thalesgroup.com

THALES
Building a future we can all trust

Etyczny, społecznie odpowiedzialny system rozpoznawania twarzy

Stanowisko firmy Thales

Wstęp

Rozpoznawanie twarzy to umiejętność, która pozwala nam funkcjonować w społeczeństwie i dbać o własne bezpieczeństwo. Chociaż się z nią rodzimy, nie wszyscy opanowujemy ją w tym samym stopniu. Według badań University of York człowiek rozpoznaje pięć tysięcy twarzy[1]. Wyjątkowe jednostki potrafią zapamiętać ich 10 tysięcy. Jednak nawet najzdolniejsi poprawnie zidentyfikują twarz na zdjęciu tylko w 80% przypadków.

Z naszych poszukiwań bezpiecznych i wygodnych metod identyfikacji ludzi wynika, że **rozpoznawanie twarzy to najmniej inwazyjna i najbardziej dostępna forma identyfikacji biometrycznej**: bezkontaktowa, szybka i niezawodna. 100 najlepszych algorytmów rozpoznawania twarzy wypróbowanych przez amerykańską agencję NIST w 2020 r. wykazało 95-procentową skuteczność w identyfikacji twarzy na zdjęciach.

Techniki rozpoznawania twarzy są nieustannie rozwijane, a aplikacje weryfikujące tożsamość – stale ulepszane. Zespoły badaczy opracowują coraz skuteczniejsze rozwiązania, łącząc specjalistyczną wiedzę w zakresie technologii weryfikacji tożsamości, biometrii i cyberbezpieczeństwa. Stają się one coraz lepsze pod względem dokładności, szybkości, najlepszych praktyk w zakresie ochrony prywatności, kwestii bezpieczeństwa, norm i komfortu użytkownika.

W niniejszym dokumencie przyglądamy się różnym aspektom tej fascynującej nowej technologii.

[1] Człowiek przeciętnie rozpoznaje 5 tys. twarzy – na podstawie badania University of York, 2018. *https://royalsocietypublishing.org/doi/full/10.1098/rspb.2018.1319*

Rozpoznawanie twarzy – najważniejsze informacje

Czym jest rozpoznawanie twarzy?

Rozpoznawanie twarzy to technologia, która ma za zadanie **automatycznie zidentyfikować osobę na podstawie jej twarzy, jeśli ta wcześniej pojawiła się w systemie. Jeśli w systemie nie ma wzorca w postaci zdjęcia danej osoby, jej identyfikacja tą metodą nie jest możliwa.** Początki techniki rozpoznawania twarzy sięgają lat 70. ubiegłego wieku, jednak w ostatnich latach dokonał się znaczący postęp dzięki komputerom o coraz większej mocy obliczeniowej, uczeniu maszynowemu i rozwojowi sztucznej inteligencji (AI).

Rozpoznawanie twarzy to **technologia biometryczna**, która wykorzystuje różne metody naukowe do identyfikacji i weryfikacji osób na podstawie analizy określonych cech fizycznych. Do innych często używanych modalności (cech) biometrycznych należą odciski palców, geometria dłoni, głos, tęczówka oka i DNA.

Jak komputer rozpoznaje twarz?

Systemy rozpoznawania twarzy nie porównują twarzy danej osoby do rzeczywistego zdjęcia: pobierają z niego najważniejsze cechy (tzw. „wektory") lub określone punkty danych na twarzy – rozstaw oczu, grzbiet nosa, osadzenie uszu czy przestrzeń między podbródkiem a ustami – tworząc unikalny wzorzec twarzy, który zostaje następnie zaszyfrowany. Zaszyfrowane dane pozyskane podczas rejestracji konkretnej osoby są przechowywane w formacie cyfrowym w postaci pliku referencyjnego lub referencyjnej bazy danych. Porównując twarz danej osoby w czasie rzeczywistym z wcześniej zarejestrowanym wizerunkiem, system jest w stanie je dopasować, oceniając jako wysokie prawdopodobieństwo, że w obu przypadkach jest to ta sama osoba.

Aby zostać zarejestrowane, początkowe zdjęcia twarzy muszą mieć określoną jakość i rozdzielczość. Wizerunki twarzy można pozyskiwać i rejestrować pojedynczo lub z galerii twarzy. Na podstawie wzorców przechowywanych w referencyjnej bazie danych nie można odtworzyć twarzy, ponieważ stanowią one zasadniczo jednokierunkową matematyczną interpretację oryginalnego wizerunku twarzy.

Dopasowanie twarzy to proces kilkuetapowy:

- Najpierw tworzy się cyfrowy wzorzec twarzy uwzględniający wszystkie najważniejsze cechy twarzy ze zdjęcia lub wizerunku danej osoby. Jest to tzw. **faza gromadzenia danych biometrycznych** lub faza rejestracji.
- Następnie w celu weryfikacji lub identyfikacji osoby **wykonuje lub pozyskuje się jej zdjęcie lub film.** W dalszej kolejności system przetwarza nowy wizerunek twarzy w oparciu o ten sam mechanizm, tworząc nowy wzorzec, który porównuje z referencyjną bazą wzorców. Osoba przesyłająca swój wizerunek twarzy zdalnie może wysłać selfie przez aplikację mobilną. Proces wykonania zdjęcia lub filmu powinien obejmować elementy detekcji żywotności, aby zapobiec *„spoofingowi"*, czyli oszustwu polegającemu na pokazaniu statycznego zdjęcia podczas zdalnej weryfikacji lub identyfikacji osoby.
- Następnie system rozpoznawania twarzy **porównuje nowo pobrany wizerunek twarzy z posiadanym wzorcem.** Jeśli między porównywaną twarzą a wzorcem zachodzi dostatecznie wysoka zgodność, osoba zostaje uznana za „rozpoznaną". W niektórych przypadkach system może znaleźć w galerii wzorców więcej niż jedno dopasowanie. System wyświetla pasujących kandydatów upoważnionej osobie w celu rozstrzygnięcia, które (o ile którekolwiek) dopasowanie jest tym właściwym.

Uwierzytelnianie a identyfikacja: czym się różnią i jak się ich używa?

Istnieją dwie możliwe metody rozpoznawania twarzy: uwierzytelnianie i identyfikacja.

Uwierzytelnianie (także: weryfikacja) ma potwierdzić tożsamość danej osoby – czy rzeczywiście jest tym, za kogo się podaje? Uwierzytelnianie polega na wykonaniu porównania 1:1 między nowym wizerunkiem danej osoby a własnym wzorcem referencyjnym – tj. osoby, za którą ta się podaje. Wymaga to wcześniejszej rejestracji i zgody weryfikowanej osoby. Weryfikacja ma na celu potwierdzenie, że twarz pokazywana w czasie rzeczywistym należy do tej samej osoby, która została wcześniej zarejestrowana w bazie. Na co dzień uwierzytelnianie jest często wykorzystywane m.in. do odblokowywania smartfonów.

Identyfikacja to proces ustalania tożsamości – kim jest dana osoba? W procesie identyfikacji zdjęcie lub film danej osoby porównuje się z bazą wzorców twarzy w celu znalezienia dopasowania – jest to tak zwana „identyfikacja 1:n", gdzie „n" oznacza całkowitą liczbę wzorców w bazie danych.

Rozpoznawanie twarzy: różne zastosowania

Rozpoznawanie twarzy – uwierzytelnianie, identyfikacja lub połączenie obu – może być wykorzystywane na wiele różnych sposobów i przynosi wiele korzyści stosującym je organizacjom i przedsiębiorstwom, a także osobom korzystającym z tej nieinwazyjnej, bezkontaktowej technologii.

- Kontrola dostępu: zapewnia łatwiejszy i bezpieczniejszy dostęp do stref ograniczonych (obiekty biurowe, imprezy sportowe, magazyny itp.).
- Lotniska/podróżowanie: systemy rozpoznawania twarzy przy stanowiskach odprawy biletowo-bagażowej, kontroli granicznej, bramkach na lotnisku itp. ułatwiają przekraczanie granicy i wejście na pokład samolotu.
- Weryfikacja tożsamości: rozpoznawanie twarzy zwiększa bezpieczeństwo korzystania z usług cyfrowych, ograniczając ryzyko oszustwa lub kradzieży tożsamości (np. zdalne potwierdzenie tożsamości przy rejestracji w serwisach internetowych, zdalne wdrażanie klientów itp.).
- Organy ścigania (tworzenie listy podejrzanych o popełnienie przestępstwa). Obok materiału dowodowego w postaci DNA i odcisków palców niektóre organy ścigania wykorzystują systemy rozpoznawania twarzy do tworzenia listy podejrzanych o popełnienie przestępstwa – jeśli istnieje nagranie wideo ze zdarzenia. W przeciwieństwie do DNA i odcisków palców rozpoznanie twarzy nie może być podstawą skazania oskarżonego. Może służyć wyłącznie do tworzenia listy podejrzanych, pozwalając organom ścigania zawęzić poszukiwania i szybciej znaleźć sprawcę. W wielu systemach prawnych może zaistnieć potrzeba przyjęcia nowych lub zmiany istniejących przepisów, aby zapobiec naruszaniu swobód obywatelskich.
- Nadzór (lokalizacja, możliwa identyfikacja i śledzenie danej osoby w czasie rzeczywistym). Z uwagi na gwałtowny wzrost liczby kamer na całym świecie, organy władzy mają możliwość identyfikacji i śledzenia na bieżąco ruchów poszczególnych osób. Zastosowanie to (słusznie) budzi obawy dotyczące swobód obywatelskich i prywatności. Z technologii rozpoznawania twarzy w tym celu powinno się korzystać wyłącznie po przyjęciu stosownych przepisów, które zapewniałyby równowagę między prawami jednostki a dobrem wspólnym. W tym zakresie systemy rozpoznawania twarzy przynoszą ogromne korzyści, pomagając organom odnaleźć zaginione dzieci, osoby o ograniczonych zdolnościach poznawczych, uprowadzone itp.

Korzystanie z technologii rozpoznawania twarzy do nadzoru w czasie rzeczywistym lub tworzenia listy podejrzanych może wymagać przyjęcia ram prawnych, które zapewniałyby poszanowanie prywatności jednostek i swobód obywatelskich – może to jednak zależeć od danej sytuacji, kraju lub systemu prawnego.

Krótsze kolejki, większe bezpieczeństwo: rozpoznawanie twarzy na lotnisku i w firmie

Rozpoznawanie twarzy przydaje się w rozmaitych sytuacjach, zwłaszcza jeśli chodzi o przemieszczanie się dużych grup ludzi i wynikające stąd kwestie bezpieczeństwa i kontroli.

Na przykład niedawno na paryskich lotniskach pod zarządem Aéroport de Paris podjęto decyzję o zastąpieniu odcisków palców technologią rozpoznawania twarzy. Po jej całkowitym wdrożeniu z przyspieszonej procedury kontroli skorzysta 45% ze 100 mln pasażerów obsługiwanych przez Aéroport de Paris rocznie (obecnie jest to 10%). Posiadacze paszportów elektronicznych okazują je przy e-bramce, gdzie są automatycznie skanowane. Otwierają się pierwsze drzwi, a pasażer pokazuje twarz do kamery. Obraz porównywany jest z danymi przechowywanymi w układzie scalonym paszportu. W ciągu kilku sekund pasażer przekracza granicę, w razie wszelkich nieprawidłowości władze otrzymują ostrzeżenie, a komfort przemieszczania się po lotnisku wzrasta.

W ten sposób rozpoznawanie twarzy może zwiększyć bezpieczeństwo i wygodę wszystkich. Technologia oznacza:

- **Prostszą i szybszą kontrolę dostępu.** Technologia rozpoznawania twarzy jest bezpieczniejsza niż tradycyjne identyfikatory (które można ukraść lub zgubić) oraz szybsza i mniej inwazyjna niż inne technologie biometryczne, takie jak analiza odcisków palców czy rozpoznawanie tęczówki;
- **Sprawniejsze wejście na pokład dzięki** automatycznej kontroli i weryfikacji osób niepożądanych stanowiących zagrożenie bezpieczeństwa, poprzez użycie twarzy pasażera jako „biletu";
- **Zautomatyzowany dostęp do** usług lub sprzętu przypominający odblokowanie smartfona poprzez rozpoznanie twarzy użytkownika;
- **Monitoring w czasie rzeczywistym** pozwalający na identyfikację i lokalizację osób w tłumie (osób poszukiwanych, zaginionych dzieci itp.);
- **Niezawodną kontrolę tożsamości** w połączeniu z paszportami elektronicznymi, w których również przechowywane są dane o twarzy: praktycznie uniemożliwia to kradzież tożsamości;
- **Alternatywne i bardziej wydajne rozwiązanie wobec kontroli** identyfikatorów lub odcisków palców: brak konieczności posiadania identyfikatora, fizycznej kontroli przez służbę ochrony lub w automatycznym terminalu, brak możliwości pożyczenia identyfikatora itp.;
- **Zastosowania komercyjne** (zakupy, płatności itp.)...

Technologia rozpoznawania twarzy wykorzystywana na lotniskach ma także inne przydatne zastosowania: umożliwia kontrolę dostępu do lokalizacji o wyższym poziomie bezpieczeństwa i wejść na imprezy masowe czy sprawdzanie tożsamości w dużych obiektach firmowych. Dzięki niej przedsiębiorstwa mogą zapewnić dostęp do określonych stref wyłącznie upoważnionym pracownikom, kontrolować osoby przychodzące do pracy i wychodzące z niej, a także usprawnić procedury bezpieczeństwa z korzyścią dla wszystkich. Dane nie muszą opuszczać urządzenia kontrolującego, a szyfrowanie dodatkowo zwiększa ich bezpieczeństwo, pozwalając uspokoić uzasadnione obawy o swobody obywatelskie.

Na lotniskach wyposażonych w systemy rozpoznawania twarzy kontrola graniczna zajmuje zaledwie 10-15 sekund! [1]

[1] La Tribune

Wydajność i komfort w jednym

Obecnie technologia rozpoznawania twarzy jest **dojrzała, niezawodna, bardzo dokładna i szybka.**

- **W porównaniu z innymi systemami biometrycznymi zasadniczo nie wymaga kontaktu fizycznego.** W przeciwieństwie do rozpoznawania odcisków palców nie budzi obaw natury zdrowotnej, ponieważ **nie wymaga fizycznego dotknięcia** czytnika. W przeciwieństwie do analizy DNA metoda jest **nieinwazyjna** i nie wymaga pobierania próbek. Jest **ergonomiczna, przyjazna w użytkowaniu** i zapewnia użytkownikowi najwyższy poziom komfortu. W odróżnieniu od systemów rozpoznawania tęczówki nie wymaga ustawienia się dokładnie przed czytnikiem. W przeciwieństwie do innych technologii (np. rozpoznawania podpisów) nie wymaga podjęcia żadnych konkretnych działań przez osobę sprawdzaną.
- **W znacznej mierze zapobiega oszustwom i kradzieży tożsamości** – w odróżnieniu od np. systemów wykorzystujących identyfikatory.
- **Jest prosta i łatwa w konfiguracji** zarówno dla zespołu informatycznego, jak i pracowników ochrony obiektu. Można ją łatwo zintegrować i wdrożyć zarówno w nowych lokalizacjach, jak i w ramach istniejących systemów nadzoru.

  W dodatku wraz z jej upowszechnieniem jest stale ulepszana: dzięki uczeniu maszynowemu rozpoznawanie twarzy staje się coraz dokładniejsze, czerpiąc z coraz większego zbioru danych. Dziesięć najlepszych algorytmów wypróbowanych przez amerykańską agencję NIST w 2020 r. wykazało ponad 98-procentową skuteczność w weryfikacji 1:1, a pięć najlepszych – ponad 99-procentową.

Przeszkody na horyzoncie!

Systemy rozpoznawania twarzy już teraz są dużo dokładniejsze od ludzi – są także znacznie sprawniejsze i pewniejsze. W dodatku cały czas są ulepszane: eksperci zapowiadają, że ich skuteczność w ciągu najbliższych czterech lat wzrośnie aż dwukrotnie! O ile technologie te już teraz znajdują szereg zastosowań przynoszących istotne korzyści, w przyszłości ich wykorzystanie tylko wzrośnie. Mimo to pojawiają się różne obawy (niekiedy jak najbardziej uzasadnione), którymi można tłumaczyć, dlaczego technologia rozpoznawania twarzy nie rozwija się tak szybko, jak mogłyby wskazywać na to jej skuteczność i siła.

Brak zaufania społecznego

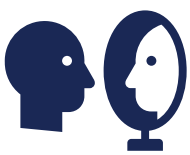
Jako ludzie często jesteśmy nieufni wobec nowych technologii – tym bardziej jeśli nie rozumiemy ich działania. Dlatego o ile wiele osób oswoiło się już z funkcją rozpoznawania twarzy, która pozwala im łatwo i sprawnie odblokować smartfona, niepokoją ich kwestie związane z ich prywatnością. Ściślej mówiąc, obawiają się możliwego bezprawnego gromadzenia i wykorzystywania ich danych biometrycznych.

Część wspomnianych obaw mogłaby rozwiać szeroka komunikacja zasad działania technologii rozpoznawania twarzy. Należy zaznaczyć, że technologie biometryczne nie muszą oznaczać scentralizowanej bazy danych. Na przykład **w paszporcie elektronicznym** zdjęcie twarzy jest **przechowywane lokalnie**, umożliwiając uwierzytelnienie jego właściciela przez system rozpoznawania twarzy. W trakcie elektronicznej identyfikacji w punkcie kontroli granicznej na lotnisku dane nie opuszczają lokalnego systemu.

Patrząc jednak szerzej, powyższe obawy świadczą o konieczności ustanowienia jasno określonych **ram prawnych** i stosowania metod rozpoznawania twarzy w ścisłej zgodności z nimi.

Obawy o „różnice statystyczne”

Opór wobec technologii rozpoznawania twarzy wynika głównie z obaw związanych z naruszeniem swobód obywatelskich i prywatności. Jednak to nie sama technologia jest zagrożeniem, lecz jej nieodpowiednie użycie. Dlatego priorytetem jest opracowanie przepisów i zasad, które zapewniałyby równowagę między ochroną swobód obywatelskich i prywatności a dobrem wspólnym.



Jak już wspomniano, wiele krajów rozważa przyjęcie ram prawnych i przepisów dotyczących metod nadzoru i ich stosowania przez organy ścigania, które chroniłyby prawa indywidualne.

Częste obawy budzą także kwestie dotyczące etyki i sprawiedliwości. Są to w szczególności:

- Obawy o dyskryminację – przeciwnicy twierdzą, że skuteczność technologii może zależeć od płci lub pochodzenia etnicznego danej osoby;
- Obawy o błędną identyfikację (fałszywe dopasowanie) i jej możliwe nieokreślone konsekwencje.

Powyższe twierdzenia w dużej mierze opierają się na wynikach starszych testów, w których wykorzystywano ograniczone i niereprezentatywne zbiory danych. Jednak ostatnie postępy w technologii rozpoznawania twarzy znacząco zmniejszyły zakres tych „różnic statystycznych". Wraz z ciągłą rozbudową zbiorów danych rośnie dokładność technologii. Coraz lepsze stają się także wzorce twarzy: wybierane cechy i kąty są bardziej neutralne. Według publikacji NIST „Face Recognition Vendor Test: Part 3: Demographics Effect" z grudnia 2019 r., zachodzi bezpośrednia korelacja między skutecznością algorytmów a danymi znajdującymi się w bazie.

Aby ograniczyć różnice statystyczne, bazy danych wymagają zróżnicowanego i reprezentatywnego zbioru danych. Z badania przeprowadzonego przez National Institute of Standards and Technology wynika, że wyniki są bardzo spójne, jeśli twarz kandydata porównuje się ze zbiorem danych osób z tego samego kraju, tej samej płci i pochodzenia etnicznego oraz w tym samym wieku. W badaniu sprawdzano działanie systemu mającego rozpoznać, czy dana osoba pochodzi z Rosji, Somalii czy Wietnamu. Okazało się, że kiedy algorytm porównywał starszą Rosjankę z bazą danych pochodzących głównie spoza Rosji, wyniki dopasowania były znacznie gorsze. Aby zapewnić niezawodność wyników niezależnie od pochodzenia etnicznego, wieku i płci, należy przede wszystkim wprowadzić do systemu rozbudowaną, różnorodną bazę danych.

Więcej informacji o badaniu można znaleźć w następującej publikacji National Institute of Standards and Technology: *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*

Brak przejrzystości

Kolejna obawa dotyczy technicznej możliwości stosowania systemu rozpoznawania twarzy bez naszej wiedzy w miejscach publicznych i prywatnych. Należy zauważyć, że już teraz nadzór wideo występuje powszechnie zarówno w przestrzeni publicznej, jak i prywatnej. Problem braku przejrzystości pojawia się w sytuacji, w której takie systemy zostają wyposażone w funkcję rozpoznawania twarzy w czasie rzeczywistym.

W kwestiach dotyczących nadzoru **Thales opowiada się za ochroną praw indywidualnych przez ustawodawcę** poprzez stanowienie przepisów regulujących użycie systemów bezpieczeństwa i podawanie do wiadomości publicznej informacji o miejscach i sytuacjach, w których tego rodzaju rozwiązania są stosowane.

Rozpoznawanie twarzy a ramy prawne

W Unii Europejskiej, Azji i Stanach Zjednoczonych technologię rozpoznawania twarzy regulują bardzo odmienne ramy prawne, które w dodatku ulegają ciągłym zmianom.

Unia Europejska: jednolite ramy prawne dla 500 mln obywateli

Od 2018 r. na całym terytorium Unii Europejskiej obowiązuje RODO (rozporządzenie o ochronie danych osobowych), które określa wytyczne dotyczące ochrony danych osobowych – w tym danych biometrycznych – w ustawodawstwie krajowym. RODO dotyczy **500 mln obywateli UE w 28 państwach** (Wielka Brytania utrzymała je w mocy mimo brexitu). Rozporządzenie przewiduje:

- **„Dobrowolne, konkretne, świadome i jednoznaczne" przyzwolenie** użytkownika na przetwarzanie jego danych osobowych;
- **„Prawo do bycia zapomnianym"**, czyli prawo użytkownika do zażądania od organizacji usunięcia jego danych osobowych;
- **Szereg obowiązków dotyczących bezpieczeństwa,** m.in. obowiązek poinformowania zainteresowanych użytkowników w przypadku wykrycia naruszenia bezpieczeństwa bazy danych.

Mimo to instytucje nadzorujące technologię cyfrową z różnych krajów wskazują na możliwość przyjęcia przepisów dotyczących konkretnie systemów rozpoznawania twarzy, które wykraczałyby poza ramy prawne regulujące gromadzenie danych osobowych. Sprawę tak skomentowała francuska Komisja ds. Wolności oraz Informatyki (fr. Commission nationale de l'informatique et des libertés, CNIL): „Technologia rozpoznawania twarzy wymaga politycznych wyborów: w sprawie roli technologii, jej wpływu na podstawowe wolności jednostki i ludzkość w epoce cyfrowej."

Stany Zjednoczone: mozaika przepisów i różnice między stanami

W Stanach Zjednoczonych poszczególne stany lub miejscowości przyjęły określone przepisy regulujące użycie lub zakazujące stosowania biometrii ogółem lub samej technologii rozpoznawania twarzy przez agencje rządowe lub prywatne przedsiębiorstwa.

- W niektórych regionach i stanach istnieją przepisy dotyczące wykorzystywania danych biometrycznych.
- W pozostałych stanach można zgodnie z prawem korzystać z oprogramowania identyfikującego osoby za pomocą obrazów zarejestrowanych bez ich zgody w przestrzeni publicznej.
- Niektóre amerykańskie miasta wprowadziły zakaz korzystania z technologii rozpoznawania twarzy przez organy ścigania zarówno w przestrzeni publicznej, jak i prywatnej.

Obecnie wiele podmiotów zainteresowanych (dostawcy i użytkownicy systemów rozpoznawania twarzy, organizacje szczebla lokalnego lub federalnego itd.) domaga się od rządu federalnego wyraźnego określenia kierunku polityki, który pozwoliłby stanom i jednostkom administracji lokalnej na podstawie jasno zdefiniowanych i wspólnych ram prawnych opracować własne przepisy.

Korzystanie z systemów rozpoznawania twarzy w sposób odpowiedzialny społecznie

Rozpoznawanie twarzy to część naszej przyszłości. Jednak niektórzy obawiają się nadużyć technologii rozpoznawania twarzy - mamy tego świadomość. Rozwiązania Thales powstają z myślą o **rygorystycznych zasadach etycznych.** Specjalizujemy się nie tylko w biometrii, ale także w cyberbezpieczeństwie. W połączeniu z podejściem Thales TrUE AI (2) nasza obszerna wiedza pozwala nam **tworzyć całościowe i bezpieczne rozwiązania, które zapewniają poufność i spójność danych, a także bezpieczne przechowywanie danych biometrycznych.**

Szersze wykorzystanie technologii rozpoznawania twarzy wydaje się nieuniknione, ponieważ jest to niezawodne i wydajne rozwiązanie, które łatwo wdrożyć i które nie wymaga użycia określonych czujników. A przede wszystkim może przysłużyć się ludziom na wiele sposobów. Zadbajmy o to, żeby odbywało się to na jak najlepszych warunkach, zwłaszcza w obszarach wrażliwych, takich jak bezpieczeństwo, zdrowie czy handel. W przyszłości mogą pojawić się nowe zastosowania technologii rozpoznawania twarzy, których jeszcze nie potrafimy sobie wyobrazić: jeszcze kilka lat temu **kto by pomyślał, że będziemy ją stosować w rolnictwie w celu lepszej identyfikacji krów i świń?**

(2) Podejście Thales TrUE AI oznacza „Transparent, Understandable and Ethical Artificial Intelligence", czyli „przejrzystą, zrozumiałą i etyczną sztuczną inteligencję". Przejrzystą sztuczną inteligencję, pozwalającą użytkownikom prześledzić dane, na podstawie których zostały wyciągnięte wnioski. Zrozumiałą sztuczną inteligencję, która pozwala wyjaśnić i uzasadnić otrzymane wyniki, i wreszcie etyczną sztuczną inteligencję zgodną z obiektywnymi normami, protokołami, przepisami i prawami człowieka. *https://www.thalesgroup.com/en/journalist/thales-podcasts*

Wszystkie nasze rozwiązania projektujemy zgodnie z rygorystycznymi zasadami etycznymi

W Thales wychodzimy z założenia, że systemy rozpoznawania twarzy muszą powstawać zgodnie z kilkoma podstawowymi zasadami.

- **Poufność i zgoda.** Konfiguracja systemu rozpoznawania twarzy wiąże się z gromadzeniem danych biometrycznych osób. Proces ten wymaga wyraźnej zgody wszystkich zainteresowanych. Należy zagwarantować poufność danych i chronić je przed wszelkimi przypadkami niezamierzonego i nieuzgodnionego ich wykorzystania.
- **Przejrzystość.** Wdrażaniu systemów rozpoznawania twarzy musi towarzyszyć całkowita przejrzystość. Osoby, których dane dotyczą, muszą mieć dostęp do opisu metod gromadzenia, przechowywania i wykorzystywania danych biometrycznych oraz okresu przechowywania informacji na ich temat.
- **Precyzja i niezawodność.** Systemy rozpoznawania twarzy muszą gwarantować maksymalną precyzję i niezawodność. Muszą opierać się na algorytmach przetwarzających bardzo różnorodny zbiór danych i być wrażliwe na wszelkie szczegóły widoczne na zarejestrowanym obrazie (okulary, czapka, szalik itp.).
- **Bezpieczeństwo.** Systemy rozpoznawania twarzy powinny z założenia zapewniać całkowite bezpieczeństwo gromadzonych i przechowywanych danych osobowych i biometrycznych. Zarejestrowane dane biometryczne powinny być zaszyfrowane zarówno w czasie ich przesyłania, jak i podczas przechowywania.
- **Etyka i zgodność.** Systemy rozpoznawania twarzy muszą być projektowane i wdrażane w całkowitej **zgodności z normami rynkowymi oraz zobowiązaniami nałożonymi przez organy regulacyjne i ustawodawstwo.** Powinny być zgodne ze standardowymi i obiektywnymi protokołami, przepisami i prawami człowieka.
- **Odpowiedzialność.** Dostawcy technologii muszą zapewnić klientom długofalowe wsparcie, oferując zrównoważone rozwiązania techniczne dostosowane do obecnych i przyszłych potrzeb.

Thales jest członkiem wielu stowarzyszeń i grup branży biometrycznej, m.in. Biometrics Institute czy International Biometric and Identity Association.

Biometrics Institute

International Biometric and Identity Association

Aby dowiedzieć się więcej na temat technologii rozpoznawania twarzy Thales,

prosimy o kontakt z Kadie-Ann Fyffe,

specjalistą ds. komunikacji w dziale Identity & Biometric Solutions

E-mail : kadie-ann.fyffe@thalesgroup.com

THALES

Building a future we can all trust

thalesgroup.com