzi EIOD „Accountability on the ground" [„Rozliczalność w praktyce"], część II, dostępnych pod adresem: https://edps.europa.eu/node/4582_en

[82] FRT, w zależności od przypadku użycia, może podlegać następującym kryteriom uruchamiającym przetwarzanie wysokiego ryzyka (z Wytycznych dotyczących oceny skutków dla ochrony danych, WP 248 rev.01): systematyczne monitorowanie, przetwarzanie danych na dużą skalę, dopasowywanie lub łączenie zbiorów danych, innowacyjne wykorzystanie lub zastosowanie nowych rozwiązań technologicznych lub organizacyjnych.

[83] Oprócz oceny ryzyka, częścią oceny skutków dla ochrony danych jest również opis przetwarzania, a także ocena konieczności i proporcjonalności, jak już opisano w powyżej. W razie potrzeby w ocenie skutków dla ochrony danych osobowych zostanie przedstawiony bardziej szczegółowy opis przepływu danych osobowych.

[84] Analiza ryzyka dla osób, których dane dotyczą, powinna obejmować ryzyko związane z miejscem porównywanych wizerunków twarzy (lokalne/zdalne), ryzyko związane z podmiotami przetwarzającymi lub podwykonawcami przetwarzania, a także ryzyko specyficzne dla uczenia maszynowego, gdy jest ono stosowane (np. zatruwanie danych (ang. data poisoning), niepożądane przykłady).

zapewnić ochronę danych osobowych i wykazanie zgodności z prawem. Ocena skutków dla ochrony danych jest procesem ciągłym, dlatego na każdym etapie projektu należy dodawać wszelkie nowe elementy przetwarzania i aktualizować ocenę ryzyka.

- Uzyskać zgodę najwyższego kierownictwa poprzez wyjaśnienie zagrożeń dla praw i wolności osób, których dane dotyczą (wynikających z przypadku użycia i technologii) oraz odpowiednich planów zarządzania ryzykiem.

3. PODCZAS ZAKUPU I PRZED WDROŻENIEM FRT

- Określić kryteria wyboru FRT (algorytmu). Właściciel procesu powinien z pomocą działu IT AI lub Data Science określić kryteria wyboru algorytmu. W praktyce obejmują one wskaźniki sprawiedliwości i wydajności określone w opisie przypadku użycia. Takie kryteria powinny również obejmować informacje dotyczące danych, na których szkolono algorytm. Aby ograniczyć stronniczość, zestaw szkoleniowy, testowy i walidacyjny muszą obejmować w wystarczającym stopniu próbki wszystkich cech podmiotów danych, wobec których stosuje się FRT (na przykład wiek, płeć i rasę). Dostawca FRT powinien przedstawić informacje i wskaźniki dotyczące zbiorów danych dotyczących szkolenia, testowania i walidacji FRT oraz opisać środki podjęte w celu zmierzenia i ograniczenia potencjalnej bezprawnej dyskryminacji i stronniczości. Właściciel procesu, o ile to możliwe, musi sprawdzić, czy istniała podstawa prawna dla dostawcy do korzystania z tego zbioru danych w celu szkolenia algorytmów (na podstawie informacji udostępnionych przez dostawcę). Właściciel procesu powinien również dopilnować, aby dostawca FRT stosował normy bezpieczeństwa związane z danymi biometrycznymi, takie jak ISO/IEC 24745, która zawiera wytyczne dotyczące ochrony informacji biometrycznych w ramach różnych wymogów dotyczących poufności, integralności i odnawialności lub odwołalności podczas przechowywania i przesyłania, a także wymogi i wytyczne dotyczące bezpiecznego i zgodnego z prywatnością zarządzania i przetwarzania informacji biometrycznych.

- Ponownie przeszkolić algorytm (jeśli to konieczne). Właściciel procesu powinien zapewnić, aby częścią zamówionych usług było również dostrojenie systemu FRT w celu osiągnięcia większej dokładności przed jego użyciem. Jeśli do spełnienia wskaźników dokładności niezbędne jest dodatkowe szkolenie zakupionego systemu FRT, właściciel procesu, oprócz podjęcia decyzji o ponownym szkoleniu, musi zdecydować, z pomocą działu IT AI lub działu Data Science, który zbiór danych będzie odpowiedni i reprezentatywny oraz sprawdzić, czy takie wykorzystanie danych jest zgodne z prawem.
- Ustanowić odpowiednie zabezpieczenia w celu uwzględnienia zagrożeń związanych z bezpieczeństwem, stronniczością i niską wydajnością. Obejmuje to ustanowienie procesu monitorowania FRT po jego użyciu (ewidencjonowanie i informacje zwrotne dotyczące dokładności i sprawiedliwości wyników). Ponadto należy zapewnić identyfikację, pomiar i ograniczenie ryzyka, które jest specyficzne dla niektórych systemów uczenia maszynowego i FRT (np. zatruwanie danych, niepożądane przykłady, inwersja modelu, ataki na białe skrzynki). Właściciel procesu powinien również ustanowić odpowiednie zabezpieczenia, aby zapewnić przestrzeganie wymogów zatrzymywania danych w odniesieniu do danych biometrycznych zawartych w zbiorze danych do ponownego szkolenia.
- Dokumentować system FRT. Powinno to obejmować ogólny opis systemu FRT, szczegółowy opis elementów systemu FRT i procesu jego tworzenia, szczegółowe informacje na temat monitorowania, funkcjonowania i kontroli systemu FRT oraz szczegółowy opis ryzyka i środków ograniczających ryzyko. Elementy zawarte w tej dokumentacji będą obejmować główne elementy opisu systemu FRT z poprzednich faz (patrz wyżej), jednak zostaną one wzbogacone o informacje

związane z monitorowaniem wydajności i wprowadzaniem zmian w systemie, w tym wszelkie aktualizacje wersji lub ponowne szkolenia.

- Stworzyć podręczniki użytkownika, wyjaśniające technologię i przypadki użycia. Muszą one w jasny sposób wyjaśniać wszystkie scenariusze i warunki wstępne, w których FRT będzie wykorzystywana.
- Przeszkolić użytkowników końcowych, jak korzystać z tej technologii. Takie szkolenia muszą wyjaśniać możliwości i ograniczenia technologii, aby użytkownicy mogli zrozumieć okoliczności, w których konieczne jest jej zastosowanie oraz przypadki, w których może być ona niedokładna. Takie szkolenia pomogą również ograniczyć ryzyko związane z brakiem kontrolowania lub krytycznej oceny wyników algorytmu.
- Konsultować się z organem nadzorczym ds. ochrony danych zgodnie z art. 28 ust. 1 lit. b) dyrektywy o ochronie danych osobowych w sprawach karnych. Przekazać informacje zgodnie z art. 13 dyrektywy o ochronie danych w sprawach karnych w celu poinformowania osób, których dane dotyczą, o przetwarzaniu i przysługujących im prawach. Powiadomienia te należy skierować do osób, których dane dotyczą, w odpowiednim języku, tak aby mogły one zrozumieć proces przetwarzania danych. Ponadto w powiadomieniach należy objaśnić podstawowe elementy technologii, w tym wskaźniki dokładności, szkoleniowe zbiory danych i środki podjęte w celu uniknięcia dyskryminacji i niskiej dokładności algorytmu.

4. ZALECENIA PO WDROŻENIU FRT

- Zapewnić interwencję ludzką i nadzór nad wynikami. Nigdy nie wolno podejmować żadnych działań dotyczących osoby fizycznej wyłącznie w oparciu o wynik FRT (oznaczałoby to naruszenie art. 11 dyrektywy o ochronie danych w sprawach karnych – zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach mające skutki prawne lub inne podobne skutki dla osoby, której dane dotyczą). Należy upewnić się, że organ ścigania dokonał przeglądu wyników FRT. Należy również zapewnić, aby użytkownicy z organów ścigania eliminowali błędy automatyzacji i badali sprzeczne informacje oraz krytycznie podchodzili do wyników technologii. W tym celu ważne jest stałe szkolenie i podnoszenie świadomości użytkowników końcowych, przy czym najwyższe kierownictwo powinno zapewnić odpowiednie zasoby kadrowe do sprawowania skutecznego nadzoru. Wiąże się to z zapewnieniem każdemu z pracowników wystarczającej ilości czasu na podważenie wyników technologii. Należy rejestrować, mierzyć i oceniać, w jakim stopniu ludzki nadzór zmienia pierwotną decyzję FRT.
- Monitorować i reagować na odchylenia modelu FRT (spadek wydajności), gdy model jest już w fazie produkcyjnej.
- Ustanowić regularny proces ponownej oceny ryzyka i środków bezpieczeństwa w każdym przypadku, gdy technologia lub przypadek użycia ulegnie zmianie.
- Dokumentować wszelkie zmiany w systemie w całym jego cyklu życia (np. aktualizacje, ponowne szkolenia).
- Ustanowić proces oraz związane z nim możliwości techniczne w celu odpowiadania na wnioski o dostęp składane przez osoby, których dane dotyczą. Zanim pojawi się jakikolwiek wniosek, należy zapewnić techniczne możliwości pozyskiwania danych, jeśli zajdzie potrzeba ich udostępnienia osobom, których dane dotyczą.
- Zapewnić wdrożenie procedur na wypadek naruszenia ochrony danych. Jeśli dojdzie do naruszenia ochrony danych osobowych, w tym danych biometrycznych, ryzyko może być wysokie. W takim przypadku wszyscy zaangażowani użytkownicy powinni być świadomi odpowiednich procedur, które należy zastosować, inspektor ochrony danych oraz osoby, których dane dotyczą, powinny zostać niezwłocznie poinformowane.

ZAŁĄCZNIK III – PRAKTYCZNE PRZYKŁADY

Istnieje wiele różnych praktycznych ustawień i celów korzystania z technologii rozpoznawania twarzy, np. w kontrolowanych środowiskach, takich jak przejścia graniczne, sprawdzanie krzyżowe z danymi z policyjnych baz danych lub z danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą, transmisje z kamer na żywo (rozpoznawanie twarzy na żywo) itp. W rezultacie zagrożenia dla ochrony danych osobowych i innych podstawowych praw i wolności w różnych przypadkach użycia znacznie się różnią. Aby ułatwić ocenę niezbędności i proporcjonalności, która powinna poprzedzać decyzję o ewentualnym wdrożeniu rozpoznawania twarzy, obecne wytyczne zawierają niewyczerpujący wykaz możliwych zastosowań FRT w dziedzinie ścigania przestępstw.

Przedstawione i ocenione scenariusze opierają się na **hipotetycznych** sytuacjach i mają na celu zilustrowanie pewnych konkretnych zastosowań FRT oraz zapewnienie pomocy w indywidualnych przypadkach, a także ustanowienie ogólnych ram. Nie są one wyczerpujące i pozostają bez uszczerbku dla jakichkolwiek trwających lub przyszłych postępowań podejmowanych przez krajowy organ nadzorczy w odniesieniu do projektowania, eksperymentowania lub wdrażania technologii rozpoznawania twarzy. Przedstawienie tych scenariuszy służy jedynie jako przykład wskazówek dla decydentów, prawodawców i organów ścigania, które zostały przedstawione w niniejszym dokumencie, na potrzeby opracowywania i planowania wdrażania technologii rozpoznawania twarzy w celu zapewnienia pełnej zgodności z dorobkiem prawnym UE w dziedzinie ochrony danych osobowych. W tym kontekście należy pamiętać, że nawet w podobnych sytuacjach związanych ze stosowaniem FRT, występowanie lub brak pewnych elementów może prowadzić do innego wyniku oceny niezbędności i proporcjonalności.

1 SCENARIUSZ 1

1.1. Opis

Zautomatyzowany system kontroli granicznej, który umożliwia zautomatyzowane przekraczanie granicy poprzez uwierzytelnienie obrazu biometrycznego przechowywanego w elektronicznym dokumencie podróży obywateli Unii Europejskiej i innych podróżnych przechodzących przez przejście graniczne oraz ustalenie, że podróżny jest prawnym posiadaczem dokumentu.

Taka weryfikacja/uwierzytelnianie obejmuje tylko rozpoznawanie twarzy „jeden do jednego” w kontrolowanym środowisku (np. na lotniskowych bramkach elektronicznych). Dane biometryczne podróżnego przechodzącego przez przejście graniczne są pobierane, gdy jest on wyraźnie poproszony o spojrzenie w kamerę w bramce elektronicznej i są porównywane z danymi przedstawionego dokumentu (paszportu, dowodu osobistego itp.), który jest wydawany zgodnie z określonymi wymogami technicznymi.

Jednocześnie, chociaż przetwarzanie w takich przypadkach zasadniczo wykracza poza zakres stosowania dyrektywy o ochronie danych w sprawach karnych, wynik weryfikacji może być również wykorzystany do dopasowania (alfanumerycznych) danych osoby z danymi z baz danych organów ścigania w ramach kontroli granicznej, a tym samym może prowadzić do działań o znaczących skutkach prawnych dla osoby, której dane dotyczą, np. zatrzymania na podstawie wpisu w SIS. W szczególnych okolicznościach dane biometryczne mogą być również wykorzystywane do wyszukiwania dopasowań w bazach danych organów ścigania (w takim przypadku na tym etapie zostanie przeprowadzona identyfikacja 1 do wielu).

Wynik przetwarzania wizerunku biometrycznego ma bezpośredni wpływ na osobę, której dane dotyczą: jedynie w przypadku pomyślnej weryfikacji umożliwia przejście przez granicę. W przypadku nieudanej identyfikacji straż graniczna musi przeprowadzić drugą kontrolę, aby upewnić się, że osoba, której dane dotyczą, nie jest osobą przedstawioną w dokumencie identyfikacyjnym.

W przypadku wykrycia wpisu w SIS lub wpisu krajowego funkcjonariusze straży granicznej muszą przeprowadzić drugą weryfikację i niezbędne dalsze kontrole, a następnie podjąć wszelkie niezbędne działania, np. zatrzymać daną osobę, poinformować o tym odpowiednie organy.

Źródło informacji:

- Rodzaje osób, których dane dotyczą:☒ wszystkie osoby fizyczne przekraczające granice
- Źródło wizerunku:☒ inne (dokument tożsamości)
- Związek z przestępczością:☒ nie jest konieczny
- Sposób przechwytywania informacji: ☒ w kabinie lub w kontrolowanym środowisku
- Kontekst – wpływ na inne prawa podstawowe: Tak, a mianowicie: ☒ prawo do swobodnego przemieszczania się ☒ prawo do azylu

Referencyjna baza danych (z którą porównywane są przechwycone informacje):

- Specyfika: ☒ konkretne bazy danych związane z kontrolą granic

Algorytm:

- Rodzaj weryfikacji: ☒ weryfikacja (uwierzytelnianie) 1 do 1

Wyniki:

- Wpływ ☒ bezpośredni (osobie, której dane dotyczą, zezwala się lub odmawia się wstępu)
- Zautomatyzowana decyzja:☒ Tak

1.2. Obowiązująca podstawa prawna

Od 2004 r., zgodnie z rozporządzeniem Rady (WE) nr 2252/2004[85], paszporty i inne dokumenty podróży wydawane przez państwa członkowskie muszą zawierać biometryczny wizerunek twarzy przechowywany w elektronicznym chipie wbudowanym w dokument.

Kodeks graniczny Schengen[86] określa wymogi dotyczące odpraw granicznych osób na granicach zewnętrznych. W przypadku obywateli Unii Europejskiej i innych osób korzystających z prawa do swobodnego przemieszczania się na mocy prawa Unii minimalne kontrole powinny polegać na weryfikacji ich dokumentów podróży, w stosownych przypadkach z wykorzystaniem urządzeń technicznych. Kodeks graniczny Schengen został następnie zmieniony rozporządzeniem (UE) 2017/2225[87], w którym wprowadzono między innymi definicje „bramek elektronicznych", „systemu zautomatyzowanej kontroli granicznej" i „systemu samoobsługi", a także możliwość przetwarzania danych biometrycznych na potrzeby dokonywania odprawy granicznej.

W związku z tym można założyć, że istnieje jasna i przewidywalna podstawa prawna zezwalająca na taką formę przetwarzania danych osobowych. Ponadto ramy prawne są przyjmowane na poziomie Unii i mają bezpośrednie zastosowanie do państw członkowskich.

[85] ROZPORZĄDZENIE RADY (WE) NR 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie.

[86] ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen).

[87] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2225 z dnia 30 listopada 2017 r. zmieniające rozporządzenie (UE) 2016/399 w zakresie korzystania z systemu wjazdu/wyjazdu.

1.3. Niezbędność i proporcjonalność – cel/waga przestępstwa

Weryfikacja tożsamości obywateli Unii Europejskiej w ramach zautomatyzowanej kontroli granicznej, z wykorzystaniem ich wizerunku biometrycznego, jest elementem odprawy granicznej na zewnętrznych granicach UE. W związku z tym jest ona bezpośrednio związana z bezpieczeństwem granic i służy celowi leżącemu w interesie ogólnym i uznanemu przez Unię. Ponadto bramki ABC przyczyniają się do przyspieszenia obsługi pasażerów i zmniejszenia ryzyka wystąpienia błędów ludzkich. Ponadto zakres, zasięg i intensywność zakłóceń w tym scenariuszu są znacznie bardziej ograniczone w porównaniu z innymi formami rozpoznawania twarzy. Niemniej jednak przetwarzanie danych biometrycznych stwarza dodatkowe ryzyko dla osób, których dane dotyczą, które właściwy organ wdrażający i obsługujący FRT musi odpowiednio uwzględnić i ograniczyć.

1.4. Wniosek

Weryfikacja tożsamości obywateli Unii Europejskiej w kontekście zautomatyzowanej kontroli granicznej jest środkiem niezbędnym i proporcjonalnym, o ile stosowane są odpowiednie zabezpieczenia, w szczególności zasady ograniczenia celu, jakości danych, przejrzystości i wysokiego poziomu bezpieczeństwa.

2 SCENARIUSZ 2

2.1. Opis

Organy ścigania ustalają system identyfikacji ofiar uprowadzeń dzieci. Upoważniony funkcjonariusz policji może przeprowadzić porównanie danych biometrycznych dziecka, co do którego istnieje podejrzenie, że zostało uprowadzone, z bazą danych ofiar uprowadzeń dzieci na ściśle określonych warunkach, wyłącznie w celu zidentyfikowania nieletnich, którzy mogą odpowiadać opisowi zaginionego dziecka, w sprawie którego wszczęto dochodzenie i wydano ostrzeżenie.

Przetwarzanie, o którym mowa, polegałoby na porównaniu twarzy lub wizerunku osoby, która może odpowiadać opisowi zaginionego dziecka, z wizerunkami przechowywanymi w bazie danych. Takie przetwarzanie odbywałoby się w określonych przypadkach, nie zaś w sposób systematyczny.

Baza danych, z którą zostanie przeprowadzone porównanie, zawiera zdjęcia zaginionych dzieci, w odniesieniu do których zgłoszono podejrzenie uprowadzenia dziecka, zagrożenie życia lub integralności fizycznej dziecka i wszczęto postępowanie przygotowawcze pod nadzorem organu sądowego oraz w odniesieniu do których wydano ostrzeżenie o uprowadzeniu dziecka. Dane są gromadzone w ramach procedur ustanowionych przez właściwy organ ścigania, tj. przez funkcjonariuszy policji upoważnionych do wykonywania zadań policji sądowej. Kategorie rejestrowanych danych osobowych są następujące:

- tożsamość, przydomek, pseudonim, pokrewieństwo, obywatelstwo, adresy, adresy e-mail, numery telefonów;
- data i miejsce urodzenia;
- informacje o pochodzeniu dziecka;
- fotografia o cechach technicznych umożliwiających wykorzystanie urządzenia do rozpoznawania twarzy i inne fotografie.

Wyniki porównania muszą również zostać sprawdzone i zweryfikowane przez upoważnionego funkcjonariusza, celem potwierdzenia wcześniejszych dowodów z wynikami porównania i wykluczenia ewentualnych wyników fałszywie dodatnich.

Zdjęcia i dane osobowe dzieci mogą być przechowywane wyłącznie przez czas trwania ostrzeżenia i muszą zostać usunięte natychmiast po zamknięciu lub zakończeniu postępowania karnego zgodnie z procedurami krajowymi, w związku z którymi zostały wprowadzone do bazy danych.

O ile okres przechowywania danych biometrycznych w bazie danych może być stosunkowo długi i określony zgodnie z prawem krajowym, korzystanie z praw osób, których dane dotyczą, a w szczególności prawa do sprostowania i usunięcia danych, stanowi dodatkową gwarancję ograniczenia ingerencji w prawo do ochrony danych osobowych osób, których dane dotyczą.

Źródło informacji:

- Rodzaje osób, których dane dotyczą: ☒ dzieci
- Źródło obrazu ☒ inne: nieokreślone z góry, podejrzana ofiara uprowadzenia dziecka
- Związek z przestępczością ☒ brak bezpośredniego związku czasowego ☒ brak bezpośredniego związku geograficznego
- Sposób przechwytywania informacji: ☒ w kabinie lub w kontrolowanym środowisku
- Kontekst: wpływa na inne prawa podstawowe ☒ Tak, a mianowicie: ☒ różne

Referencyjna baza danych (z którą porównywane są przechwycone informacje):

- Specyfika ☒ konkretna baza danych

Algorytm:

- Rodzaj weryfikacji :☒ identyfikacja 1 do wielu

Wyniki:

- Wpływ ☒ bezpośredni
- Zautomatyzowana decyzja: ☒ NIE, obowiązkowy przegląd przez upoważnionego funkcjonariusza

Analiza prawna:

- Obowiązujące ramy prawne: ☒ szczególne przepisy prawa krajowego dotyczące tego przetwarzania (rozpoznawanie twarzy)

2.2. Obowiązująca podstawa prawna

Prawo krajowe przewiduje specjalne ramy prawne ustanawiające bazę danych, określające cele przetwarzania, a także kryteria uzupełniania bazy danych, dostępu do niej i korzystania z niej. Akty prawne niezbędne do jej wdrożenia przewidują również określenie okresu przechowywania, a także odnoszą się do obowiązujących zasad integralności i poufności. Akty prawne przewidują również sposoby przekazywania informacji osobie, której dane dotyczą, a w tym przypadku dysponentowi (dysponentom) władzy rodzicielskiej, a także wykonywanie praw osoby, której dane dotyczą i w stosownych przypadkach ewentualne ich ograniczenie. Podczas przygotowywania wniosku dotyczącego odpowiedniego aktu prawnego należało skonsultować się z krajowym organem nadzorczym.

2.3. Niezbędność i proporcjonalność – cel / waga przestępstwa / liczba osób niezaangażowanych, ale na które przetwarzanie danych ma wpływ

Warunki i zabezpieczenia przetwarzania

Funkcjonariusz może porównać wizerunek twarzy tylko w ostateczności, gdy nie ma innych mniej inwazyjnych środków i gdy jest to bezwzględnie niezbędne, na przykład w przypadku wątpliwości co

do autentyczności dokumentu tożsamości podróżującego małoletniego lub po dokonaniu weryfikacji wcześniejszych dowodów i zebranych materiałów wskazujących na możliwą zgodność z opisem zaginionego dziecka, w sprawie którego prowadzone jest postępowanie przygotowawcze.

Dodatkowym zabezpieczeniem jest również obowiązkowy przegląd i weryfikacja wyników porównania rozpoznawania twarzy przez upoważnionego funkcjonariusza, celem potwierdzenia wcześniejszych dowodów z wynikami porównania i wykluczenia ewentualnych wyników fałszywie dodatnich.

Zamierzony cel

Utworzenie bazy danych służy ważnym celom leżącym w ogólnym interesie publicznym, w szczególności zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych i wykonywaniu kar oraz ochronie praw i wolności innych osób. Utworzenie bazy danych i przewidziane przetwarzanie danych może przyczynić się do identyfikacji dzieci będących ofiarami uprowadzenia, a zatem może być uznane za środek odpowiedni do realizacji uzasadnionego celu, jakim jest prowadzenie dochodzeń w sprawie takich przestępstw i ich ściganie.

Cel i uzupełnienie bazy danych

Cele przetwarzania są jasno określone przez prawo, a baza danych jest wykorzystywana wyłącznie w celu identyfikacji zaginionych dzieci, w odniesieniu do których zgłoszono podejrzenie uprowadzenia dziecka i wszczęto postępowanie przygotowawcze pod nadzorem organu sądowego oraz w odniesieniu do których wydano ostrzeżenie o uprowadzeniu dziecka. Warunki określone przez prawo dotyczące uzupełniania bazy danych mają na celu ścisłe ograniczenie liczby osób, których dane dotyczą i danych osobowych, które mają być zawarte w bazie danych. Osoba posiadająca odpowiedzialność rodzicielską za dziecko musi zostać poinformowana o przetwarzaniu i warunkach wykonywania praw dziecka w odniesieniu do przetwarzania biometrycznego przewidzianego do celów identyfikacji lub do danych osobowych dziecka przechowywanych w bazie danych.

2.4. Wniosek

Biorąc pod uwagę niezbędność i proporcjonalność planowanego przetwarzania, a także najlepszy interes dziecka w przeprowadzaniu takiego przetwarzania danych osobowych oraz pod warunkiem, że istnieją wystarczające gwarancje, aby w szczególności zapewnić korzystanie z praw osób, których dane dotyczą – w szczególności biorąc pod uwagę fakt, że mają być przetwarzane dane dzieci, takie zastosowanie przetwarzania rozpoznawania twarzy można uznać za prawdopodobnie zgodne z prawem UE.

Ponadto biorąc pod uwagę rodzaj przetwarzania i zastosowaną technologię, która wiąże się z wysokim ryzykiem dla praw i wolności osób, których dane dotyczą, EROD uważa, że przygotowanie wniosku dotyczącego aktu prawnego, który ma zostać przyjęty przez parlament narodowy, lub aktu regulacyjnego opartego na takim akcie prawnym, który odnosi się do planowanego przetwarzania, musi obejmować uprzednie konsultacje z organem nadzorczym w celu zapewnienia spójności i zgodności z obowiązującymi ramami prawnymi, por. art. 28 ust. 2 dyrektywy o ochronie danych w sprawach karnych.

3 SCENARIUSZ 3

3.1. Opis

W trakcie interwencji policji podczas zamieszek i późniejszych dochodzeń wiele osób zidentyfikowano jako podejrzanych, np. w wyniku wcześniejszych dochodzeń z wykorzystaniem nagrań z systemu CCTV

lub zeznań świadków. Zdjęcia tych podejrzanych porównuje się ze zdjęciami osób, które zarejestrowano w systemie CCTV lub na urządzeniach mobilnych na miejscu przestępstwa lub w jego okolicy.

W celu uzyskania bardziej szczegółowych dowodów dotyczących osób podejrzanych o udział w zamieszkach towarzyszących demonstracji, policja tworzy bazę danych składającą się z materiałów zdjęciowych luźno powiązanych pod względem miejsca i czasu z zamieszkami. Baza danych zawiera prywatne nagrania przesłane policji przez obywateli, materiały z systemów CCTV transportu publicznego, materiały z nadzoru wideo należące do policji oraz materiały opublikowane przez media bez żadnych konkretnych ograniczeń lub zabezpieczeń. Wykazanie poważnych zachowań przestępczych nie jest warunkiem koniecznym do gromadzenia plików w bazie danych. W związku z tym w bazie danych zapisywane są osoby niezaangażowane w zamieszki – duży odsetek miejscowej ludności, która przypadkowo przechodziła obok w momencie demonstracji lub uczestniczyła w demonstracji, ale nie w zamieszkach. Baza zawiera tysiące plików wideo i obrazów.

Za pomocą oprogramowania do rozpoznawania twarzy wszystkie twarze pojawiające się w tych plikach są przypisywane do niepowtarzalnych identyfikatorów twarzy. Twarze poszczególnych podejrzanych są następnie automatycznie porównywane z tymi identyfikatorami. Baza danych składająca się ze wszystkich wzorców biometrycznych w tysiącach plików wideo i zdjęć jest przechowywana do czasu zakończenia wszystkich możliwych dochodzeń. Odpowiedzialni funkcjonariusze analizują dopasowania pozytywne, a następnie podejmują decyzję o dalszych działaniach. Działania te mogą obejmować przypisanie pliku znalezionego w bazie danych do akt karnych określonej osoby, a także dalsze czynności, takie jak przesłuchanie tej osoby lub jej zatrzymanie.

Prawo krajowe przewiduje ogólny przepis, zgodnie z którym przetwarzanie danych biometrycznych w celu jednoznacznej identyfikacji osoby fizycznej jest dopuszczalne, jeżeli jest to bezwzględnie niezbędne i podlega odpowiednim zabezpieczeniom praw i wolności danej osoby.

Źródło informacji:

- Rodzaje osób, których dane dotyczą: ☒ wszystkie osoby
- Źródło obrazu: ☒ przestrzeń publiczna ☒ podmiot prywatny ☒ inne osoby ☒ inne: media
- Związek z przestępczością: ☒ niekoniecznie bezpośredni związek geograficzny lub czasowy
- Sposób przechwytywania informacji: ☒ zdalnie
- Kontekst – wpływ na inne prawa podstawowe: Tak, a mianowicie ☒ kontekst wolności zgromadzeń
- Możliwości uzyskania dodatkowych źródeł informacji na temat osoby, której dane dotyczą: ☒ inne: niewykluczone (takie jak korzystanie z bankomatów lub sklepów), ze względu na brak kontroli motywów na zdjęciach.

Referencyjna baza danych (z którą porównywane są przechwycone informacje):

- Specyfika: ☒ konkretne bazy danych związane z obszarem przestępczości

Algorytm:

- Rodzaj przetwarzania:☒ identyfikacja 1 do wielu

Wyniki:

- Wpływ: ☒ bezpośredni (np. osoba, której dane dotyczą, może zostać zatrzymana, przesłuchana)
- Zautomatyzowana decyzja: ☒ NIE
- Okres przechowywania: do czasu zakończenia wszystkich możliwych dochodzeń

Analiza prawna:

- Rodzaj wcześniejszych informacji przekazanych osobie, której dane dotyczą: ☒ informacje ogólne na stronie internetowej organu ścigania
- Obowiązujące ramy prawne: ☒ dyrektywa o ochronie danych w sprawach karnych w większości skopiowana do prawa krajowego ☒ Ogólne prawo krajowe dotyczące wykorzystywania danych biometrycznych przez organy ścigania

3.2. Obowiązująca podstawa prawna

Jak wyjaśniono powyżej, podstawy prawne jedynie powtarzające klauzulę ogólną art. 10 dyrektywy o ochronie danych osobowych w sprawach karnych nie są wystarczająco jasne, aby zapewnić osobom fizycznym odpowiednie wskazanie warunków i okoliczności, w których organy ścigania są uprawnione do korzystania z nagrań CCTV z przestrzeni publicznej w celu stworzenia biometrycznego wzorca ich twarzy i porównania go z policyjnymi bazami danych, innymi dostępnymi nagraniami CCTV lub prywatnymi itp. Ramy prawne ustanowione w tym scenariuszu nie spełniają zatem minimalnych wymogów, aby służyć jako podstawa prawna.

3.3. Niezbędność i proporcjonalność

W tym przykładzie przetwarzanie danych budzi różne obawy w świetle zasad niezbędności i proporcjonalności z kilku powodów:

Osoby nie są podejrzane o popełnienie poważnego przestępstwa. Wykazanie poważnego zachowania przestępczego nie jest warunkiem koniecznym do korzystania z plików w bazie danych zawierających materiały wizerunkowe. Ponadto bezpośredni związek czasowy i geograficzny z przestępstwem nie jest warunkiem koniecznym do wykorzystania plików z bazy danych. W rezultacie w bazie danych biometrycznych przechowywany będzie znaczny odsetek lokalnej populacji potencjalnie przez kilka lat, aż do zakończenia wszystkich dochodzeń.

Baza danych miejsc zbrodni nie zawiera wyłącznie obrazów spełniających wymogi proporcjonalności, co skutkuje nieograniczoną liczbą obrazów do porównania. Jest to sprzeczne z zasadą minimalizacji danych. Mniejsza liczba obrazów umożliwiłaby również zastosowanie niealgorytmicznych i mniej inwazyjnych środków, np. korzystanie z usług tzw. superrozpoznawacza (ang. super recognizer)[88].

Ponieważ przykład dotyczy okoliczności protestu, prawdopodobne jest również, że obrazy ujawniają poglądy polityczne uczestników demonstracji, co stanowi drugą szczególną kategorię danych, których może dotyczyć ten scenariusz. W tym scenariuszu nie jest jasne, w jaki sposób można zapobiec gromadzeniu tych danych i przy użyciu jakich zabezpieczeń. Ponadto, gdy osoby, których dane dotyczą, dowiedzą się, że z powodu udziału w demonstracji wpisano ich do policyjnej bazy danych biometrycznych, może to mieć poważny „efekt mrożący" w odniesieniu do ich przyszłego korzystania z prawa do zgromadzeń.

Wzorce biometryczne w bazie danych mogą być również porównywane między sobą. Dzięki temu policja może nie tylko wyszukać konkretną osobę we wszystkich materiałach, ale także odtworzyć

[88] Tj. osoby o nadzwyczajnej zdolności rozpoznawania twarzy. Porównaj również: Face Recognition by Metropolitan Police Super-Recognisers [Rozpoznawanie twarzy przez super-rozpoznawaczy policji metropolitalnej], 26 lutego 2016 r., DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

wzorzec zachowania danej osoby na przestrzeni kilku dni. Może również gromadzić dodatkowe informacje o osobach, takie jak ich kontakty społeczne i aktywność polityczna.

Fakt, że dane są przetwarzane bez wiedzy osób, których dane dotyczą, dodatkowo zwiększa ingerencję.

Mając na uwadze, że ludzie nieustannie robią zdjęcia i nagrywają filmy, a także to, że nawet materiał pochodzący z wszechobecnego monitoringu CCTV można analizować pod względem danych biometrycznych, wzrasta ryzyko powstania poważnych „efektów mrożących".

Kolejnym powodem do niepokoju jest szerokie wykorzystanie prywatnych zdjęć i filmów, w tym potencjalne nadużycia, takie jak donosicielstwo. Ponieważ nadużycia takie jak donosicielstwo stanowią ryzyko nieodłącznie związane z postępowaniem karnym jako takim, ryzyko to jest znacznie większe ze względu na skalowalność przetwarzanych danych i liczbę zaangażowanych osób, ponieważ ludzie mogą przesyłać również materiały dotyczące konkretnej osoby lub grupy osób, których nie lubią. Żądania policji dotyczące przesyłania fotografii i filmów mogą sprawić, że udostępnianie materiałów stanie się dla ludzi bardzo łatwe, zwłaszcza gdy istnieje możliwość zrobienia tego anonimowo lub przynajmniej bez konieczności osobistego stawiania się i identyfikacji na komisariacie policji.

3.4. Wniosek

W przykładzie nie ma konkretnego przepisu, który mógłby służyć za podstawę prawną. Jednak nawet gdyby istniała wystarczająca podstawa prawna, wymogi niezbędności i proporcjonalności nie zostałyby spełnione, co skutkowałoby nieproporcjonalną ingerencją w prawa osoby, której dane dotyczą, do poszanowania życia prywatnego i ochrony danych osobowych na mocy Karty.

4 SCENARIUSZ 4

4.1. Opis

Policja wdraża sposób identyfikacji podejrzanych o popełnienie poważnego przestępstwa uchwyconego na nagraniu CCTV przy wykorzystaniu technologii FRT używanej retrospektywnie. Funkcjonariusz ręcznie wybiera obraz (lub obrazy) podejrzanych w materiale wideo, który zebrano z miejsca przestępstwa lub innego miejsca w ramach postępowania przygotowawczego, a następnie wysyła obraz (lub obrazy) do wydziału kryminalistycznego. Wydział kryminalistyczny wykorzystuje FRT do dopasowania tych obrazów do zdjęć osób, które zostały wcześniej zgromadzone w bazie danych przez policję (tak zwana baza danych identyfikacyjnych, która składa się z podejrzanych i byłych skazanych). Baza danych identyfikacyjnych jest dla tej procedury – tymczasowo i w odizolowanym środowisku – analizowana za pomocą FRT, aby umożliwić proces dopasowywania. Aby zminimalizować ingerencję w prawa i interesy dopasowanych osób, bardzo ograniczona liczba pracowników wydziału kryminalistycznego ma pozwolenie na przeprowadzenie faktycznej procedury dopasowania, dostęp do danych jest ograniczony do tych funkcjonariuszy, którym powierzono konkretne akta, a przed przekazaniem jakichkolwiek wyników funkcjonariuszowi prowadzącemu dochodzenie przeprowadzana jest ręczna kontrola wyników. Dane biometryczne nie są przekazywane poza kontrolowane, odizolowane środowisko. W dalszej części dochodzenia wykorzystuje się wyłącznie wynik i zdjęcie (a nie wzorzec biometryczny). Pracownicy przechodzą specjalne szkolenie w zakresie zasad i procedur tego przetwarzania, a wszystkie czynności przetwarzania danych osobowych i biometrycznych są w wystarczającym stopniu określone w prawie krajowym.

Źródło informacji:

- Rodzaje osób, których dane dotyczą: ☒ osoby podejrzane zidentyfikowane na podstawie nagrań CCTV
- Źródło obrazu:☒ przestrzeń publiczna ☒ internet
- Związek z przestępczością: ☒ bezpośredni związek czasowy
  ☒ bezpośredni związek geograficzny
- Sposób przechwytywania informacji: ☒ zdalnie
- Kontekst – wpływ na inne prawa podstawowe: Tak, a mianowicie: ☒ wolność zgromadzeń ☒ wolność słowa ☒ różne: __

Referencyjna baza danych (z którą porównywane są przechwycone informacje):

- Specyfika: ☒ konkretne bazy danych związane z obszarem przestępczości

Algorytm:

- Rodzaj przetwarzania:☒ identyfikacja 1 do wielu

Wyniki:

- Wpływ:☒ bezpośredni (np. osoba, której dane dotyczą, jest zatrzymana lub przesłuchiwana)
- Zautomatyzowana decyzja: ☒ NIE

Analiza prawna:

- Obowiązujące ramy prawne: ☒ szczególne przepisy prawa krajowego dotyczące tego przetwarzania (rozpoznawanie twarzy) przez właściwy organ

4.2. Obowiązująca podstawa prawna

W tym scenariuszu w prawie krajowym określono, że dane biometryczne można wykorzystywać do przeprowadzania analizy kryminalistycznej, jeżeli jest to absolutnie niezbędne do osiągnięcia celu polegającego na zidentyfikowaniu osób podejrzanych o popełnienie poważnego przestępstwa poprzez dopasowanie obrazów w bazie danych identyfikacyjnych. Zgodnie z prawem krajowym określono, które dane mogą być przetwarzane, a także procedury zachowania integralności i poufności danych osobowych oraz procedury ich niszczenia, zapewniając w ten sposób wystarczające zabezpieczenia przed ryzykiem nadużycia i arbitralności.

4.3. Niezbędność i proporcjonalność

Na poziomie kryminalistycznym korzystanie z rozpoznawania twarzy jest zdecydowanie bardziej efektywne czasowo niż ręczne dopasowywanie. Wcześniejsza ręczna selekcja obrazów ogranicza zakłócenia w porównaniu z przeglądaniem całego materiału wideo w bazie danych, a tym samym pozwala odróżnić i namierzyć tylko osoby objęte celem, którym jest zwalczanie poważnych przestępstw. Niemniej jednak nadal ważne jest, aby sprawdzić, czy dopasowanie można wykonać ręcznie w rozsądnym czasie, w zależności od danego przypadku. Ograniczenie osób mających dostęp do technologii i danych osobowych zmniejsza ich wpływ na prawo do prywatności i ochrony danych, a także sprawia, że wzorce biometryczne nie są przechowywane ani wykorzystywane na późniejszym etapie dochodzenia. Ręczna kontrola wyniku oznacza również ograniczone ryzyko wystąpienia fałszywie dodatnich wyników.

4.4. Wniosek

Ważne jest, aby przepisy krajowe zapewniały odpowiednią podstawę prawną dla przetwarzania danych biometrycznych, a także podstawę prawną dla prowadzenia krajowej bazy danych wykorzystywanej do dopasowywania danych. W tym scenariuszu wprowadzono kilka środków w celu

ograniczenia ingerencji w prawa do ochrony danych, takich jak warunki korzystania z FRT określone w podstawie prawnej, liczba osób mających dostęp do technologii i danych biometrycznych, kontrole ręczne itp. FRT znacznie poprawia wydajność pracy dochodzeniowej wydziału kryminalistycznego policji, opiera się na prawie umożliwiającym policji przetwarzanie danych biometrycznych, gdy jest to absolutnie konieczne, a zatem w tych granicach można uznać za zgodną z prawem ingerencję w prawa jednostki.

5 SCENARIUSZ 5

5.1. Opis

Zdalna identyfikacja biometryczna to proces, w ramach którego tożsamość wielu osób jest ustalana z pomocą identyfikatorów biometrycznych (wizerunku twarzy, sposobu chodzenia, tęczówek itp.) na odległość, w przestrzeni publicznej oraz w sposób ciągły lub trwały, poprzez porównywanie z danymi (biometrycznymi) przechowywanymi w bazie danych[89]. Zdalną identyfikację biometryczną przeprowadza się w czasie rzeczywistym, jeśli przechwycenie materiału obrazu, porównanie i identyfikacja odbywają się bez znaczącego opóźnienia.

Przed każdym wdrożeniem zdalnej identyfikacji biometrycznej w czasie rzeczywistym policja sporządza listę obserwacyjną osób będących przedmiotem zainteresowania w ramach dochodzenia. Zawiera wizerunki twarzy poszczególnych osób. W oparciu o dane wywiadowcze sugerujące, że określone osoby będą przebywać w określonym obszarze, takim jak centrum handlowe lub plac publiczny, policja decyduje, kiedy, gdzie i na jak długo wdrożyć zdalną identyfikację biometryczną.

W dniu akcji umieszczają na miejscu samochód policyjny jako centrum kontroli, z wyższym rangą funkcjonariuszem policji na pokładzie. W samochodzie znajdują się monitory wyświetlające nagrania z kamer CCTV umieszczonych w pobliżu, zainstalowanych doraźnie lub podłączonych do transmisji wideo z kamer już zainstalowanych. Gdy piesi przechodzą obok kamer, technologia izoluje obrazy twarzy, konwertuje je na wzorzec biometryczny i porównuje je z wzorcami biometrycznymi osób znajdujących się na liście obserwowanych.

Jeśli wykryte zostanie potencjalne dopasowanie między osobą z listy obserwacyjnej a osobą przechodzącą przed kamerami, do funkcjonariuszy w furgonetce wysyłane jest powiadomienie, a następnie informują oni funkcjonariuszy na miejscu, jeśli wynik jest pozytywny, np. za pośrednictwem urządzenia radiowego. Funkcjonariusz w terenie podejmie wówczas decyzję, czy interweniować, zbliżyć się, czy ostatecznie zatrzymać określoną osobę. Działania podjęte przez funkcjonariusza w terenie są rejestrowane. W przypadku niejawnej kontroli, przechowywane są zebrane informacje (takie jak to, z kim dana osoba przebywa, w co jest ubrana i dokąd zmierza).

Prawo krajowe przewiduje ogólny przepis, zgodnie z którym przetwarzanie danych biometrycznych w celu jednoznacznej identyfikacji osoby fizycznej jest dopuszczalne, jeżeli jest to bezwzględnie niezbędne i podlega odpowiednim zabezpieczeniom praw i wolności określonej osoby.

Źródło informacji:

- Rodzaje osób, których dane dotyczą: ☒ wszystkie osoby
- Źródło obrazu: ☒ przestrzeń publiczna
- Związek z przestępczością: ☒ niekoniecznie bezpośredni związek geograficzny lub czasowy
- Sposób przechwytywania informacji: ☒ zdalnie

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

- Kontekst – wpływ na inne prawa podstawowe: Tak, a mianowicie: ☒ wolność zgromadzeń ☒ wolność słowa ☒ różne
- Możliwości uzyskania dodatkowych źródeł informacji na temat osoby, której dane dotyczą: ☒ inne: niewykluczone (np. korzystanie z bankomatów lub sklepów)

Referencyjna baza danych (z którą porównywane są przechwycone informacje):

- Specyfika: ☒ konkretne bazy danych związane z obszarem przestępczości

Algorytm:

- Rodzaj przetwarzania:☒ identyfikacja 1 do wielu

Wyniki:

- Wpływ:☒ bezpośredni (np. osoba, której dane dotyczą, jest zatrzymana lub przesłuchiwana)
- Zautomatyzowana decyzja: ☒ NIE
- Okres przechowywania: do czasu zakończenia wszystkich możliwych dochodzeń

Analiza prawna:

- Rodzaj wcześniejszych informacji przekazanych osobie, której dane dotyczą: ☒ informacje ogólne na stronie internetowej organu ścigania
- Obowiązujące ramy prawne: ☒ dyrektywa o ochronie danych w sprawach karnych w większości skopiowana do prawa krajowego ☒ Ogólne prawo krajowe dotyczące wykorzystywania danych biometrycznych przez organy ścigania

5.2. Obowiązująca podstawa prawna

Podstawy prawne jedynie powtarzające klauzulę ogólną art. 10 dyrektywy o ochronie danych osobowych w sprawach karnych nie są wystarczająco jasne, aby zapewnić osobom fizycznym odpowiednie wskazanie warunków i okoliczności, w których organy ścigania są uprawnione do korzystania z nagrań CCTV z przestrzeni publicznej w celu stworzenia biometrycznego wzorca ich twarzy i porównania go z policyjnymi bazami danych. Ramy prawne ustanowione w tym scenariuszu nie spełniają zatem minimalnych wymogów, aby służyć jako podstawa prawna[90].

5.3. Niezbędność i proporcjonalność

Wymóg niezbędności i proporcjonalności staje się tym wyższy, im głębsza jest ingerencja. Zdalna identyfikacja biometryczna w przestrzeni publicznej niesie ze sobą szereg konsekwencji w zakresie praw podstawowych:

Scenariusze obejmują monitorowanie każdego przechodnia w danej przestrzeni publicznej. Tym samym poważnie wpływa to na uzasadnione oczekiwania społeczeństwa w zakresie anonimowości w przestrzeni publicznej[91]. Jest to warunek wstępny dla wielu aspektów procesu demokratycznego, takich jak decyzja o dołączeniu do stowarzyszenia obywatelskiego, odwiedzanie zgromadzeń i spotykanie się z ludźmi ze wszystkich środowisk społecznych i kulturowych, udział w protestach politycznych i odwiedzanie wszelkiego rodzaju miejsc. Pojęcie anonimowości w przestrzeni publicznej

[90] W przypadkach, w których projekt naukowy mający na celu badanie wykorzystania FRT wymagałby przetwarzania danych osobowych, ale takie przetwarzanie nie podlegałoby art. 4 ust. 3 dyrektywy o ochronie danych w sprawach karnych lub nie wchodziłoby w zakres prawa Unii, zastosowanie miałoby RODO. Dyrektywa o ochronie danych w sprawach karnych nadal miałaby zastosowanie w przypadku projektów pilotażowych, po których nastąpiłyby działania organów ścigania.

[91] Odpowiedź EROD do posłów do Parlamentu Europejskiego dotycząca aplikacji do rozpoznawania twarzy opracowanej przez Clearview AI, 10 czerwca 2020 r., nr ref.: OUT2020-0052.

jest niezbędne do swobodnego gromadzenia i wymiany informacji i pomysłów. Gwarantuje pluralizm opinii, wolność pokojowych zgromadzeń i wolność zrzeszania się oraz ochronę mniejszości, a także wspiera zasady podziału władzy oraz mechanizmy kontroli i równowagi. Naruszenie zasady anonimowości w przestrzeni publicznej może wywołać poważny „efekt mrożący" dla obywateli. Mogą oni powstrzymywać się od pewnych zachowań, które mieszczą się w ramach wolnego i otwartego społeczeństwa. Miałoby to wpływ na interes publiczny, ponieważ demokratyczne społeczeństwo wymaga samostanowienia i udziału swoich obywateli w procesie demokratycznym.

Jeśli taka technologia zostanie zastosowana, zwykły spacer po ulicy, do metra lub do piekarni w obszarze objętym jej działaniem doprowadzi do gromadzenia danych osobowych, w tym danych biometrycznych, przez organy ścigania, a także, zgodnie z pierwszym scenariuszem, do porównywania z policyjnymi bazami danych. Sytuacja, w której tego samego dokonano by poprzez pobranie odcisków palców, byłaby w oczywisty sposób nieproporcjonalna.

Liczba osób, których dane dotyczą, jest niezwykle wysoka, ponieważ dotyczy to każdego, kto przechodzi przez daną przestrzeń publiczną. Ponadto scenariusze zakładałyby zautomatyzowane masowe przetwarzanie danych biometrycznych, a także masowe porównywanie danych biometrycznych z policyjnymi bazami danych.

W całym orzecznictwie europejskim masowa inwigilacja jest zabroniona (np. ETPC w sprawie S. i Marper przeciwko Zjednoczonemu Królestwu uznał, że masowe zatrzymywanie danych biometrycznych stanowi „nieproporcjonalną ingerencję" w prawo do prywatności, gdyż nie jest ono uważane za „konieczne w demokratycznym społeczeństwie").

Zdalna identyfikacja biometryczna jest tak skłonna do poddawania ludzi masowej inwigilacji, że nie istnieją niezawodne sposoby jej ograniczenia. Zasadniczo różni się od nadzoru wideo jako takiego, ponieważ już samo możliwe wykorzystanie materiału wideo bez identyfikacji biometrycznej jest poważną ingerencją, ale jednocześnie jest ograniczone, podczas gdy w przypadku zastosowania FRT, już szeroko rozpowszechniony system nadzoru wideo jako główne źródło danych ulegnie zmianie jakościowej. Ponadto, zwłaszcza w odniesieniu do sugerowanych „efektów mrożących", ewentualne ograniczenia w stosowaniu już istniejących systemów nadzoru wideo nie będą widoczne, a tym samym nie będą budzić zaufania opinii publicznej.

Zdalna identyfikacja biometryczna przez organy policyjne sprawia, że każdy jest traktowany jako potencjalny podejrzany. Jednak w państwie prawa obywateli uznaje się za niewinnych, dopóki nie zostanie im udowodnione wykroczenie. Zasada ta znajduje również częściowe odzwierciedlenie w dyrektywie o ochronie danych w sprawach karnych, w której podkreślono potrzebę rozróżnienia, w miarę możliwości, między traktowaniem osób skazanych za przestępstwa lub podejrzanych, w stosunku do których organy ścigania muszą mieć „poważne podstawy, by przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony" (art. 6 lit. a) dyrektywy o ochronie danych w sprawach karnych), w porównaniu z osobami, które nie są skazane lub nie są podejrzane o działalność przestępczą.

Technologia ta, zastosowana w węzłowych punktach transportowych lub w przestrzeni publicznej, pozwoli organom ścigania na jednoznaczną identyfikację pojedynczej osoby oraz śledzenie i analizowanie jej miejsca pobytu i przemieszczania się, co pozwoli na ujawnienie nawet najbardziej wrażliwych informacji o określonej osobie (nawet preferencji seksualnych, religii, problemów zdrowotnych). Wiąże się to z ogromnym ryzykiem nieuprawnionego dostępu do danych i ich wykorzystania.

Instalacja systemu, który umożliwia odkrycie istoty zachowania i cech określonej osoby, prowadzi do silnych „efektów mrożących". Sprawia, że ludzie mają wątpliwości, czy przyłączyć się do danej manifestacji, co szkodzi procesowi demokratycznemu. Również spotykanie się i publiczne przebywanie z kimś, o kim wiadomo, że ma problemy z policją lub zachowuje się w nietypowy sposób, może być postrzegane jako krytyczne, ponieważ takie zachowanie może przyciągnąć uwagę algorytmu systemu, a tym samym organów ścigania.

Niemożliwa jest ochrona osób, które są szczególnie podatne na zagrożenia, takich jak dzieci. Co więcej, narażone są osoby, które mają interes zawodowy w zachowaniu poufności swoich kontaktów i często są do tego prawnie zobowiązane, takie jak dziennikarze, prawnicy i duchowni. Może to prowadzić np. do ujawnienia źródła i dziennikarza lub faktu, że dana osoba konsultuje się z obrońcą w sprawach karnych. Problem ten dotyczy nie tylko przypadkowych miejsc publicznych, w których np. spotykają się dziennikarze i ich źródła, ale także miejsc publicznych niezbędnych do zbliżenia się i uzyskania dostępu do instytucji lub specjalistów w tej dziedzinie.

Co więcej, dyskomfort jaki ludzie odczuwają w związku z użytkowaniem FRT może prowadzić do zmiany ich zachowania, unikania miejsc, w których FRT jest wykorzystywana, a tym samym wycofywania się z życia społecznego i wydarzeń kulturalnych. W zależności od zakresu wdrożenia FRT wpływ na ludzi może być na tyle znaczący, aby wpłynąć na ich zdolność do godnego życia[92].

W związku z tym istnieje duże prawdopodobieństwo, że wpłynie to na istotę – nienaruszalny rdzeń – prawa do ochrony danych osobowych. Można wskazać w szczególności następujące mocne przesłanki (por. sekcja 3.1.3.2 wytycznych): unikalne cechy biologiczne ludzi są na dużą skalę automatycznie przetwarzane przez organy ścigania za pomocą algorytmów opartych na wiarygodności, przy czym wyniki można objaśnić tylko w ograniczonym zakresie. Ograniczenia prawa do prywatności i ochrony danych są nakładane niezależnie od indywidualnego zachowania danej osoby lub okoliczności jej dotyczących. Statystycznie rzecz biorąc, większość osób, których dane dotyczą, a na które wpływ ma ta ingerencja, to osoby działające zgodnie z prawem. Istnieją jedynie ograniczone możliwości przekazywania informacji osobie, której dane dotyczą. Odwołanie się do sądu w większości przypadków będzie możliwe dopiero w późniejszym terminie.

Poleganie na systemie opartym na wiarygodności i o ograniczonej możliwości wyjaśnienia może prowadzić do rozproszenia odpowiedzialności oraz braku skutecznych środków naprawczych, co może stanowić zachętę do zaniedbań.

Gdy taki system, który można zastosować również do istniejących kamer CCTV, zostanie wdrożony, przy bardzo niewielkim wysiłku i w sposób niewidoczny dla osób fizycznych, może on zostać niewłaściwie wykorzystany i umożliwić systematyczne i szybkie sporządzanie list osób w podziale na pochodzenie etniczne, płeć, religię itp. Zasada przetwarzania danych osobowych na podstawie wcześniej ustalonych kryteriów, takich jak miejsce pobytu osoby i przebyta trasa, jest już praktykowana[93] i może prowadzić do dyskryminacji.

---

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

[93] Porównaj artykuł 6 Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania oraz art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiającego europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniającego rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226.

W związku z wrażliwością, ekspresyjnością i ilością przetwarzanych danych, systemy zdalnego rozpoznawania twarzy w publicznie dostępnych miejscach mogą być wykorzystywane niezgodnie z przeznaczeniem, ze szkodą dla osób, których dotyczą. Takie dane mogą być również łatwo gromadzone i niewłaściwie wykorzystywane w celu wywierania presji na kluczowe podmioty w ramach mechanizmów kontroli i równowagi, takie jak opozycja polityczna, funkcjonariusze i dziennikarze.

Wreszcie, systemy FRT często wiążą się z wysokim prawdopodobieństwem dyskryminacji ze względu na rasę i płeć: wyniki fałszywie dodatnie w nieproporcjonalny sposób wpływają na osoby należące do mniejszości rasowej i kobiety[94], co prowadzi do dyskryminacji. Działania policji podejmowane po uzyskaniu fałszywie dodatniego wyniku, takie jak przeszukania i zatrzymania, dodatkowo stygmatyzują te grupy.

5.4. Wniosek

Wyżej wymienione scenariusze dotyczące zdalnego przetwarzania danych biometrycznych w przestrzeni publicznej do celów identyfikacji nie zapewniają właściwej równowagi między konkurującymi interesami prywatnymi i publicznymi, a zatem stanowią nieproporcjonalną ingerencję w prawa osoby, której dane dotyczą, wynikające z art. 7 i 8 Karty.

6 SCENARIUSZ 6

6.1. Opis

Prywatny podmiot dostarcza aplikację, w której obrazy twarzy są pobierane z internetu w celu utworzenia bazy danych. Użytkownik, np. policja, może następnie zamieścić zdjęcie i za pomocą identyfikacji biometrycznej aplikacja spróbuje dopasować je do obrazów twarzy lub wzorców biometrycznych w swojej bazie danych.

Lokalna jednostka policji prowadzi dochodzenie w sprawie przestępstwa zarejestrowanego na nagraniu wideo, w którym nie można zidentyfikować wielu potencjalnych świadków i podejrzanych poprzez dopasowanie zebranych informacji do jakichkolwiek wewnętrznych baz danych lub danych wywiadowczych. Osoby fizyczne, na podstawie zebranych informacji, nie są zarejestrowane w żadnej istniejącej bazie danych policji. Policja decyduje się na użycie narzędzia opisanego powyżej, które jest dostarczane przez prywatną firmę, w celu identyfikacji osób za pomocą danych biometrycznych.

Źródło informacji:

- Rodzaje osób, których dane dotyczą: ☒ wszyscy obywatele (świadkowie) ☒ skazani ☒ podejrzani
- Źródło obrazu: ☒ nagranie wideo z miejsca publicznego lub zebrane gdzie indziej dane w ramach postępowania przygotowawczego
- Związek z przestępczością:☒ nie jest konieczny
- Sposób przechwytywania informacji: ☒ zdalnie
- Kontekst – wpływ na inne prawa podstawowe: Tak, a mianowicie: ☒ wolność zgromadzeń ☒ wolność słowa ☒ różne: __

Referencyjna baza danych (z którą porównywane są przechwycone informacje):

- Specyfika: ☒ ogólne bazy danych tworzone na podstawie danych z internetu

Algorytm:

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

- Rodzaj przetwarzania: ☒ identyfikacja 1 do wielu

Wyniki:

- Wpływ ☒ bezpośredni (np. osoba, której dane dotyczą, jest zatrzymana, przesłuchiwana, dyskryminacyjne zachowanie)
- Zautomatyzowana decyzja: ☒ NIE

Analiza prawna:

- Rodzaj informacji przekazanych wcześniej osobie, której dane dotyczą: ☒ Nie

6.2. Obowiązująca podstawa prawna

Gdy podmiot prywatny świadczy usługę obejmującą przetwarzanie danych osobowych, dla której określa cel i środki (w tym przypadku „scraping" obrazów z internetu w celu utworzenia bazy danych), ten podmiot prywatny musi mieć podstawę prawną do takiego przetwarzania. Ponadto organ ścigania, który zdecyduje się na korzystanie z tej usługi do swoich celów, musi mieć podstawę prawną do przetwarzania, dla którego określa cele i środki. Muszą istnieć ramy prawne określające główny cel, dane osobowe, które mają być przetwarzane, cele przetwarzania oraz procedury zachowania integralności i poufności danych osobowych, a także procedury ich niszczenia, aby organ ścigania mógł przetwarzać dane biometryczne.

Scenariusz ten zakłada gromadzenie danych osobowych na masową skalę od osób nieświadomych tego, że ich dane są gromadzone. Takie przetwarzanie mogłoby być zgodne z prawem wyłącznie w bardzo wyjątkowych okolicznościach. W zależności od tego, gdzie znajduje się baza danych, korzystanie z takiej usługi może wiązać się z przekazywaniem danych osobowych lub szczególnych kategorii danych osobowych poza Unię Europejską (np. „wysyłanie" przez policję obrazu twarzy w nagraniu z monitoringu lub zebranego w inny sposób), co wymaga spełnienia szczególnych warunków takiego przekazywania, zob. art. 39 dyrektywy o ochronie danych w sprawach karnych.

W tym scenariuszu nie ma szczegółowych przepisów, które umożliwiałyby takie przetwarzanie przez organ ścigania.

6.3. Niezbędność i proporcjonalność

Korzystanie z usługi przez organ ścigania oznacza, że dane osobowe są udostępniane podmiotowi prywatnemu, który korzysta z bazy danych, w której dane osobowe są gromadzone w sposób nieograniczony i na masową skalę. Nie ma związku między zgromadzonymi danymi osobowymi a zamierzonym celem organu ścigania. Udostępnianie danych przez organ ścigania podmiotowi prywatnemu oznacza również brak kontroli organu nad danymi przetwarzanymi przez podmiot prywatny oraz duże trudności dla osób, których dane dotyczą, w korzystaniu z przysługujących im praw, ponieważ nie będą one świadome, że ich dane są przetwarzane w ten sposób. Oznacza to, że możliwość takiego przetwarzania jest bardzo ograniczona. Wątpliwe jest, czy jakikolwiek cel spełniałby wymogi określone w dyrektywie, ponieważ wszelkie odstępstwa od praw do prywatności i ochrony danych oraz ograniczenia tych praw mają zastosowanie jedynie wtedy, gdy jest to bezwzględnie niezbędne. Ogólny interes skuteczności w zwalczaniu poważnych przestępstw sam w sobie nie może uzasadniać przetwarzania, w sytuacji gdy tak ogromne ilości danych są gromadzone bezkrytycznie. Przetwarzanie to nie spełniałoby zatem wymogów dotyczących niezbędności i proporcjonalności.

6.4. Wniosek

Brak jasnych, precyzyjnych i przewidywalnych zasad spełniających wymogi art. 4 i 10 dyrektywy oraz brak dowodów na to, że przetwarzanie to jest bezwzględnie niezbędne do osiągnięcia zamierzonych

celów, prowadzi do wniosku, że korzystanie z tej aplikacji nie spełniałoby wymogów w zakresie niezbędności i proporcjonalności oraz oznaczałoby nieproporcjonalną ingerencję w prawa osób, których dane dotyczą, do poszanowania życia prywatnego i ochrony danych osobowych na mocy Karty.