28 stycznia 2021 r. T-PD(2020)03rev4

KOMITET KONSULTACYJNY KONWENCJI O OCHRONIE
OSÓB W ZWIĄZKU Z AUTOMATYCZNYM PRZETWARZANIEM
DANYCH OSOBOWYCH

KONWENCJA 108

Wytyczne dotyczące rozpoznawania twarzy

Spis treści

Rozpoznawanie twarzy to automatyczne przetwarzanie obrazów cyfrowych zawierających twarze osób w celu identyfikacji lub weryfikacji tych osób za pomocą szablonów twarzy.

Wrażliwość informacji o charakterze biometrycznym została wyraźnie uznana poprzez włączenie danych jednoznacznie identyfikujących osobę do szczególnych kategorii danych w art. 6 zaktualizowanej Konwencji o ochronie osób w związku z przetwarzaniem danych osobowych[1] (zwanej dalej „Konwencją 108+ ").

Kontekst przetwarzania obrazów ma znaczenie dla określenia wrażliwego charakteru danych, ponieważ nie każde przetwarzanie obrazów wiąże się z przetwarzaniem danych wrażliwych. Obrazy będą objęte definicją danych biometrycznych tylko wtedy, gdy będą przetwarzane za pomocą specjalnego środka technicznego, który pozwala na jednoznaczną identyfikację lub uwierzytelnienie osoby fizycznej[2].

Niniejsze wytyczne dotyczą zastosowań technologii rozpoznawania twarzy, w tym technologii rozpoznawania twarzy na żywo. Zastosowania tej technologii są liczne i zróżnicowane, a niektóre z nich mogą poważnie naruszać prawa osób, których dane dotyczą. Akty prawne zezwalające na szeroki nadzór nad jednostkami mogą być sprzeczne z prawem do poszanowania życia prywatnego[3].

Integracja technologii rozpoznawania twarzy z istniejącymi systemami nadzoru stwarza poważne zagrożenie dla prawa do prywatności i ochrony danych osobowych, a także dla innych praw podstawowych, ponieważ korzystanie z tych technologii nie zawsze wymaga świadomości lub współpracy osób, których dane biometryczne są przetwarzane, biorąc pod uwagę na przykład możliwość dostępu do cyfrowych obrazów osób w Internecie.

Aby zapobiec takim naruszeniom, Strony Konwencji 108+ powinny zapewnić, że rozwój i wykorzystywanie technologii rozpoznawania twarzy będą prowadzone z poszanowaniem prawa do prywatności i ochrony danych, wzmacniając w ten sposób prawa człowieka i podstawowe wolności poprzez wdrażanie zasad zapisanych w Konwencji w specyficznym kontekście technologii rozpoznawania twarzy.

Niniejsze wytyczne[4] zapewniają zestaw środków odniesienia, których rządy, twórcy technologii rozpoznawania twarzy, producenci, usługodawcy i podmioty stosujące technologie rozpoznawania twarzy powinny przestrzegać i je stosować, aby zapewnić, że nie wpływają one niekorzystnie na godność ludzką, prawa człowieka i podstawowe wolności jakiejkolwiek osoby, w tym prawo do ochrony danych osobowych.

Wytyczne mają zakres ogólny i obejmują zastosowania technologii rozpoznawania twarzy w sektorze prywatnym i publicznym. Nie wykluczają, że we właściwych ramach prawnych wymagane będą dalsze

[1] *Protokół zmieniający do Konwencji 108 CETS nr 223*, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

[2] Paragraf 59 Raportu Wyjaśniającego do Konwencji 108+.

[3] *Deklaracja Komitetu Ministrów Rady Europy w sprawie zagrożeń dla praw podstawowych wynikających ze śledzenia cyfrowego i innych technologii nadzoru*, przyjęta 13 czerwca 2013 r., dostępna na: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168068460d.

[4] Niniejsze wytyczne opierają się na raporcie Sandry Azria i Frédérica Wickerta z 2019 r. *Rozpoznawanie twarzy: obecna sytuacja i wyzwania*, dostępnym pod adresem: https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1.

środki ochronne, w zależności od przypadku zastosowania. Oceniają różne zastosowania tych technologii w różnych sektorach, biorąc pod uwagę cele tych zastosowań i ich potencjalny wpływ na prawo do ochrony danych i inne prawa podstawowe.

Cele egzekwowania prawa oznaczają w niniejszych wytycznych zapobieganie przestępstwom, prowadzenie dochodzeń w ich sprawie i ich ściganie oraz wykonywanie sankcji karnych. Obejmuje to utrzymywanie porządku publicznego przez policję (określane dalej jako „cele egzekwowania prawa")[5]. Pod pojęciem „organy ds. egzekwowania prawa" rozumie się szerzej prokuratury i / lub inne organy publiczne i / lub prywatne upoważnione na mocy prawa do przetwarzania danych osobowych w tych samych celach (zwane dalej „organami ds. egzekwowania prawa").

Żadne z postanowień niniejszych wytycznych nie powinno być interpretowane jako wykluczające lub ograniczające postanowienia Konwencji 108[6]. Wytyczne te uwzględniają również nowe zabezpieczenia przewidziane przez Konwencję 108+.

I. WYTYCZNE DLA USTAWODAWCÓW I DECYDENTÓW

1. Zgodność z prawem

Zgodnie z art. 6 Konwencji 108+ przetwarzanie szczególnych kategorii danych, takich jak dane biometryczne, jest dozwolone tylko wtedy, gdy takie przetwarzanie opiera się na odpowiedniej podstawie prawnej, a prawo krajowe zapewnia uzupełniające i odpowiednie zabezpieczenia.

Zabezpieczenia te są dostosowane do ryzyka oraz do interesów, praw i wolności, które mają być chronione.

Niektóre przepisy prawa[7] co do zasady wprowadzają zakaz takiego przetwarzania i zezwalają na jego realizację jedynie w drodze wyjątku, w określonych szczególnych przypadkach (np. za wyraźną zgodą osób fizycznych, w celu ochrony ich żywotnych interesów lub gdy przetwarzanie jest niezbędne ze względu na nadrzędny interes publiczny) i podlegać zabezpieczeniom odpowiednim do tego ryzyka.

Konieczność stosowania technologii rozpoznawania twarzy należy ocenić wraz z proporcjonalnością do celu i wpływem na prawa osób, których dane dotyczą.

Należy kategoryzować różne przypadki wykorzystania oraz ustanowić ramy prawne mające zastosowanie do przetwarzania danych biometrycznych poprzez rozpoznawanie twarzy. Te ramy prawne powinny, w zależności od różnych zastosowań, odnosić się w szczególności do:

[5] Cele egzekwowania prawa odpowiadają „celom policji" w Praktycznym przewodniku dotyczącym wykorzystywania danych osobowych w sektorze policji, zob. Komitet Konwencji 108, Praktyczny przewodnik dotyczący wykorzystywania danych osobowych w sektorze policji (T-PD(2018)01), dostępny na: https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5.

[6] Oczywiście w przypadku Stron Konwencji, które są państwami członkowskimi Rady Europy, żadne postanowienia wytycznych nie mogą być ponadto interpretowane jako wykluczające lub ograniczające postanowienia Europejskiej Konwencji Praw Człowieka.

[7] Zobacz artykuł 9 *rozporządzenia ogólnego o ochronie danych Unii Europejskiej (RODO).*

- szczegółowego wyjaśnienia konkretnego zastosowania i celu;
- minimalnej niezawodności i dokładności[8] zastosowanego algorytmu;
- czasu przechowywania wykorzystanych zdjęć;
- możliwości audytu tych kryteriów;
- możliwości śledzenia procesu;
- zabezpieczeń.

1.1. Ścisłe ograniczenie określonych zastosowań przez prawo

Poziom inwazyjności rozpoznawania twarzy i związanego z tym naruszenia prawa do prywatności i ochrony danych będzie różny w zależności od konkretnej sytuacji wykorzystania rozpoznawania twarzy i będą przypadki, w których prawo krajowe będzie je ściśle ograniczać, a nawet całkowicie zakaże, w przypadku gdy proces demokratyczny doprowadzi do takiej decyzji.

Wykorzystywanie technologii rozpoznawania twarzy na żywo w niekontrolowanych środowiskach[9], w świetle inwazyjności, jaką stwarza dla prawa do prywatności i godności osób, w połączeniu z ryzykiem negatywnego wpływu na inne prawa człowieka i podstawowe wolności[10], powinno być przedmiotem demokratycznej debaty na temat wykorzystywania tych technologii i możliwości moratorium do czasu pełnej analizy.

Korzystanie z funkcji rozpoznawania twarzy wyłącznie w celu określenia koloru skóry, przekonań religijnych lub innych, płci, pochodzenia rasowego lub etnicznego, wieku, stanu zdrowia lub stanu społecznego danej osoby powinno być zabronione, chyba że prawo przewiduje odpowiednie zabezpieczenia w celu uniknięcia jakiegokolwiek ryzyka dyskryminacji[11].

Podobnie, rozpoznawanie emocji[12] można również przeprowadzić za pomocą technologii rozpoznawania twarzy, aby prawdopodobnie wykryć cechy osobowości, uczucia, zdrowie psychiczne lub zaangażowanie pracowników na podstawie obrazów twarzy. Powiązanie rozpoznania emocji, na przykład, z zatrudnianiem personelu, dostępem do ubezpieczenia, edukacją, może stanowić poważne zagrożenie, zarówno na poziomie indywidualnym, jak i społecznym, i powinno być zabronione.

1.2. Podstawa prawna w różnych kontekstach

Ramy prawne mające zastosowanie do przetwarzania danych biometrycznych poprzez rozpoznawanie twarzy, oprócz elementów wymienionych w sekcji 1, powinny uwzględniać:
- różne fazy wykorzystywania technologii rozpoznawania twarzy, w tym tworzenie baz danych i fazy

[8] Dokładność algorytmu można wyrazić poprzez ocenę fałszywie dodatnich lub fałszywie ujemnych błędów generowanych przez oprogramowanie.
[9] Pojęcie „niekontrolowanego środowiska" obejmuje miejsca swobodnie dostępne dla osób, przez które mogą również przechodzić, w tym przestrzenie publiczne i quasi-publiczne, takie jak centra handlowe, szpitale czy szkoły.
[10] Zobacz *Wytyczne dotyczące sztucznej inteligencji i ochrony danych*: https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7.
[11] Mogłoby na przykład być dozwolone do celów projektu badań medycznych, z zastrzeżeniem odpowiednich zabezpieczeń przewidzianych prawem.
[12] „Rozpoznawanie emocji" to wykorzystywanie technologii do próby zidentyfikowania lub sklasyfikowania ludzkich emocji.

zastosowania;
- sektory, w których stosowane są te technologie;

- inwazyjność rodzajów technologii rozpoznawania twarzy, takich jak technologie rozpoznawania twarzy na żywo lub nie na żywo, przy jednoczesnym zapewnieniu jasnych wskazówek dotyczących zgodności z prawem.

1.2.1. Integracja obrazów cyfrowych z technologiami rozpoznawania twarzy

Ustawodawcy i decydenci zapewnią, aby obrazy dostępne w formacie cyfrowym nie mogły być przetwarzane w celu wyodrębnienia szablonów biometrycznych[13] ani nie mobły być zintegrowane z systemami biometrycznymi bez określonej podstawy prawnej do nowego przetwarzania, gdy obrazy te zostały pierwotnie pobrane do innych celów (na przykład z mediów społecznościowych)media.

Ponieważ wyodrębnianie szablonów biometrycznych z obrazów cyfrowych wiąże się z przetwarzaniem danych wrażliwych, należy zabezpieczyć rozważane poniżej możliwe podstawy prawne, różniące się dla różnych sektorów i zastosowań.

W szczególności wykorzystywanie obrazów cyfrowych, które zostały umieszczone w Internecie, w tym w mediach społecznościowych lub internetowych witrynach do zarządzania zdjęciami, lub zostały przechwycone przez obiektyw monitorujących kamer wideo, nie może być uznane za zgodne z prawem wyłącznie na tej podstawie, że dane osobowe zostały w sposób oczywisty udostępnione przez osoby, których dane dotyczą.

Ustawodawcy i decydenci powinni dopilnować, aby istniejące bazy danych zawierające obrazy cyfrowe, które były pierwotnie wykorzystywane do innych celów, mogły być wykorzystywane wyłącznie do wyodrębniania szablonów biometrycznych i integracji ich z systemami biometrycznymi, jeżeli służy to nadrzędnym uzasadnionym celom i jest przewidziane przez prawo oraz jest ściśle konieczne (niezbędne) i proporcjonalne do tych celów (na przykład do celów egzekwowania prawa lub celów medycznych).

1.2.2. Wykorzystywanie technologii rozpoznawania twarzy w sektorze publicznym

Zgoda nie powinna co do zasady stanowić podstawy prawnej wykorzystywanej do rozpoznawania twarzy prowadzonego przez organy publiczne ze względu na brak równowagi uprawnień między osobami, których dane dotyczą, a organami publicznymi. Z tego samego powodu co do zasady nie powinna być podstawą prawną rozpoznawania twarzy prowadzonego przez podmioty prywatne uprawnione do wykonywania podobnych zadań jak organy publiczne.

Zgodność z prawem stosowania technologii rozpoznawania twarzy opiera się na celach przetwarzania danych biometrycznych przewidzianych przez prawo oraz na niezbędnych zabezpieczeniach uzupełniających Konwencję 108+.

Ustawodawcy i decydenci muszą określić szczegółowe zasady dotyczące przetwarzania danych biometrycznych za pomocą technologii rozpoznawania twarzy do celów egzekwowania prawa.

[13] „Szablon biometryczny" to cyfrowa reprezentacja unikalnych cech, które zostały wyodrębnione z próbki biometrycznej, i jest przechowywana w biometrycznej bazie danych.

Przepisy te zagwarantują, że takie wykorzystywanie będzie ściśle konieczne (niezbędne) i proporcjonalne do tych celów, oraz określi niezbędne zabezpieczenia, które należy zapewnić.

Organy ds. egzekwowania prawa

Przetwarzanie danych biometrycznych przez technologie rozpoznawania twarzy do celów identyfikacji w kontrolowanym[14] lub niekontrolowanym środowisku powinno być ogólnie ograniczone do celów egzekwowania prawa. Powinno być prowadzone wyłącznie przez właściwe organy w zakresie bezpieczeństwa.

Przepisy mogą przewidywać różne testy konieczności (niezbędności) i proporcjonalności w zależności od tego, czy celem jest weryfikacja czy identyfikacja, biorąc pod uwagę potencjalne zagrożenia dla praw podstawowych i pod warunkiem, że obrazy osób fizycznych są gromadzone zgodnie z prawem.

Do celów identyfikacji należy przestrzegać ścisłej konieczności i proporcjonalności zarówno podczas tworzenia bazy danych (listy obserwacyjnej), jak i wdrażania (na żywo) technologii rozpoznawania twarzy w niekontrolowanym środowisku.

Przepisy powinny określać jasne parametry i kryteria, których organy ds. egzekwowania prawa powinny przestrzegać, tworząc bazy danych (listy obserwacyjne) do konkretnych, zgodnych z prawem i wyraźnych celów egzekwowania prawa (na przykład w przypadku podejrzenia poważnych przestępstw lub zagrożenia bezpieczeństwa publicznego).

Biorąc pod uwagę inwazyjność tych technologii, na etapie wdrażania technologii rozpoznawania twarzy na żywo w niekontrolowanych środowiskach prawo gwarantuje, że organy ds. egzekwowania prawa wykażą, że różne czynniki, w tym miejsce i czas wdrożenia tych technologii, uzasadniają ścisłą konieczność i proporcjonalność zastosowań.

Inne organy publiczne

Ustawodawcy i decydenci określą szczegółowe zasady przetwarzania danych biometrycznych za pomocą technologii rozpoznawania twarzy w innych istotnych interesach publicznych przez organy publiczne, które nie realizują celów związanych z egzekwowaniem prawa.

Przepisy mogą przewidywać różne testy konieczności (niezbędności) i proporcjonalności w zależności od tego, czy celem jest weryfikacja czy identyfikacja, biorąc pod uwagę potencjalne zagrożenia dla praw podstawowych i pod warunkiem, że obrazy osób fizycznych są gromadzone zgodnie z prawem.

Biorąc pod uwagę potencjalną ingerencję tych technologii, prawodawcy i decydenci muszą zapewnić, aby wyraźna i precyzyjna podstawa prawna zapewniała niezbędne zabezpieczenia przetwarzania danych biometrycznych. Taka podstawa prawna będzie obejmować ścisłą konieczność i proporcjonalność tych zastosowań oraz będzie uwzględniać wrażliwość osób, których dane dotyczą, oraz charakter środowiska, w którym te technologie są wykorzystywane do celów weryfikacji.

Na przykład zapewnienie bezpieczeństwa w kontrolowanych lub niekontrolowanych środowiskach, w tym w szkołach lub innych budynkach publicznych, co do zasady nie powinno być uważane za ściśle konieczne i proporcjonalne, jeżeli istnieją mniej inwazyjne mechanizmy alternatywne.

[14] Pojęcie „kontrolowane środowisko" obejmuje przypadki, w których systemy biometryczne mogą być wykorzystywane tylko przy udziale danej osoby.

1.2.3. Wykorzystywanie technologii rozpoznawania twarzy w sektorze prywatnym

Wykorzystywanie technologii rozpoznawania twarzy przez podmioty prywatne, z wyjątkiem podmiotów prywatnych uprawnionych do wykonywania podobnych zadań jak organy publiczne, wymaga zgodnie z art. 5 Konwencji 108+ wyraźnej, konkretnej, dobrowolnej i świadomej zgody osób, których dane dotyczą, których dane biometryczne są przetwarzane.

Biorąc pod uwagę wymóg wyrażenia takiej zgody przez osoby, których dane dotyczą, wykorzystywanie technologii rozpoznawania twarzy może mieć miejsce wyłącznie w kontrolowanych środowiskach w celu weryfikacji, uwierzytelnienia lub kategoryzacji[15].

W zależności od celu należy zwrócić szczególną uwagę na jakość wyraźnej zgody osoby, której dane dotyczą, gdy stanowi ona podstawę prawną przetwarzania.

Aby zapewnić dobrowolność wyrażenia zgody, osobom, których dane dotyczą, należy zaoferować alternatywne rozwiązania w stosunku do korzystania z technologii rozpoznawania twarzy (na przykład za pomocą hasła lub identyfikatora), które są łatwe w użyciu, ponieważ jeżeli byłyby zbyt długie lub skomplikowane w porównaniu z technologią rozpoznawania twarzy, wybór nie byłby prawdziwy.

W przypadku wyrażenia zgody w określonym celu dane osobowe nie powinny być przetwarzane w sposób niezgodny z tym celem. Podobnie w przypadku ujawnienia danych stronie trzeciej, takie ujawnienie powinno również podlegać wymogowi szczególnej zgody.

Podmioty prywatne nie wdrażają technologii rozpoznawania twarzy w niekontrolowanych środowiskach, takich jak centra handlowe, zwłaszcza w celu identyfikacji osób będących przedmiotem zainteresowania, do celów marketingowych lub do celów bezpieczeństwa prywatnego.

Przejścia przez środowisko, w którym używane są technologie rozpoznawania twarzy, nie można uznać za wyraźną zgodę.

2. Niezbędne zaangażowanie organów nadzorczych

Zgodnie z art. 15 ust. 3 konwencji 108+ należy konsultować się z organami nadzorczymi w sprawie wniosków dotyczących wszelkich środków ustawodawczych lub administracyjnych, które wiążą się z przetwarzaniem danych osobowych za pomocą technologii rozpoznawania twarzy. Konieczne jest systematyczne angażowanie organów nadzorczych, a w szczególności konsultowanie się z nimi w sprawie ewentualnych eksperymentów lub przewidywanego zastosowania.

W związku z tym należy konsultować się z tymi organami systematycznie i przed planowanymi projektami.

Podobnie powinny one mieć dostęp do przeprowadzonych ocen skutków, a także do wszystkich audytów, sprawozdań i analiz przeprowadzonych w kontekście takich eksperymentów lub projektów.

Ustawodawcy i decydenci powinni zapewnić skuteczną współpracę między różnymi organami nadzorczymi właściwymi do nadzorowania różnych aspektów takich operacji przetwarzania danych, w

[15] „Kategoryzacja biometryczna” oznacza proces ustalania, czy dane biometryczne osoby należą do grupy o określonej z góry charakterystyce w celu podjęcia określonego działania.

przypadku gdy różne organy są odpowiedzialne za kontrolę zgodności takich czynności przetwarzania z prawem.

3. Certyfikacja

Ustawodawcy i decydenci powinni stosować różne mechanizmy, aby zapewnić rozliczalność twórców, producentów, usługodawców lub podmiotów korzystających z tych technologii.

Ustanowienie niezależnego i kwalifikowanego mechanizmu certyfikacji w zakresie rozpoznawania twarzy i ochrony danych w celu wykazania pełnej zgodności prowadzonych operacji przetwarzania byłoby podstawowym elementem budowania zaufania użytkowników.

Taka certyfikacja mogłaby być wdrożona zgodnie z zastosowaniem sztucznej inteligencji wykorzystywanej przez technologię rozpoznawania twarzy: jeden rodzaj certyfikacji do kategoryzacji struktur (projekt algorytmu, integracja algorytmu itp.), a inny do kategoryzacji algorytmów (rozpoznawanie komputerowe, inteligentne wyszukiwanie, itp.).

4. Podnoszenie świadomości

Świadomość osób, których dane dotyczą, oraz zrozumienie przez ogół społeczeństwa technologii rozpoznawania twarzy i ich wpływu na prawa podstawowe powinny być aktywnie wspierane poprzez dostępne i edukacyjne działania.

Chodzi o to, aby zapewnić dostęp do prostych pojęć, które mogłyby ostrzec osoby, których dane dotyczą, zanim zdecydują się na skorzystanie z technologii rozpoznawania twarzy, aby zrozumieć, co to znaczy wykorzystywać dane wrażliwe, takie jak dane biometryczne, jak działa rozpoznawanie twarzy, oraz ostrzec je o potencjalnym niebezpieczeństwie, zwłaszcza w przypadku niewłaściwego wykorzystania.

Ustawodawcy i decydenci powinni ułatwiać publiczne zaangażowanie w opracowywanie i wykorzystywanie tych technologii oraz w zapewnianie odpowiednich zabezpieczeń w celu ochrony praw podstawowych podczas korzystania z rozpoznawania twarzy.

II. WYTYCZNE DLA TWÓRCÓW, PRODUCENTÓW I DOSTAWCÓW USŁUG

Ta sekcja wytycznych obejmuje w szczególności kwestie związane z fazami rozwoju i produkcji technologii rozpoznawania twarzy. W przypadku gdy twórcy, producenci i usługodawcy przetwarzają dane biometryczne do własnych celów w fazie rozwoju, będą ponadto zainteresowani sekcją III wytycznych dotyczących podmiotów stosujących taką technologię.

1. Jakość danych i algorytmów

1.1. Reprezentatywność wykorzystanych danych

Podobnie jak inne mające zastosowanie instrumenty prawne, konwencja 108+ w art. 5 zawiera wymóg dotyczący prawidłowości danych. W związku z tym twórcy lub producenci technologii rozpoznawania twarzy, a właściwie również podmioty korzystające z technologii rozpoznawania twarzy, będą musieli podjąć kroki w celu zapewnienia prawidłowości danych dotyczących rozpoznawania twarzy. W szczególności będą musieli unikać błędnego etykietowania, a tym samym wystarczająco testować swoje systemy oraz identyfikować i eliminować rozbieżności w prawidłowości, zwłaszcza w odniesieniu do demograficznych różnic w kolorze skóry, wieku i płci, a tym samym unikać niezamierzonej dyskryminacji.

Ponadto, aby zapewnić zarówno jakość danych, jak i skuteczność algorytmów, algorytmy będą musiały zostać opracowane z wykorzystaniem syntetycznych zbiorów danych opartych na wystarczająco zróżnicowanych zdjęciach kobiet i mężczyzn, o różnym kolorze skóry, o różnej morfologii, w każdym wieku i pod różnymi kątami kamery. Należy przewidzieć procedury awaryjne na wypadek awarii systemu, jeśli właściwości fizyczne nie odpowiadają standardom technicznym.

Dane biometryczne w nieunikniony sposób ujawniające inne wrażliwe dane, takie jak informacje o rodzaju choroby lub niepełnosprawności fizycznej, musiałyby podlegać uzupełniającym odpowiednim zabezpieczeniom.

1.2. Czas życia danych

System rozpoznawania twarzy wymaga okresowego odnawiania danych (zdjęć twarzy do rozpoznania) w celu szkolenia i doskonalenia stosowanego algorytmu.

Każdy algorytm ma określony procent niezawodności rozpoznawania, zarówno podczas jego tworzenia, jak i użytkowania. W związku z tym ważne wydaje się być datowanie i rejestrowanie tego procentu, aby monitorować jego ewolucję. W przypadku pogorszenia się niezawodności algorytmu konieczne będzie odnowienie zdjęć treningowych i w związku z tym poproszenie o dostarczenie bardziej aktualnych zdjęć. Pozwoli to również uchronić się przed konsekwencjami zmian kształtu twarzy (na skutek starzenia, stosowania akcesoriów - przekłuwania lub innych - lub innych modyfikacji).

Te rekordy dotyczące procentowej niezawodności można łatwo udostępniać osobom fizycznym lub zainteresowanym klientom lub podmiotom korzystającym z technologii rozpoznawania twarzy, na przykład w postaci tablicy wskaźników, aby ułatwić im wybór co do nabycia i wdrożenia określonej technologii.

2. Niezawodność wykorzystanych narzędzi

Niezawodność zastosowanych narzędzi zależy od skuteczności algorytmu. Skuteczność ta zależy od różnych czynników, między innymi: fałszywych wyników dodatnich, fałszywych wyników ujemnych, wydajności w różnych oświetleniach, niezawodności w przypadku twarzy odwróconych od aparatu, wpływu nakrycia twarzy.

Należy zapewnić jak najwyższy poziom niezawodności, biorąc pod uwagę, że korzystanie z systemu rozpoznawania twarzy może mieć bardzo poważne negatywne konsekwencje dla danej osoby.

3. Świadomość

Firmy opracowujące i sprzedające technologie rozpoznawania twarzy powinny podejmować rozsądne kroki - takie jak wydawanie zaleceń i udzielanie porad - aby pomóc korzystającym z nich podmiotom w stosowaniu przejrzystości i poszanowaniu prywatności (poprzez dostarczenie im przykładowego języka dla ich polityk prywatności lub rekomendowanie łatwego do zrozumienia oznakowania, które wskazuje, że technologia rozpoznawania twarzy została wdrożona w określonej przestrzeni).

4. Rozliczalność

Firmy opracowujące i sprzedające technologie rozpoznawania twarzy powinny przyjąć określone środki w celu zapewnienia zgodności z zasadami ochrony danych, takie jak:

- włączenie ochrony danych w projekt i architekturę produktów i usług w zakresie rozpoznawania twarzy, a także w wewnętrzne systemy informatyczne oraz zintegrowanie wykorzystania dedykowanych narzędzi, w tym automatycznego usuwania surowych danych po wyodrębnieniu szablonów biometrycznych;

- oferowanie pewnego poziomu elastyczności w projektowaniu tych technologii w celu dostosowania zabezpieczeń technicznych zgodnie z zasadami ograniczenia celu, minimalizacji danych i ograniczenia czasu przechowywania danych;

- wdrożenie procesu przeglądu wewnętrznego mającego na celu określenie i zminimalizowanie potencjalnego wpływu na prawa i podstawowe wolności, zanim technologie rozpoznawania twarzy staną się dostępne;

- włączenie podejścia do ochrony danych do swoich praktyk organizacyjnych, w tym przydzielenie dedykowanego personelu, zapewnienie pracownikom szkolenia w zakresie ochrony prywatności oraz przeprowadzanie ocen skutków dla ochrony danych w przypadku opracowywania lub modyfikowania produktów i usług rozpoznawania twarzy.

III. WYTYCZNE DLA PODMIOTÓW WYKORZYSTUJĄCYCH TECHNOLOGIE ROZPOZNAWANIA TWARZY

Podmioty[16] przetwarzające dane biometryczne przy zastosowaniu technologii rozpoznawania twarzy muszą przestrzegać wszystkich obowiązujących zasad i przepisów dotyczących ochrony danych. Podmioty wykorzystujące technologie rozpoznawania twarzy muszą być w stanie wykazać, że takie zastosowanie jest ściśle niezbędne i proporcjonalne w określonym kontekście ich stosowania oraz że nie narusza praw osób, których dane dotyczą.

[16] W niniejszej sekcji Wytycznych termin „podmioty" obejmuje administratorów danych, a w stosownych przypadkach podmioty przetwarzające, zarówno w sektorze publicznym, jak i prywatnym.

Podmioty mogą powoływać się na wyjątki przewidziane w obowiązującym prawodawstwie zgodnym z art. 11 Konwencji 108+ (przewidzianym przez prawo, dążące do określonego, prawnie uzasadnionego celu, szanujące istotę podstawowych praw i wolności oraz stanowiące konieczny i proporcjonalny środek w demokratycznym społeczeństwie).

Podmioty wykorzystujące technologie rozpoznawania twarzy muszą zapewnić, że dobrowolne użycie tej technologii nie będzie miało wpływu na osoby, które przypadkowo zetkną się z nią w sposób niezamierzony.

1. Zgodność przetwarzania danych z prawem i jakość danych

Podmioty będą opierać się na różnych podstawach prawnych w zależności od ich sektorów i celów stosowania technologii rozpoznawania twarzy wymienionych w sekcji I.

Przejrzystość i rzetelność

Ponieważ technologie rozpoznawania twarzy mogą być wykorzystywane bez żadnego zamiaru lub bez jakiejkolwiek współpracy z osobami, których dane dotyczą, przejrzystość i rzetelność przetwarzania mają ogromne znaczenie i będą musiały zostać należycie rozważone przez podmioty stosujące tę technologię.

Podmioty będą musiały dostarczyć wszelkich niezbędnych informacji na temat przetwarzania, wyszczególnionych w art. 8 Konwencji 108+.

Czynniki, które zadecydują o tym, czy zapewniono przejrzystość, obejmują na przykład to, czy informacje są przekazywane osobom fizycznym, kontekst zbierania danych, rozsądne oczekiwania co do sposobu wykorzystania danych, czy rozpoznawanie twarzy jest jedynie cechą produktu lub usługi czy raczej integralną częścią samej usługi. Osoby powinny był również informowane o tym, jak może wpłynąć na nie zbieranie, wykorzystywanie lub wymiana danych dotyczących rozpoznawania twarzy, zwłaszcza gdy dotyczą one osób znajdujących się w szczególnie trudnej sytuacji. Przekazane informacje muszą również określać, jakie prawa i środki ochrony prawnej przysługują osobom, których dane dotyczą.

Polityka prywatności dotycząca rozpoznawania twarzy lub materiały informacyjne dotyczące technologii powinny zawierać, oprócz informacji przewidzianych w art. 8 Konwencji 108+, następujące informacje[17]:

- czy i w jakim zakresie dane dotyczące rozpoznawania twarzy mogą być przekazywane stronom trzecim (i gdy ma to zastosowanie, informacje o tożsamości kontrahentów będących stronami trzecimi, otrzymujących dane w trakcie dostarczania produktu lub usługi);
- zatrzymywanie, usuwanie lub deidentyfikacja (pozbawianie elementów identyfikacyjnych) danych przetwarzanych w formie rozpoznawania twarzy;
- punkty kontaktowe dostępne dla osób fizycznych, które mogą zadawać pytania dotyczące zbierania, wykorzystywania i wymiany danych przetwarzanych w formie rozpoznawania twarzy;

[17] Zob. zalecenia Future Privacy Forum „Zasady prywatności w zakresie technologii rozpoznawania twarzy w zastosowaniach komercyjnych" https://fpf.org/blog/fpf-releases-understanding-facial-detection-characterization-and-recognition-technologies-and-privacy-principles-for-facial-recognition-technology-in-commercial-applications/

- w przypadku gdy praktyki zbierania, wykorzystywania i wymiany ulegają istotnej zmianie, podmioty powinny aktualizować swoją politykę prywatności lub upublicznić te zmiany w świetle kontekstu zmiany i jej wpływu na osoby fizyczne.

W przypadku tworzenia przez organy ds. egzekwowania prawa baz danych do celów identyfikacji lub weryfikacji, obowiązek przejrzystości może być proporcjonalnie ograniczony, tak aby nie naruszać celów egzekwowania prawa, zgodnie z art. 11 Konwencji 108+ i z zastrzeżeniem jego wymagań.

W przypadku wykorzystywania na żywo technologii rozpoznawania twarzy w niekontrolowanym środowisku organy ds. egzekwowania prawa mogą przyjąć warstwowe podejście do dostarczania niezbędnych informacji osobom, których dane dotyczą w niekontrolowanym środowisku.

Pierwsza warstwa dostarczania informacji będzie zawierać czytelne i zrozumiałe informacje o celu przetwarzania, organie wykorzystującym tę technologię, czasie trwania przetwarzania i objętym obszarze, a także będzie umieszczana w odpowiednim sąsiedztwie miejsca, w którym technologie te są wykorzystywane.

Druga warstwa dostarczania informacji będzie zawierać wszystkie niezbędne informacje wymagane zgodnie z art. 8 Konwencji 108+, które należy umieścić w punktach wejścia do miejsca zastosowania.

Ukryte wykorzystywanie technologii rozpoznawania twarzy na żywo przez organy ds. egzekwowania prawa może być możliwe, jeżeli jest to ściśle niezbędne i proporcjonalne, aby zapobiec bezpośredniemu i znacznemu zagrożeniu dla bezpieczeństwa publicznego, które powinno zostać udokumentowane przed ukrytym wykorzystaniem.

Ograniczenie celu, minimalizacja danych i ograniczenie czasu przechowywania

Dane osobowe podlegające przetwarzaniu powinny być zbierane w wyraźnych, konkretnych i prawnie uzasadnionych celach i nie powinny być przetwarzane w sposób niezgodny z tymi celami zgodnie z art. 5 ust. 4 Konwencji 108+.

Ponadto, przed jakimkolwiek kolejnym przetwarzaniem podmioty będą musiały rozważyć, czy cele nowego przetwarzania są zgodne z pierwotnie określonymi celami. W przeciwnym razie nowe przetwarzanie będzie wymagało odrębnej podstawy prawnej.

Podmioty muszą przestrzegać zasady minimalizacji danych, która wymaga, aby przetwarzane były tylko wymagane informacje, a nie wszystkie informacje dostępne podmiotom.

Podmioty muszą również ustalić okres zatrzymywania, który nie może być dłuższy niż okres niezbędny do konkretnego celu przetwarzania, oraz muszą zapewnić usunięcie szablonów biometrycznych po zakończeniu tego celu. Przy określaniu okresu zatrzymywania/ należy wziąć pod uwagę biometryczny charakter danych osobowych.

Przy wdrażaniu technologii rozpoznawania twarzy na żywo podmioty muszą ponadto zapewnić, aby różne okresy przechowywania miały zastosowanie do różnych faz przetwarzania:

- w przypadku braku dopasowania szablonów biometrycznych, szablon biometryczny osób przechodzących przez niekontrolowane środowisko nie może zostać zachowany i musi zostać automatycznie usunięty;

- w przypadku dopasowania szablony biometryczne można zatrzymywać przez ściśle ograniczony czas przewidziany przez prawo z niezbędnymi zabezpieczeniami i raportami dotyczącymi dopasowania, w tym dane osobowe mogą być również zatrzymywanie przez ograniczony czas;

- w każdym przypadku należy usunąć listę obserwacyjną i szablony biometryczne po zakończeniu realizacji celu, w którym zastosowano technologie rozpoznawania twarzy na żywo.

Prawidłowość

Podmioty muszą zapewnić prawidłowość i uaktualnianie szablonów biometrycznych i obrazów cyfrowych. Na przykład, jakość obrazów i szablonów biometrycznych umieszczonych na listach obserwacyjnych musi być sprawdzona, aby zapobiec potencjalnym fałszywym dopasowaniom, ponieważ niska jakość obrazów może spowodować wzrost liczby błędów. Jest to bezpośrednio związane ze źródłami obrazów zestawionych na liście obserwacyjnej, które wymagają ścisłego przestrzegania zasad ochrony danych, takich jak zasada ograniczenia celu.

W przypadku błędnych dopasowań podmioty podejmą wszelkie uzasadnione kroki w celu skorygowania przyszłych zdarzeń oraz zapewnienia prawidłowości obrazów cyfrowych i szablonów biometrycznych.

2. Bezpieczeństwo danych

Jakiekolwiek niepowodzenie w zakresie bezpieczeństwa danych może mieć szczególnie poważne konsekwencje dla osób, których dane dotyczą, ponieważ nieuprawnione ujawnienie takich wrażliwych danych nie może zostać naprawione.

Należy zatem wdrożyć silne środki bezpieczeństwa, zarówno na poziomie technicznym, jak i organizacyjnym, w celu ochrony danych dotyczących rozpoznawania twarzy i zestawów obrazów przed utratą i nieuprawnionym dostępem lub wykorzystaniem danych na wszystkich etapach przetwarzania, niezależnie od tego, czy chodzi o zbieranie, przekazywanie i przechowywanie.

Podmioty podejmą działania mające na celu zapobieganie atakom specyficznym dla technologii, w tym atakom prezentacyjnym i atakom morfingu.

Każde naruszenie bezpieczeństwa danych, które może poważnie kolidować z prawami i podstawowymi wolnościami osób, których dane dotyczą, musi zostać zgłoszone organowi nadzorczemu oraz, w stosownych przypadkach, osobom, których dane dotyczą.

Środki bezpieczeństwa powinny ewoluować w czasie i w odpowiedzi na zmieniające się zagrożenia i zidentyfikowane podatności. Powinny być również proporcjonalne do wrażliwości danych, kontekstu wykorzystywania określonej technologii rozpoznawania twarzy i jej celów, prawdopodobieństwa wyrządzenia szkody osobom fizycznym i innych istotnych czynników.

Rygorystyczne praktyki zatrzymywania i usuwania - poprzez bezpieczne procedury - danych dotyczących rozpoznawania twarzy, przy jak najkrótszym okresie zatrzymywania, przyczyniają się również do zmniejszenia narażenia na zagrożenia.

3. Rozliczalność

Podmioty podejmą wszelkie odpowiednie działania w celu wypełnienia swoich zobowiązań i wykazania, że przetwarzanie danych pod ich kontrolą jest zgodne ze zobowiązaniami, jak przewidziano w art. 10 Konwencji 108+.

Podmioty stosujące technologie rozpoznawania twarzy muszą uwzględnić następujące środki organizacyjne:

- wdrażanie przejrzystych polityk, procedur i praktyk w celu zapewnienia, że ochrona praw osób, których dane dotyczą, leży u podstaw stosowania przez nie technologii rozpoznawania twarzy;
- publikowanie sprawozdań na temat przejrzystości dotyczących konkretnego wykorzystania technologii rozpoznawania twarzy;
- ustanawianie i dostarczanie programów szkoleniowych i procedur audytu dla osób odpowiedzialnych za przetwarzanie danych dotyczących rozpoznawania twarzy;
- ustanawianie wewnętrznych komitetów weryfikacyjnych w celu oceny i zatwierdzania wszelkiego przetwarzania danych dotyczących rozpoznawania twarzy;
- umowne rozszerzenie odpowiednich wymogów na dostawców usług będących stronami trzecimi, partnerów biznesowych lub inne podmioty wykorzystujące technologię rozpoznawania twarzy (oraz odmowa dostępu stronom trzecim, które by ich nie przestrzegały);
- w sektorze publicznym: ograniczenia związane z uprzednią oceną w podstępowaniach o udzielenia zamówień publicznych z udziałem dostawców narzędzi do rozpoznawania twarzy, ocena minimalnych poziomów skuteczności pod względem prawidłowości, w szczególności w odniesieniu do celów egzekwowania prawa.

Podmioty podejmą niezbędne środki techniczne w celu zapewnienia jakości danych biometrycznych poprzez stosowanie uzgodnionych na szczeblu międzynarodowym norm technicznych, w zależności od kontekstu ich wykorzystania.

Podmioty wykorzystujące technologie rozpoznawania twarzy powinny zagwarantować, że operatorzy –(ludzie) będą nadal odgrywać decydującą rolę w działaniach podejmowanych w oparciu o wyniki tych technologii. Podmioty korzystające z tych technologii powinny podejmować środki organizacyjne w celu nadzorowania operatorów (ludzi) podejmujących decyzje, które mogą mieć znaczący wpływ na jednostki.

3.1. Ocena skutków dla ochrony danych

Podmioty wykorzystujące technologie rozpoznawania twarzy muszą dokonać oceny skutków przed przetwarzaniem, ponieważ stosowanie tych technologii wiąże się z przetwarzaniem danych biometrycznych i stanowi wysokie ryzyko naruszenia praw podstawowych osób, których dane dotyczą.

Podczas dokonywania oceny skutków podmioty nie tylko rozpoznają ryzyko wynikające z potencjalnego przetwarzania, ale także rozważą niezbędne środki łagodzące, aby zaradzić tym zagrożeniom poprzez podjęcie niezbędnych środków technicznych i organizacyjnych. W tej ocenie wyjaśnią one m.in.:

- zgodność z prawem stosowania tych technologii;
- jakie prawa podstawowe są zagrożone w procesie przetwarzania biometrycznego;
- podatność na zagrożenia osób, których dane dotyczą;
- w jaki sposób można skutecznie ograniczyć te zagrożenia.

Biorąc pod uwagę zastosowanie technologii rozpoznawania twarzy w niekontrolowanych środowiskach, organy ds. egzekwowania prawa będą musiały:

- ocenić i wyjaśnić w swojej ocenie ścisłą konieczność (niezbędność) i proporcjonalność wdrażania tych technologii;
- zająć się ryzykiem dla różnych praw podstawowych, w tym ochrony danych, prywatności, wolności wypowiedzi, wolności zgromadzeń, swobody przemieszczania się lub antydyskryminacji, w zależności od potencjalnych zastosowań w różnych miejscach.

Ocenę skutków mogłyby dokonać same podmioty, niezależny podmiot monitorujący, audytor posiadający odpowiednią wiedzę fachową, która pomoże ustalić, zmierzyć lub nakreślić wpływ i ryzyko na przestrzeni czasu.

W trakcie przygotowywania oceny skutków podmioty muszą współpracować z zainteresowanymi stronami, w tym z osobami, których to dotyczy, w celu oceny potencjalnych skutków z ich perspektywy.

Takie oceny skutków muszą być przeprowadzane w regularnych odstępach czasowych.

W przypadku zidentyfikowania ryzyka zainteresowane podmioty powinny mieć możliwość zwracania się do wszelkich istniejących komitetów etycznych oraz do właściwych organów nadzorczych w celu zbadania potencjalnych zagrożeń.

Po zakończeniu oceny podmioty powinny ją opublikować w celu uzyskania opinii publicznej na temat potencjalnego zastosowania technologii rozpoznawania twarzy.

3.2. Ochrona danych w fazie projektowania

Ochrona danych w fazie projektowania obejmuje cały łańcuch wartości przetwarzania za pomocą technologii rozpoznawania twarzy. Podmioty wykorzystujące te technologie do celów identyfikacji lub weryfikacji muszą dopilnować, aby wykorzystywane przez nie produkty lub usługi były zaprojektowane do przetwarzania danych biometrycznych zgodnie z zasadami ograniczenia celu, minimalizacji danych i ograniczonego okresu przechowywania danych, a także do integracji wszystkich innych niezbędnych zabezpieczeń w technologiach.

Kiedy podmioty ustalają cechy techniczne tych technologii, wdrażają te zasady w fazie projektowania, aby zapewnić, że ich wdrożenie będzie zgodne z prawem do ochrony danych.

4. Ramy etyczne

Oprócz przestrzegania zobowiązań prawnych kluczowe znaczenie ma również zapewnienie ram etycznych dla stosowania tej technologii, w szczególności w odniesieniu do większego ryzyka związanego z wykorzystaniem technologii rozpoznawania twarzy w niektórych sektorach. Mogłoby to przybrać formę niezależnych rad doradczych ds. etyki, które mogłyby być konsultowane przed i podczas dłuższych zastosowań, przeprowadzać audyty i publikować wyniki swoich badań w celu uzupełnienia lub zatwierdzenia odpowiedzialności (rozliczalności) podmiotu. Wyraźne względy etyczne mogą pomóc w znalezieniu odpowiedniej równowagi między konkurencyjnymi interesami w sposób ewidentnie uczciwy.[18]

[18] Zob. Wytyczne w sprawie sztucznej inteligencji i ochrony danych, dostępne pod adresem https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7

Ponadto, aby uniknąć łamania praw człowieka, komitety ekspertów z różnych dziedzin będą prawdopodobnie definiować najtrudniejsze przypadki wykorzystania technologii rozpoznawania twarzy.

W tej kwestii istotną rolę do odegrania mają również sygnaliści, a pracownicy podmiotów korzystających z tych rozwiązań powinni mieć możliwość korzystania z odpowiedniego statusu ochrony, jak przewidziano w szczególności w Zaleceniu (2014)7 Komitetu Ministrów Rady Europy w sprawie ochrony sygnalistów.

IV. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

Ponieważ rozpoznawanie twarzy opiera się na przetwarzaniu danych osobowych, wszystkie prawa przewidziane w art. 9 Konwencji 108+ są zagwarantowane dla osób, których dane dotyczą, w szczególności prawo do informacji, prawo dostępu, prawo do zapoznania się z uzasadnieniem, prawo do sprzeciwu, prawo do sprostowania danych.

Prawa te mogą być ograniczone, ale tylko wtedy, gdy takie ograniczenie jest przewidziane przez prawo, respektuje istotę podstawowych praw i wolności oraz stanowi niezbędny i proporcjonalny środek w społeczeństwie demokratycznym do określonych i prawnie uzasadnionych celów (takich jak egzekwowanie prawa), zgodnie z art. 11 konwencji 108+.

W przypadku ograniczenia praw osób, których dane dotyczą, organy ds. egzekwowania prawa muszą informować osoby, których dane dotyczą m.in. o przysługującym im prawie do wniesienia skargi do organów nadzorczych oraz o ich ogólnym prawie do skutecznego środka ochrony prawnej

W przypadku fałszywych dopasowań, osoby, których dane dotyczą, mogą zażądać sprostowania, aby uniknąć kolejnych/powtarzających się fałszywych dopasowań.

W przypadku gdy wykorzystanie technologii rozpoznawania twarzy ma na celu umożliwienie podjęcia decyzji wyłącznie w oparciu o zautomatyzowane przetwarzanie, które miałoby istotny wpływ na osobę, której dane dotyczą, musi ona w szczególności być uprawniona do nieprowadzenia takiego przetwarzania bez uwzględnienia jej opinii.

Przy wdrażaniu technologii rozpoznawania twarzy na żywo, jeżeli operatorzy działający wyłącznie na podstawie wyników tych technologii, można uznać, że jest to wyłącznie zautomatyzowane podejmowanie decyzji, co miałoby znaczący wpływ na osobę, której dane dotyczą, ze względu na konsekwencje ewentualnych fałszywych dopasowań. Osoba, której dane dotyczą, może zatem zażądać, zgodnie z art. 9 ust. 1 lit. a) Konwencji 108+, uwzględnienia jej opinii.