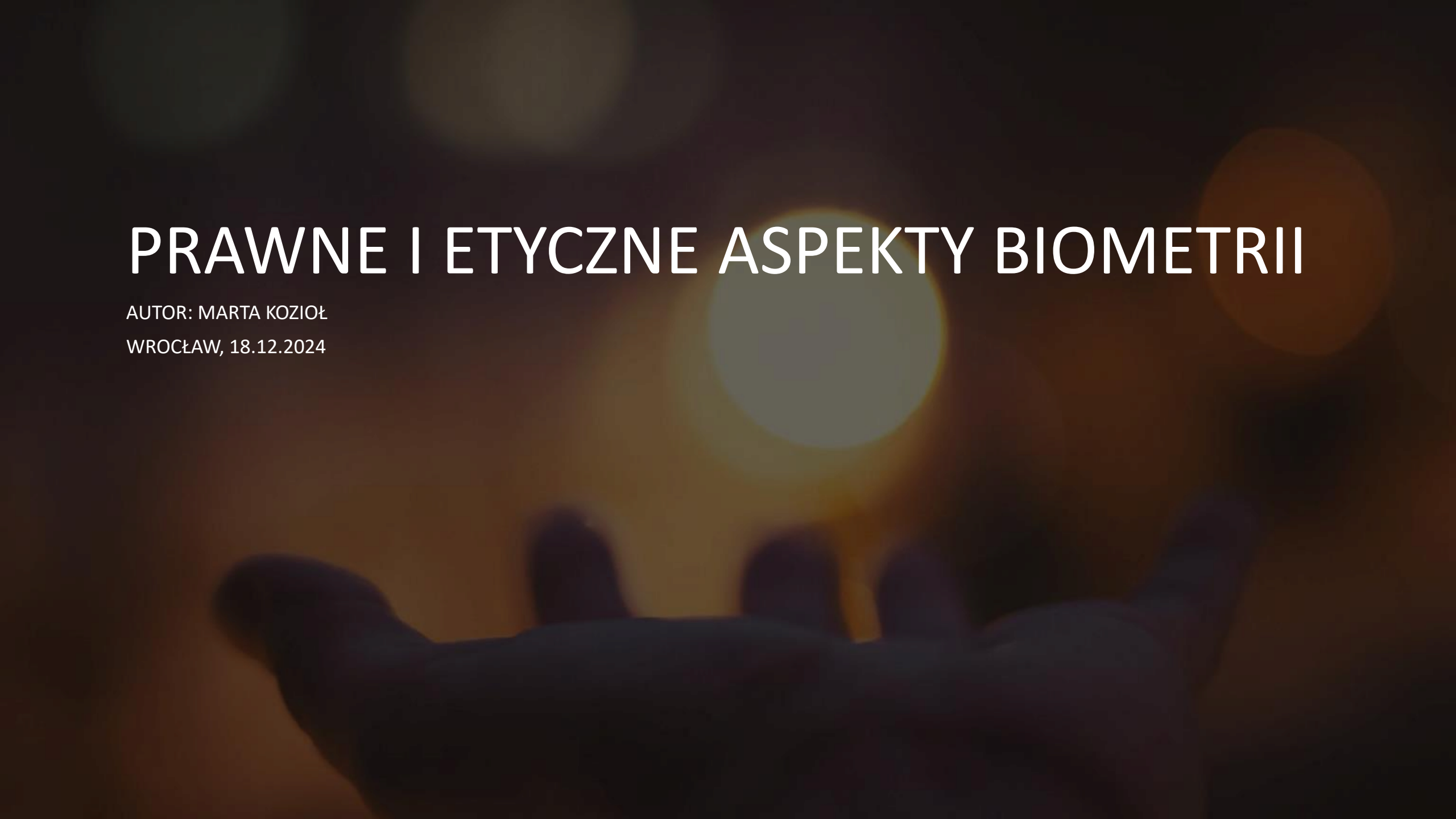
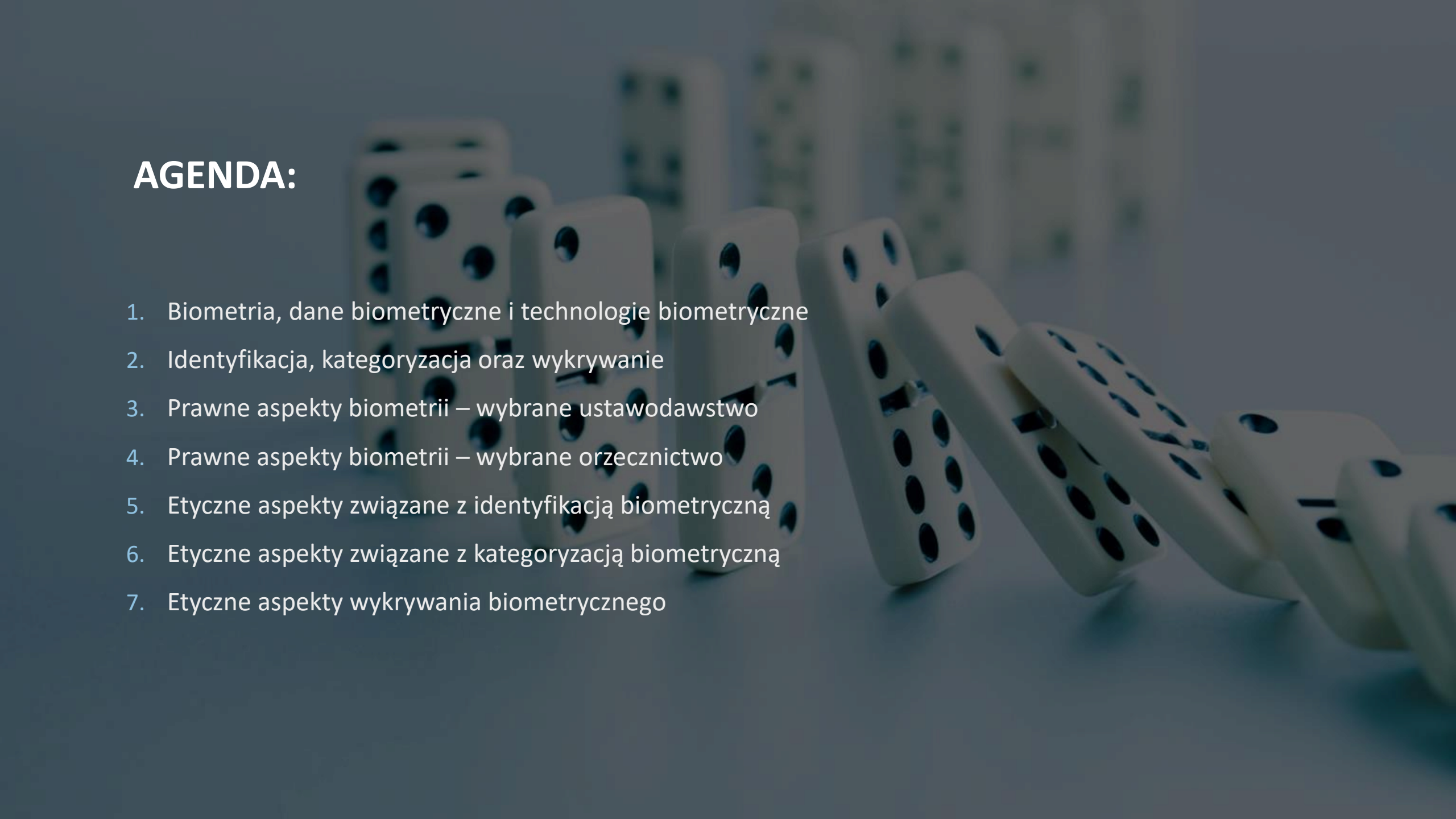
PRAWNE I ETYCZNE ASPEKTY BIOMETRII

AUTOR: MARTA KOZIOŁ

WROCŁAW, 18.12.2024





AGENDA:

1. Biometria, dane biometryczne i technologie biometryczne
2. Identyfikacja, kategoryzacja oraz wykrywanie
3. Prawne aspekty biometrii – wybrane ustawodawstwo
4. Prawne aspekty biometrii – wybrane orzecznictwo
5. Etyczne aspekty związane z identyfikacją biometryczną
6. Etyczne aspekty związane z kategoryzacją biometryczną
7. Etyczne aspekty wykrywania biometrycznego

BIOMETRIA
DANE BIOMETRYCZNE
I TECHNOLOGIE BIOMETRYCZNE

jest połączeniem dwóch słów z języka greckiego: ***bios*** – życie, natomiast ***metron*** – mierzyć
nauka, która wykorzystując zasady statystyki matematycznej i **opisuje zmienność cech populacji organizmów żywych**

BIOMETRIA

użycie specyficznych atrybutów odzwierciedlających unikalne cechy osoby, takie jak: odcisk linii papilarnych palca, struktura układu żył (palca, nadgarstka), cechy charakterystyczne głosu **w celu potwierdzenia tożsamości osoby**

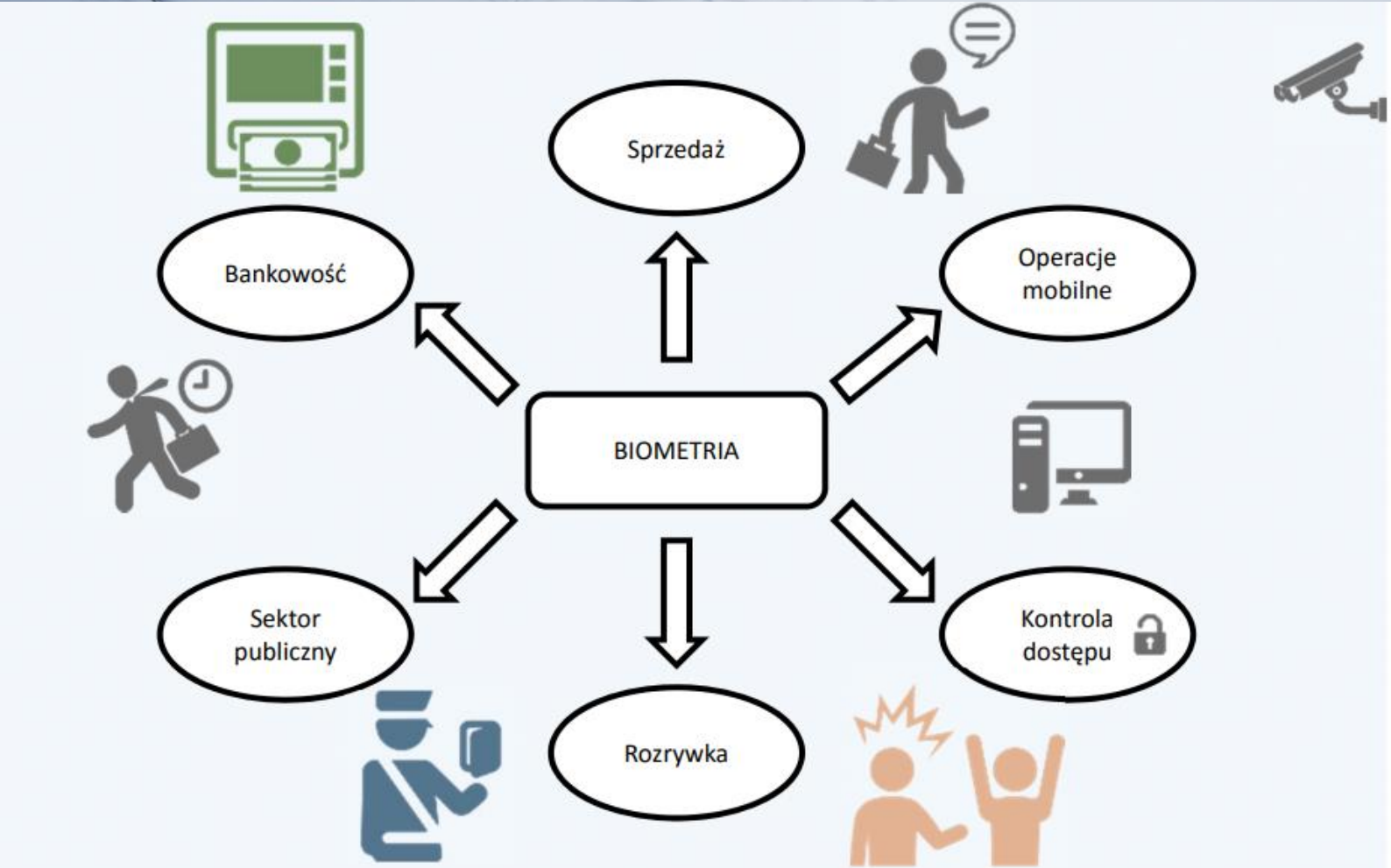
Norma ISO/IEC 2382:2015 Information technology – Vocabulary

system, którego zadaniem jest **automatyczne rozpoznanie lub uwierzytelnienie osoby fizycznej** na podstawie jej cech biologicznych lub behawioralnych.

Norma ISO/IEC 24745:2011 Information technology – Security techniques – Biometric information protection

SYSTEM BIOMETRYCZNY

OBSZARY ZASTOSOWAŃ BIOMETRII



Źródło: Przegląd technologii biometrycznych, A. Czyżewski, P. Hoffmann

DANE BIOMETRYCZNE

właściwości biologiczne, cechy fizjologiczne, cechy życiowe lub powtarzalne czynności, przy czym te cechy i/lub czynności dotyczą wyłącznie danej osoby, a jednocześnie są wymierne, nawet jeżeli schematy używane w praktyce do ich pomiaru charakteryzuje pewien stopień prawdopodobieństwa

Opinia 4/2007 Grupy Roboczej Art. 29 (WP136)

dane osobowe, które **wynikają ze specjalnego przetwarzania technicznego** dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz **umożliwiają lub potwierdzają jednoznaczną identyfikację** tej osoby, takie jak: wizerunek twarzy lub dane daktyloskopijne

Art. 4 pkt 14 RODO

informacje wyodrębnione **z próbki biometrycznej** i stosowane do **utworzenia wzorca odniesienia** albo **wzorca dopasowywania**

PN-ISO 19092:2008

FORMY WYSTĘPOWANIA DANYCH BIOMETRYCZNYCH

Dane biometryczne wykorzystywane w systemach biometrycznych do identyfikacji lub weryfikacji osób mogą występować w formie przetworzonej lub nieprzetworzonej, tzw. surowej.

Surowe dane biometryczne

nieprzetworzone cyfrowe dane biometryczne pobrane z urządzenia pomiarowego (np. obraz odcisku palca, lub strumień audio), nadające się do późniejszego przetwarzania **w celu utworzenia próbki biometrycznej lub wzorca.**

Wzorzec odniesienia

dane reprezentujące miary biometryczne zarejestrowanej osoby, wyodrębnione z próbki biometrycznej zarejestrowanej osoby, zazwyczaj przechowywane w systemie biometrycznym i stosowane przez system biometryczny **w celu sprawdzenia zgodności z przedkładanymi później wzorcami dopasowania.**

Wzorzec dopasowania

dane reprezentujące miary biometryczne osoby, wyodrębnione z próbki biometrycznej **w celu porównania z wzorcami odniesienia.**

obejmują **wszelkie technologie lub operacje**,

które polegają **na określonym technicznym przetwarzaniu danych** odnoszących się do **fizycznych, fizjologicznych lub behawioralnych** aspektów ludzkiego ciała (w tym w ruchu);

dla celów:

- **uwierzytelnianie/identyfikacji** osób;
- **kategoryzacji** jednostek ludzkich według stałych lub długookresowych charakterystycznych cech (w tym: w celu przewidywania przyszłych zachowań);
- **wykrywania** chwilowych lub stałych **stanów człowieka** (takich jak: strach, zmęczenie lub choroba).

EP Study on Biometric Recognition and Behavioural Detection

TECHNOLOGIE BIOMETRYCZNE

TECHNIKI BIOMETRYCZNE

Biometria odcisku palca	*Biometria tęczówki*	*Biometria siatkówki*	*Biometria podpisu*	*Biometria głosowa*
Biometria kształtu ucha	*Biometria kształtu twarzy*	*Biometria chodu*	*Biometria układu żył*	*DNA*

TECHNOLOGIE BIOMETRYCZNE

można podzielić m.in. z uwagi **na identyfikatory: silne, słabe i miękkie**.

- **Silna biometria** umożliwia lub potwierdza jednoznaczną identyfikację osoby fizycznej, np. *odciski palców, biometrię tęczówki, siatkówki*
- **Słaba biometria** to cechy, które są mniej wyjątkowe lub mniej stabilne, np. *kształt ciała, wzorce behawioralne, głos*
- **Miękka biometria** obejmuje cechy, które są ogólne w charakterze i nie są jednoznacznie związane z osobą, np. *płeć lub wiek*

Nowoczesne technologie biometryczne **umożliwiają konwersję analogowo-cyfrową** i **automatyczne przetwarzanie** identyfikatorów biometrycznych.

TECHNOLOGIE BIOMETRYCZNE

można również podzielić m.in. na **pierwszą i drugą generację.**

Pierwsza generacja:

- Skoncentrowana na silnej biometrii i unikalności identyfikacji lub uwierzytelnienia poszczególnych osób.
- Pierwsze przypadki użycia na dużą skalę zaczęły się pod koniec lat 90. w USA, a rozwój nastąpił po atakach terrorystycznych w 2001 r. i wprowadzeniu paszportów biometrycznych zawierających odciski palców i dane twarzy
- Biometria pierwszej generacji stała się bardziej niezawodna i zaawansowana
- Biometria rozwinęła się w narzędzie do szybkiej i niezawodnej identyfikacji lub uwierzytelniania z szeroką gamą kontekstów, w tym do celów egzekwowania prawa, głosowania wyborczego, a nawet do systemu oceny społecznej
- Techniki te zastępują tradycyjne hasła jako środek bezpieczeństwa z najnowszymi technologiami rozpoznawania twarzy umożliwiając identyfikację w czasie krótszym niż jedna sekunda

TECHNOLOGIE BIOMETRYCZNE

Druga generacja:

- Skupia się na słabej biometrii od zdolności motorycznych po mowę ciała, chód i interakcje
- Powszechnie określana jako „biometria behawioralna", ponieważ analizowane jest cyfrowe, fizyczne i poznawcze zachowanie ludzi, a nie statyczne cechy, takie jak odciski palców
- Wykorzystywane przez sektor prywatny np. jako ukierunkowany marketing, wykrywanie zmęczenia lub senność podczas jazdy, a także diagnostyka medyczna
- Oferuje nowe możliwości organom ścigania i kontroli granicznej, umożliwiając m.in. w celu wykrycie osób o podejrzanym zachowaniu mogących wskazywać na zamiary popełnienia przestępstwa

Granice między technologiami pierwszej i drugiej generacji mogą jednak ulec zatarciu, w szczególności behawioralne i emocjonalne systemy, które w dużym stopniu opierają się na technologii rozpoznawania twarzy.


IDENTYFIKACJA
WERYFIKACJA
KATEGORYZACJA
WYKRYWANIE BIOMETRYCZNE

IDENTYFIKACJA ORAZ WERYFIKACJA BIOMETRYCZNA

Identyfikacja - metoda identyfikacji lub potwierdzania tożsamości osoby na podstawie: unikalnych cechy fizycznych, fizjologicznych lub behawioralnych danej osoby z innymi wzorcami biometrycznymi zgromadzonymi w bazie danych **w celu ustalenia tożsamości**

Porównanie wzorców vs dane użytkownika (N:1)

Weryfikacja – wskazanie po danych konkretnego użytkownika, a następnie porównaniu wskazanego identyfikatora ze wzorcem zapisanym w bazie **w celu potwierdzenia tożsamości**

Porównanie wzorca vs dane użytkownika (1:1)

IDENTYFIKACJA

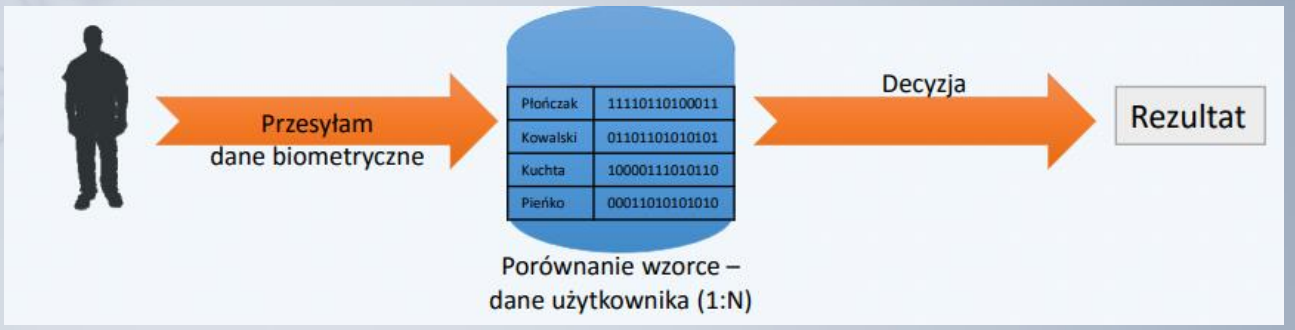
analiza cech użytkownika, a następnie porównanie ich ze wszystkim dostępnymi wzorcami w bazie

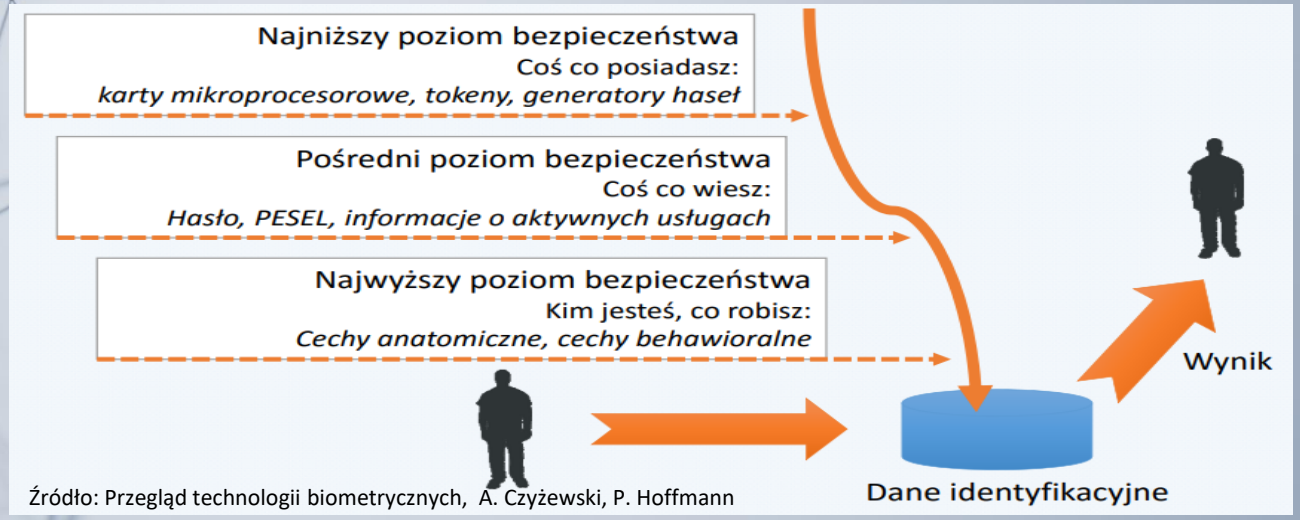
WERYFIKACJA

przedstawienie się użytkownika, a następnie porównaniu wskazanego identyfikatora ze wzorcem zapisanym w bazie

UWIERZYTELNIANIE

proces weryfikacji tożsamości użytkownika, sprawd zenie, kontrola zgodności z prawdą, określenie aute ntyczności, stwierdzenie, poświadczenie prawdziwo ści również z uwzględnieniem określonego prawdopodobieństwa





Źródło: Przegląd technologii biometrycznych, A. Czyżewski, P. Hoffmann

KATEGORYZACJA BIOMETRYCZNA

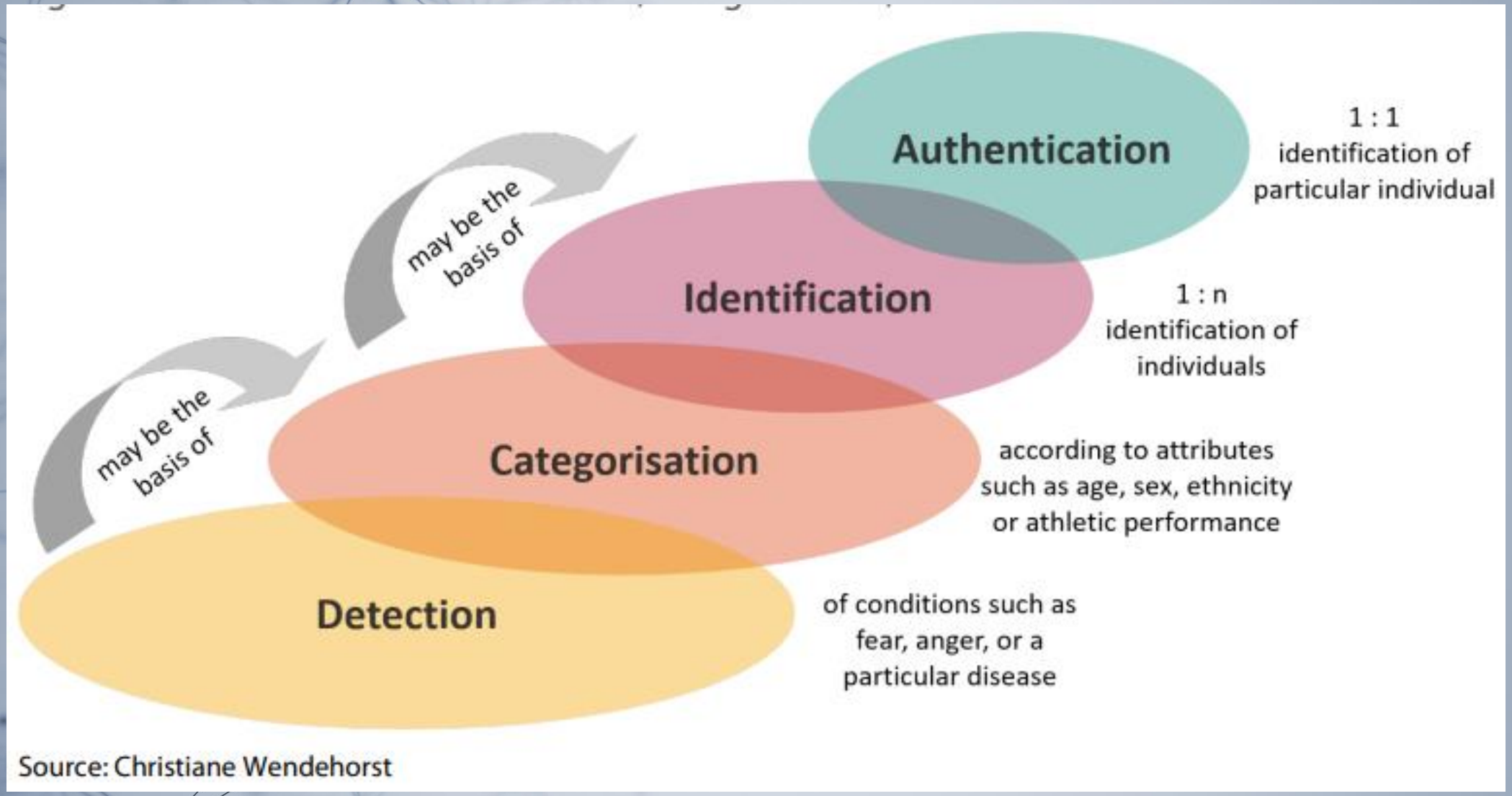
- Dane, które jako takie nie są właściwe do jednoznacznej identyfikacji osoby mogą być **wykorzystane do przyporządkowania** tej osoby do **określonych kategorii**, takich jak: płeć, wiek, pochodzenie etniczne, poglądy polityczne lub religijne, czy stan zdrowia
- Wzrost technik kategoryzacji biometrycznej nastąpił wraz ze wzrostem wykorzystania technologii biometrycznych słabych i miękkich
- W przypadku, gdy konkretna osoba jest przypisana do kilku różnych kategorii to, to łączne przypisanie **może** - w zależności od okoliczności, takich jak liczba i szczegółowość kategorii - **umożliwić lub potwierdzić identyfikację tej osoby fizycznej**

WYKRYWANIE BIOMETRYCZNE

Może być używane w odniesieniu do wielu technik biometrycznych, których **celem jest wykrycie pewnych ludzkich stanów**, takich jak: gniew, strach, konkretna intencja (np. do popełnienia przestępstwa) lub określona choroba

Pojawiły się **systemy rozpoznawania emocji**, czyli systemy identyfikacji lub wnioskowania z emocji, myśli lub intencji osób na podstawie biosygnałów, które wiążą się z szeregiem problemów etycznych

Wraz z rosnącym wykorzystaniem słabej i/lub miękkiej biometrii oraz coraz szerszej gamy biosygnałów i cech behawioralnych, które mogą być wyczuwane i analizowane za pomocą maszyn coraz trudniej jest wyznaczyć wyraźną granicę między technikami biometrycznymi a innymi formami np. profilowania osób



Source: Christiane Wendehorst

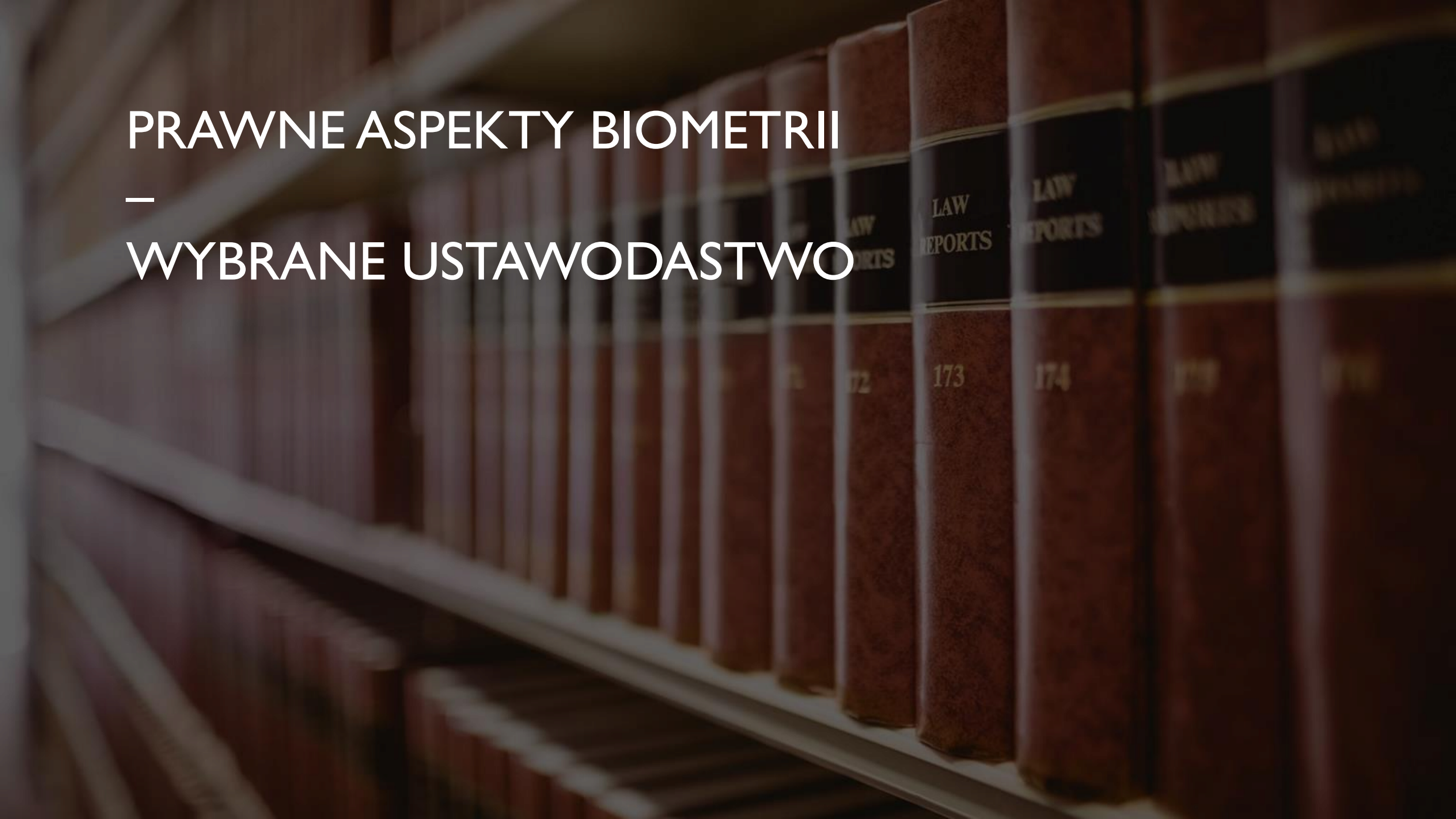
„BIOMETRYCZNY”

oznacza pewien stopień niezmienność, dana osoba ma niewielką szansę na zmianę lub nie ma jej wcale

na przykład: osoba nie może, według własnego uznania zmienić swojej twarzy lub wzoru daktyloskopijnego

zwykle rozumiany jako obejmujący zachowanie, które nie może być kontrolowane przez ludzką wolę w większym stopniu

na przykład: zachowania zakupowe, historia przeglądania czy treść komunikacji



PRAWNE ASPEKTY BIOMETRII – WYBRANE USTAWODASTWO

PRAWNE ASPEKTY BIOMETRII
WYBRANE USTAWODAWSTWO

Europejska konwencja praw człowieka (EKPC)

Powszechnej Deklaracji Praw Człowieka (PDPC ONZ)

Karta Praw Podstawowych Unii Europejskiej (KPP UE)

Ogólne rozporządzenie o ochronie danych (RODO)

Dyrektywa o ochronie danych w obszarze policji i wymiaru sprawiedliwości (LED)

Rozporządzenie w sprawie norm dotyczących zabezpieczeń danych biometrycznych w paszportach i dokumentach podróży

Przepisy dotyczące kontroli granicznej i bezpieczeństwa

Rozporządzenie w sprawie sztucznej inteligencji (AI Act)

Rozporządzenia w sprawie jednolitego rynku usług cyfrowych (Akt o usługach cyfrowych/DSA)

EUROPEJSKA KONWENCJA PRAW CZŁOWIEKA (EKPC)

- Opracowana przez Radę Europy w 1950 r., weszło w życie w 1953 r., w Polsce w 1993 r.
- Rada Europy to **międzynarodowa organizacja międzyrządowa zajmująca się prawami człowieka**
- W skład wchodzą wszystkie państwa UE, Wielka Brytania, Turcja, ale i Armenia, Azerbejdżan, czy Gruzja (*uwaga*: do marca 2022 r. Rosja była członkiem Rady Europy zanim została zawieszona, a następnie sama odeszła)
- EKPC zawiera katalog praw podstawowych, a także dodatkowe protokoły (np. Protokół 6 znosi karę śmierci)
- W odniesieniu do technik biometrycznych w EKPC szczególnej uwagi wymagają m.in. prawo do życia, prawo do rzetelnego procesu sądowego, zakaz karania bez ustawy oraz prawo do poszanowania życia prywatnego i rodzinnego oraz również prawo do prywatności

EUROPEJSKA KONWENCJA PRAW CZŁOWIEKA (EKPC)

- Stosowanie technik biometrycznych do celów nadzoru może być sprzeczne z gwarantowaną w EKPC wolnością słowa, w tym wolnością wyrażania poglądów, myśli, sumienia i wyznania, a także z wolnością zgromadzeń i zrzeszania się
- Ogólny zakaz dyskryminacji wynikający z takich powodów jak: płeć, rasę, kolor skóry, język, religia, poglądy polityczne lub inne, pochodzenie narodowe lub społeczne, status mniejszości narodowej, majątek, urodzenie lub z jakichkolwiek innych przyczyn (Protokół 12 EKPC)
- Żadne z tych praw nie ma jednak charakteru bezwzględnego i w związku z tym może podlegać ograniczeniom, jeśli jest ono przewidziane zgodnie z prawem i spełnione są podstawy określone w odpowiednie ustawie
- Aby zapewnić skuteczną ochronę zagwarantowanych praw i wolności, ustanowiono Europejski Trybunał Praw Człowieka (ETPC). Każda osoba może zwrócić się do Trybunału, jeśli uzna, że prawa określone w EKPC zostały naruszone przez państwo-stronę, ale tylko wtedy, gdy wyczerpane zostały wszystkie krajowe środki odwoławcze, a państwo jest stroną EKPC

POWSZECHNA DEKLARACJA PRAW CZŁOWIEKA (PDPC ONZ)

- Ogłoszona przez Organizację Narodów Zjednoczonych w 1948 r. w wyniku wydarzeń II wojny światowej
- Stanowi kamień milowy w historii praw człowieka, a jej poprzedniczka to Karta Narodów Zjednoczonych
- Nie jest wiążąca jak traktat, czy konwencja, a jest **uznawana za prawo zwyczajowe**
- PDPC to artykuły zawarte w samej deklaracji, ale i rezolucje wydawane przez Radę Bezpieczeństwa ONZ
- Szczególnej uwagi wymagają m.in. prawo do życia, wolności, bezpieczeństwa, prawo do prywatności, wolności myśli, opinii i wypowiedzi

POWSZECHNA DEKLARACJA PRAW CZŁOWIEKA (PDPC ONZ)

- Rada Bezpieczeństwa Organizacji Narodów Zjednoczonych wydała kilka rezolucji dotyczących gromadzenia oraz udostępniania danych biometrycznych do celów walki z terroryzmem
- Rezolucja nr 2160 zachęca państwa członkowskie ONZ do przesyłania do INTERPOLU zdjęć i innych danych biometrycznych osób wspierających talibów oraz zawiera zalecenie, aby takie udostępnianie danych miało miejsce zgodnie z prawem krajowym i międzynarodowym
- Rezolucja nr 2322 rozszerzyła rekomendację dla udostępniania danych biometrycznych terrorystów i członków organizacji terrorystycznych
- Rezolucja 2396 poszła dalej i nałożyła wiążący obowiązek rozwijania zdolności biometrycznych zgodnie z prawem krajowym i międzynarodowym dot. praw człowieka

KARTA PRAW PODSTAWOWYCH UNII EUROPEJSKIEJ (KPP UE)

- Opracowana przez Unię Europejską w 2000 r., z poprawkami podpisana w 2007 r., w Polsce podpisany w 2007 r., w życie weszła w 2009 r.
- Składa się z preambuły oraz 54 artykułów podzielonych na 7 rozdziałów
- Zawiera zbiór fundamentalnych praw człowieka i obowiązków obywatelskich
- Szczególnej uwagi wymagają m.in. ochrona godności ludzkiej, prawo do wolności, do poszanowania prywatności, ochrony danych osobowych, wolności myśli, sumienia i religii, równości wobec prawa, zakazu wszelkiej dyskryminacji, poszanowanie różnorodności kulturowej

KARTA PRAW PODSTAWOWYCH UNII EUROPEJSKIEJ (KPP UE)

- W kontekście technik biometrycznych prawo do poszanowania życia prywatnego i ochrona danych osobowych zostały przywołane w kilku sprawach przed TSUE w zakresie zbierania danych biometrycznych pierwszej generacji do paszportów
- Istotną rolę w dyskusjach etycznych dotyczących stosowania technik biometrycznych odgrywa art. 1, który stanowi, że „godność ludzka jest nienaruszalna" i „musi być szanowana i chroniona"
- W swej istocie godność ludzka jest rozumiana jako zakaz instrumentalizacji lub uprzedmiotowienie istot ludzkich. Pojęcie godności jest jednak niezwykle szerokie, co z jednej strony daje bardzo szerokie i elastyczne pole zastosowania, ale z drugiej sprawia, że trudno jest uchwycić jego dokładny charakter prawny
- KPP UE zakazuje wszelkiej dyskryminacji ze względu na płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religia lub przekonania, poglądy polityczne lub inne, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek lub orientację seksualną

ROZPORZĄDZENIE O OCHRONIE DANYCH OSOBOWYCH (RODO)

- Akt prawa UE przyjęty w 2016 r., wszedł w życie w 2018 r., w tym w Polsce
- Zastąpił dotychczasową dyrektywę unijną 95/46/WE z 1995 r.
- RODO zawiera przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych
- Jeden z celów wdrożenia RODO, to zaktualizowanie przepisów będących odpowiedzią na zagrożenia wynikające z użycia w przetwarzaniu danych osobowych nowoczesnych technologii
- RODO jest częścią pakietu unijnego wraz z dyrektywą o ochronie danych obszarze policji i wymiaru sprawiedliwości dotyczącego reformy ochrony danych osobowych

ROZPORZĄDZENIE O OCHRONIE DANYCH OSOBOWYCH (RODO)

- RODO nie tylko wprowadza **definicję „danych biometrycznych”,** ale także nakłada surowe wymagania dotyczące przetwarzania danych biometrycznych
- Zgodnie z RODO **dane biometryczne to** dane osobowe, które wynikają ze specjalnego przetwarzania technicznego dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne
- **Dane osobowe mogą być przetwarzane tylko** wtedy, gdy zachodzi jedna z podstaw określonych w art. 6 ust. 1 RODO m.in. zgoda, niezbędne do wykonania umowy, niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, czy niezbędne do celów wynikających z prawnie uzasadnionych interesów
- RODO (art. 9 ust. 1) zasadniczo zabrania przetwarzania **danych biometrycznych** i innych danych wrażliwych w celu identyfikacji - ta ogólna zasada podlega wyjątkom szczegółowo wymienionym w art. 9 ust. 2 RODO tj. m.in. zgoda, niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi

ROZPORZĄDZENIE O OCHRONIE DANYCH OSOBOWYCH (RODO)

- RODO ogranicza również stosowanie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach (profilowanie)
- RODO daje osobie, której dane dotyczą prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, która to decyzja wywołuje wobec nich skutki prawne lub wpływa na nie w podobnie istotny sposób. W pełni zautomatyzowana decyzja to taka, w której nie ma ingerencji człowieka, a wynikiem przetwarzania jest decyzja bez interwencji człowieka
- Trzy **wyjątki**: zautomatyzowana decyzja jest zgodna z RODO, jeśli (1) jest to konieczne do zawarcia lub wykonania umowy, (2) dozwolone na mocy prawa UE lub prawa państwa członkowskiego lub (3) na podstawie wyraźnej zgody
- Jednak nawet jeśli ma zastosowanie jeden z wyjątków, to zautomatyzowane przetwarzanie musi podlegać **odpowiednim zabezpieczeniom** tj. poinformowaniu o tym osób, których dane dotyczą oraz **prawo do uzyskania interwencji człowieka**, aby uzyskać wyjaśnienie podjętej decyzji
- Art. 22 ust. 4 RODO określa jeszcze dokładniejsze **wyjątki** w zakresie przetwarzania danych biometrycznych tj. osoba, której dane dotyczą: (1) wyrazi na to wyraźną zgodę lub jeśli (2) przetwarzanie jest niezbędne ze względu na ważny interes publiczny

DYREKTYWA O OCHRONIE DANYCH W OBSZARZE POLICJI I WYMIARU SPRAWIEDLIWOŚCI (LED)

- Przetwarzanie danych osobowych, w tym danych biometrycznych w celach profilaktycznych, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania kar kryminalnych jest wyłączone z zakresu RODO i zostało ujęte w dyrektywie o egzekwowaniu prawa (LED)
- LED jedynie ustawia ogólne zasady dla organów ścigania
- Przetwarzanie danych biometrycznych w celu jednoznacznej identyfikacji osoby fizycznej przez organy ścigania jest dozwolone tylko wtedy, gdy: zostało uznane za bezwzględnie konieczne i podlegające odpowiednim zabezpieczeniom praw i wolności podmiotu danych
- Przetwarzanie musi: (1) być dozwolone na mocy prawa UE lub prawa państwa członkowskiego, (2) chronić żywotne interesy osoby, której dane dotyczą, lub innej osoby fizycznej, lub (3) dotyczyć danych, które zostały w sposób oczywisty upublicznione przez osobę, której dane dotyczą
- Jeżeli przetwarzanie narusza art. 10 LED, danemu podmiotowi przysługuje prawo żądania usunięcia jego danych

DYREKTYWA O OCHRONIE DANYCH W OBSZARZE POLICJI I WYMIARU SPRAWIEDLIWOŚCI (LED)

- Wykorzystanie zautomatyzowanego podejmowania decyzji opartego na danych biometrycznych są dozwolone tylko wtedy, gdy są wystarczające gwarancje praw i wolności osoby, których dane dotyczą, w szczególności prawo do uzyskania interwencji człowieka
- Ograniczenia LED są mniej konkretne niż te określone RODO
- LED określa jedynie, że muszą istnieć odpowiednie środki w celu zapewnienia ochrony prawa i wolności osoby, której dane dotyczą, oraz uzasadnione interesy oraz że zabronione jest profilowanie, które prowadzi do dyskryminacji osób fizycznych ze względu na dane wrażliwe
- LED wymaga również od państw członkowskich wdrożenia odpowiednich środków bezpieczeństwa
- Obejmują one środki takie jak: kontrola użytkownika, kontrola przechowywania, kontrola dostępu i integralności i powinien brać pod uwagę ryzyko związane z przetwarzaniem danych, takie jak: przypadkowe lub niezgodne z prawem zniszczenie, utrata, zmiana lub nieuprawnione ujawnienie lub dostęp do danych osobowych dane przekazywane, przechowywane lub w inny sposób przetwarzane, co może w szczególności prowadzić do fizycznych, materialnych lub szkody niematerialne

ROZPORZĄDZENIE DOTYCZĄCE ZABEZPIECZEŃ DANYCH BIOMETRYCZNYCH W PASZPORTACH I DOKUMENTACH PODRÓŻY

- Rozporządzenie z 2004 r. wprowadzające jako pierwsze rozporządzenie szczególne zezwolenie na zbieranie, przechowywanie i wykorzystywanie danych biometrycznych
- Paszporty i dokumenty podróży wydane przez państwa członkowskie UE muszą uwzględnić wysoce zabezpieczony nośnik danych, który zawiera wizerunek twarzy i dwa odciski palców
- W celu ochrony danych biometrycznych przed nieuprawnionego dostępu i nadużycia, rozporządzenie wymaga od państw członkowskich zapewnienia, że dane są zabezpieczone, a nośnik pamięci ma wystarczającą pojemność i zdolność do zagwarantowania integralności, autentyczność i poufność danych
- Tylko personel krajowego organu odpowiedzialnego za wydawanie paszportów jest upoważniony do zbierania identyfikatorów biometrycznych oraz czyni to zgodnie z Europejską Konwencją Praw Człowieka (EKPC) i Konwencją ONZ o prawach dziecka
- Identyfikatory biometryczne mogą być wykorzystywane wyłącznie do weryfikacji autentyczności dokumentu oraz do weryfikacji tożsamości posiadacza

PRZEPISY DOTYCZĄCE KONTROLI GRANICZNEJ I BEZPIECZEŃSTWA

- **Rozporządzenie EES** ma na celu lepsze zarządzanie granicami zewnętrznymi oraz zapobieganie nielegalnej imigracji i przedłużaniu pobytu
- W tym celu państwa członkowskie muszą ustanowić System wjazdu-wyjazdu, który rejestruje i przechowuje datę, godzinę oraz miejsce wjazdu i wyjazdu obywateli z dowolnego państwa trzeciego przekraczających granicę strefy Schengen. Informacje te są łączone z danymi daktyloskopijnymi, a wizerunek twarzy i informacje z dokumentem podróży
- Dane gromadzone w ramach systemu EES mogą być również wykorzystywane w celu zapobiegania, wykrywania i prowadzenia dochodzeń w sprawie terroryzmu
- W motywach rozporządzenia w sprawie EES zagwarantowano, aby EES było zgodne z KPP UE, a organy krajowe mogą rejestrować i wykorzystywać wyłącznie dane biometryczne zgodnie z KPP UE i EKPC
- Chociaż okres retencji danych został skrócony do trzech lat wciąż pojawiają się obawy dot. proporcjonalności systemu EES, ponieważ dane wrażliwe milionów ludzi są gromadzone w sposób nieukierunkowany i przechowywane przez dłuższy czas

PRZEPISY DOTYCZĄCE KONTROLI GRANICZNEJ I BEZPIECZEŃSTWA

- **System Informacyjny Schengen (SIS)** to narzędzie rekompensujące zniesienie kontroli na granicach pomiędzy państwami Obszaru Schengen
- Polega na zapewnieniu, aby każde z państw Obszaru Schengen posiadało ten sam zestaw informacji pozwalający na dostęp, przy pomocy zautomatyzowanych środków wyszukiwania do wpisów dotyczących osób i przedmiotów w celu kontroli granicznej oraz innych kontroli policyjnych i celnych prowadzonych w ramach danego kraju oraz w celu wydawania wiz, dokumentów pobytowych i wykonywania przepisów prawnych o cudzoziemcach w kontekście stosowania Konwencji Wykonawczej do Układu z Schengen
- SIS umożliwia przesyłanie danych biometrycznych, w tym odcisków palców, odcisków dłoni i wizerunków twarzy
- Nowe przepisy dotyczące SIS wymagają również, aby państwa członkowskie mogły korzystać z funkcji wyszukiwania odcisków palców we wszystkich czynnościach operacyjnych

PRZEPISY DOTYCZĄCE KONTROLI GRANICZNEJ I BEZPIECZEŃSTWA

- **Decyzja z Prüm** zobowiązuje państwa członkowskie do posiadania systemu, który umożliwia organom innych Państwa UE na automatyczne przeszukiwanie krajowych baz danych DNA i odcisków palców pod kątem bezpieczeństwa celem zapobiegania atakom terrorystycznym lub ścigania przestępstw
- W swej istocie Decyzja z Prüm ustanawia zdecentralizowaną sieć wymiany danych biometrycznych składającą się z krajowych bazy danych, które są ze sobą połączone
- Państwa niebędące członkami UE uczestniczące w systemie Prüm to Norwegia, Szwajcaria i Islandia

ROZPORZĄDZENIE W SPRAWIE SZTUCZNEJ INTELIGENCJI W UE (AI ACT)

- AI Act to zestaw przepisów regulujących funkcjonowanie sztucznej inteligencji mających na celu głównie **ochronę człowieka przed negatywnymi konsekwencjami działalności AI**
- Projekt dokumentu opracowany przez Komisję Europejska w 2021 r.
- Wszedł w życie 1 sierpnia 2024 roku jako pierwsza w skali świata kompleksowa regulacja prawna dla systemów i modeli sztucznej inteligencji
- Komisja Europejska w projekcie zdecydowała się na podejście oparte na ryzyku, rozróżnia zastosowania sztucznej inteligencji, które tworzą (1) niedopuszczalne ryzyko, (2) wysokie ryzyko oraz (3) niskie lub minimalne ryzyko
- AI Act definuje „**dane biometryczne**” jako dane osobowe będące wynikiem specjalnego przetwarzania technicznego, które dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej, takich jak wizerunek twarzy lub dane daktyloskopijne
- AI Act ma na celu rozbudowanie ochrony osób fizycznych, np. kiedy mowa o zakazanych praktykach w zakresie AI, niedozwolonym było wykorzystywanie jakichkolwiek danych biometrycznych do wnioskowania na ich podstawie orientacji seksualnej, przekonań religijnych czy przynależności do związków zawodowych

ROZPORZĄDZENIE W SPRAWIE SZTUCZNEJ INTELIGENCJI W UE (AI ACT)

- Przetwarzanie danych biometrycznych jest wymienione jako system wysokiego ryzyka
- Oznacza to, że ich użycie nie jest zabronione, ale podlega szeregowi obowiązkowych wymogów
- Wymagania te obejmują m.in. wdrożenie systemu zarządzania ryzykiem, odpowiednie praktyki zarządzania danymi i zarządzania, a także zapewnienie przejrzystości oraz odpowiedniego nadzoru ludzkiego
- Dostawca sztucznej inteligencji wysokiego ryzyka musi przestrzegać bardziej rygorystycznych procedur oceny zgodności
- Europejski Inspektor Ochrony Danych Osobowych podniósł, że zastosowanie sztucznej inteligencji pozbawia ludzi anonimowości w przestrzeni publicznej, niezbędnej do tego, żeby bezpiecznie protestować i wyrażać obywatelskie niezadowolenie bez obawy o potencjalne reperkusje

PROJEKT ROZPORZĄDZENIA W SPRAWIE SZTUCZNEJ INTELIGENCJI W UE (AI ACT)

- AI Act zabrania stosowania AI do zdalnej identyfikacji osób w czasie rzeczywistym, z wyjątkiem realizacji 3 celów:

[1] ukierunkowanego wyszukiwania konkretnych ofiar (uprowadzenia, handel ludźmi i wykorzystywanie seksualne ludzi, poszukiwanie zaginionych osób),

[2] zapobieżenie konkretnemu, istotnemu i bezpośredniemu zagrożeniu życia i bezpieczeństwa osób albo groźbie ataku oraz

[3] zlokalizowanie/identyfikacja osoby podejrzanej o popełnienie przestępstwa

- W tych ramach system AI powinien służyć jedynie do potwierdzenia tożsamości poszukiwanej osoby. Wyjątki te wymagają rygorystycznej oceny sytuacji, biorąc pod uwagę wagę i potencjalne konsekwencje dla praw i wolności jednostki.
- Do zdalnej identyfikacji biometrycznej **nie należą** systemy AI przeznaczone do weryfikacji biometrycznej, która obejmuje uwierzytelnianie, prowadzone **jedynie w celu potwierdzenia**, że dana osoba fizyczna jest osobą, za którą się podaje, oraz potwierdzenia tożsamości osoby fizycznej wyłącznie **w celu uzyskania dostępu** do usługi, uruchomienia urządzenia lub uzyskania bezpiecznego dostępu do pomieszczeń.

ROZPORZĄDZENIE W SPRAWIE JEDNOLITEGO RYNKU USŁUG CYFROWYCH (AKT O USŁUGACH CYFROWYCH/DSA)

- Akt o usługach cyfrowych obowiązuje od 17 lutego 2024 r.
- DSA nakłada obowiązki dla dostawców usług cyfrowych, które mają zapewnić:

  - równe traktowanie działalności w świecie rzeczywistym tzw. offline i usług świadczonych drogą elektroniczną tzw. online;

  - przejrzystość w dostarczaniu treści reklamowych;

  - poszanowanie podstawowych praw i wolności konsumentów

- Zgodnie z DSA **niedozwolone** jest prezentowanie na platformach internetowych **reklam opartych na profilowaniu z wykorzystaniem szczególnych kategorii danych osobowych** (danych wrażliwych), co oznacza dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, dane genetyczne i biometryczne czy dane dotyczące zdrowia

PRAWNE ASPEKTY BIOMETRII – WYBRANE ORZECZNICTWO

PRAWNE ASPEKTY BIOMETRII
WYBRANE ORZECZNICTWO

Orzecznictwo Europejskiego Trybunału Praw Człowieka (ETPCz)

Orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (TSUE)

Orzecznictwo polskie - WSA i NSA

ORZECZNICTWO EUROPEJSKIEGO TRYBUNAŁU PRAW CZŁOWIEKA (ETPCz)

- W sprawie dot. **przechowywania zdjęć skazanych terrorystów w Irlandii**. ETPCz uznał, że przechowywanie podstawowych danych osobowych osoby aresztowanej, a nawet innych osób obecnych w tym czasie: nie może wykraczać poza uzasadnione granice procedury dochodzeniowej w sprawie przestępstw terrorystycznych

- W sprawie S. i Marper przeciwko Zjednoczonemu Królestwu, ETPCz musiał podjąć **decyzję o zatrzymaniu odcisków palców i próbek danych komórkowych w bazach danych DNA**. ETPCz uznał, że przechowywanie odcisków palców wymaga minimum zabezpieczeń dotyczących: czas trwania, przechowywanie i usuwanie danych, zwłaszcza jeśli dane są przetwarzane automatycznie
- ETPCz stwierdził również, że poziom ingerencji może się różnić w zależności od różnych kategorii danych osobowych stwierdzając, że odciski palców mają mniejszy wpływ na życie prywatne niż próbki DNA
- ETPCz uznał, że zatrzymywanie próbek DNA służy uzasadnionemu celowi wykrywania przestępstw, ale przechowywanie danych DNA narusza art. 8 Konwencji, ponieważ przechowywane były nie tylko dane osób skazanych, ale także dane oskarżonych, którzy zostali już uniewinnieni a ich dane były przechowywane bezterminowo

ORZECZNICTWO EUROPEJSKIEGO TRYBUNAŁU PRAW CZŁOWIEKA (ETPCz)

- W sprawie Van der Velden ETPCz uznał, że **pobieranie próbek DNA** nie narusza art. 7 Konwencji. ETPCz uznał obowiązek poddania się badaniom DNA osób skazanych za przestępstwa o określonej wadze, odnotowując znaczny wkład danych DNA w egzekwowanie prawa
- ETPCz uznał również, że ze względu na wykorzystywanie, do którego w szczególności materiał komórkowy może być przydatny w przyszłości, bezterminowe przechowywanie tego materiału wykracza poza zakres neutralnej identyfikacji danych, takich jak odciski palców oraz jest wystarczająco inwazyjny, aby stanowić ingerencję w prawo do: poszanowanie życia prywatnego, o którym mowa w art. 8 ust. 1 Konwencji

- W sprawie Gaughran przeciwko Wielkiej Brytanii ETPCz uznał, że niedopuszczalne jest w przypadku **odcisków palców i profili DNA osób skazanych za wykroczenia** przechowywanie ich danych bezterminowo bez możliwości żądania usunięcia te dane. Taka ingerencja w prawo skarżącego do poszanowania życia prywatnego nie może być uznana za niezbędną w demokratycznym społeczeństwie
- ETPCz w swoich rozważaniach uznał, że: zachowanie odcisków palców i fotografii do czasu śmierci można uznać za porównywalne z bezterminowym przechowywaniem

ORZECZNICTWO TRYBUNAŁU SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ (TSUE)

- W sprawie Schwarz TSUE stwierdził, że **przetwarzanie odcisków palców** nie wykracza poza to, co jest konieczne do osiągnięcia celu rozporządzenia nr 2252/2004, który zobowiązuje organy państwowe do pobierania i przechowywania odcisków palców **przy wydawaniu paszportu**, jakim jest ochrona przeciwko nielegalnemu używaniu paszportów
- TSUE wyraźnie wspomniał, że niezgodność między odciskami palców posiadacza paszportu, a danymi w tym dokumencie nie są oparte na automatycznej decyzji, takiej jak odmowa wjazdu do Unii Europejskiej, a spowodują bardziej szczegółową kontrolę tej osoby w celu ostatecznego ustalenia jej tożsamość

ORZECZNICTWO TRYBUNAŁU SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ (TSUE)

- W sprawie Burgemeester TSUE uznał, że rozporządzenie nr 2252/2004 nie ma zastosowania do wykorzystywania i przechowywania danych biometrycznych **do innych celów niż wydanie paszportu.** Kwestie te należą wyłącznie do kompetencji państw członkowskich
- Prawa podstawowe gwarantowane przez KPP UE mają zastosowanie tylko tam, gdzie prawodawstwo krajowe nie spełnia wymogów w zakresie prawa Unii
- TSUE doszedł do wniosku, że centralne przechowywanie danych biometrycznych jest sprzeczne z art. 7 i 8 KPP UE, ale jest proporcjonalne i niezbędne do zwalczania oszustw dotyczących tożsamości i dokumentów
- TSUE stwierdził również, że okres przechowywania wynoszący pięć lat nie jest nadmierny i jest uzasadniony w świetle celu, jakim jest zapobieganie i zwalczanie oszustw dotyczących tożsamości i dokumentów

ORZECZNICTWO POLSKICH SĄDÓW ADMINISTRACYJNYCH

Naczelny Sąd Administracyjny w wyroku (sygn. akt I OSK 249/09) uznał, że wykorzystywanie danych biometrycznych pracowników do kontroli czasu pracy narusza zasadę adekwatności. Sąd ten wskazał, że wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników jest nieproporcjonalne do zamierzonego celu ich przetwarzania

Wyrok Wojewódzkiego Sądu Administracyjnego (sygn. akt II SA/Wa 809/20), który uchylił decyzję Prezesa UODO nakładającą karę na szkołę, przetwarzającą dane biometryczne uczniów jest w opozycji do wcześniejszego orzecznictwa NSA

- Prezes UODO nałożył na szkołę karę w wysokości 20 tys. zł za to, że przetwarzała dane biometryczne dzieci i nakazał jej usunąć te dane. Decyzja ta została zaskarżona do WSA, który ją uchylił
- WSA uznał w tej sprawie, że wyrażenie zgody przewidziane w art. 9 ust. 1 lit. a RODO legalizuje pobieranie i przetwarzanie danych biometrycznych dzieci
- UODO jednak nie może się z tym zgodzić. Udzielona przez rodziców zgoda na przetwarzanie danych biometrycznych ich dzieci nie może być uznana za dobrowolną, skoro jej brak wywoływał negatywne skutki w postaci konieczności przepuszczenia w kolejce po posiłek, tych dzieci, których rodzice taką zgodę wyrazili
- Prezes UODO złożył do NSA kasację od wspomnianego wyroku WSA, który uchylił decyzję organu nadzorczego. Zdaniem UODO w sprawie doszło nie tylko do naruszenia zasad określonych w RODO, tj. minimalizacji i adekwatności, dobrowolności wyrażenia zgody, ale i do dyskryminacji niektórych uczniów

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- Główny problem etyczny podnoszony konkretnie w związku z identyfikacją biometryczną jest związany ze **stworzeniem i przechowywaniem unikalnego szablonu** identyfikującego konkretną osobę
- Cechy, które jednoznacznie identyfikują daną osobę są częścią jej ciała, a ich gromadzenie i używanie **narusza osobistą autonomię i godność człowieka**
- Każdy, kto wejdzie w posiadanie szablonu w przyszłości, ma możliwość śledzenia i rozpoznawania tej osoby w dowolnym miejscu na świecie i potencjalnie z każdym zamiarem
- Po utworzeniu szablonu biometrycznego i zapisaniu go w referencyjnej bazie danych, ktokolwiek wejdzie w posiadanie tego szablonu jest w stanie zidentyfikować i prześledzić odpowiednią osobę w dowolnym miejscu na świecie, stwarzając **poważne ryzyko dla tej osoby, że zostanie namierzona i poddana inwigilacji**
- **Jednostka nie ma możliwości ucieczki od tego, ponieważ jednostka nie może zmienić silnych identyfikatorów biometrycznych**
- Kwestie etyczne, jakie budzi **stosowanie metod identyfikacji biometrycznej** w miejscach publicznych odnoszą się nie tylko konkretnie do biometrii, ale także do **nadzoru osób na dużą skalę** jako takiego lub do celów, w jakich technologia jest używana i jak jest używana

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- Profile biometryczne są podatne na zagrożenia poufności i naruszenie cyberbezpieczeństwa
- Naruszenia danych osobowych zawsze prowadzą do ingerencji w osoby, których dane dotyczą, **prawo do ochrony danych i życia prywatnego**, ryzyko naruszenia praw podstawowych jest większe, jeśli naruszenie dotyczy szablonów biometrycznych
  - Po pierwsze dlatego, że szablonów biometrycznych można używać do zdalnego śledzenia i nadzoru na całym świecie
  - Po drugie, identyfikatory biometryczne są coraz częściej wykorzystywane do celów uwierzytelniania, dlatego każdy, kto kontroluje szablony biometryczne, może ich używać do tworzenia „fałszywki” i popełniać oszustwa dotyczące tożsamości
  - Wreszcie, osoby fizyczne mają tylko ograniczoną liczbę identyfikatorów biometrycznych, które są **praktycznie niezmienne**. Ataki mające na celu uzyskanie nieautoryzowanego dostępu do szablonów biometrycznych mogą być skierowane przeciwko biometrii bazy danych systemu lub przy przekazywaniu wzorców biometrycznych
- W przypadku ujawnienia szablonów biometrycznych ryzyko dla osoby, której dane dotyczą, dotyczy nie tylko informacji wrażliwych, ale i możliwości wyodrębnienia z samego zapisanego szablonu biometrycznego, danych takich jak pochodzenie etniczne osoby lub prawdopodobieństwo niektórych chorób

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- Ze względu na swoją wyjątkowość szablony biometryczne pozwalają wydajnie **identyfikować i śledzić bez ograniczeń** czasowych oraz miejscowych
- Są często powiązane z innymi danymi osobowymi i można je porównywać z danymi pochodzącymi z różnych źródeł, które umożliwiają **tworzenie rozbudowanych profili** osób, które to mogą mieć poważny **wpływ na życie prywatne osoby**
- W rękach niewłaściwych podmiotów zwiększają również ryzyko tzw. **spoofingu**, czyli obchodzenia systemów biometrycznych poprzez przedstawianie sfałszowanych identyfikatorów biometrycznych
- Podczas gdy niektóre identyfikatory, takie jak tęczówka, są raczej trudne do odtworzenia, **inne można łatwiej sfałszować**, np. biometryczny szablon odcisku palca może być użyty do stworzenia sztucznych palców

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

Case: w 2019 **na konferencji Black Hat w USA** zaprezentowano sposób obchodzenia wykrywania żywotności w technologii Face ID od Apple. Firma Apple ma wielu klientów-okularników i ma też fioła na punkcie *user experience*, więc nie chciała utrudniać nikomu życia koniecznością zdejmowania okularów do odblokowania telefonu.

Jeśli użytkownik założył okulary, to Face ID nie tworzyła i nie analizowała trójwymiarowego modelu okolicy oczu. To naprowadziło badaczy na genialnie proste rozwiązanie. Trzeba było stworzyć okulary z przekonującym (dla AI) obrazem oczu, który może być płaski.

Case: w 2020 r. **badacze z Cisco Talos** osiągnęli 80% skuteczności atakując czytniki odcisków palców przy pomocy replik odcisków wytworzonych z użyciem drukarki 3D.

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- Mogą się pojawić problemy etyczne związane z **algorytmicznym podejmowaniem decyzji** dot. procedur decyzyjnych systemu, które są zwykle kodowane przez programistów zgodnie z konkretnymi potrzebami użytkowników, zwykle różne pasujące wyniki będą wyzwalać różne reakcje, np. wysoki wynik dopasowania może prowadzić do przyznania lub odmowy dostępu do: budynku, wniosku o dodatkowe dane uwierzytelniające lub wzmocnionego nadzoru
- Dane wynikające z identyfikacji, mogą być przechowywane i dalej przetwarzane w celach **wykraczających poza identyfikację**, takich jak tworzenie profilu mobilności
- Często „silne” dane biometryczne są zbierane razem ze „słabymi”, takimi jak płeć, wiek, pochodzenie etniczne lub wzrost, które mogą: być używane w połączeniu z silnymi identyfikatorami w celu **poprawy wskaźników powodzenia techniki identyfikacji**

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- Kwestie **dyskryminacji lub stygmatyzacji** pojawiają się na przykład przy rozpoznawaniu twarzy - nie powinno ono być mniej dokładne w przypadku osób kolorowych i w każdym przypadku zmniejszona dokładność musi być należycie uwzględniona
- Wykorzystywany **do celów egzekwowania prawa**, błędnie przypisywany wysoki wynik dopasowania może mieć drastyczne konsekwencje dla poszkodowanych, takie jak bezprawne aresztowanie lub w najgorszym przypadku bezprawne skazanie
- Nawet jeśli błędna decyzja systemu algorytmicznego zostanie skorygowana, sam fakt, że został przypisany do stygmatyzującej kategorii, takiej jak „handlarz narkotyków", „przestępca seksualny" lub „terrorysta", może samo w sobie poważnie wpływać na życie prywatne danej osoby

Case: **Alonzo Sawyera (USA)** tj. przypadek niesłusznego skazania mężczyzny przez amerykański wymiar sprawiedliwości z powodu błędu AI (patrz także: Randall Reid, Nijeer Parks, Robert Williams).

Pierwszym problemem jest uprzedzenie AI odpowiedzialnej za systemy rozpoznawania twarzy. Cechą wspólną wszystkich wymienionych mężczyzn jest ich ciemny kolor skóry. Skuteczność danego modelu zależy całkowicie od wielkości i jakości danych treningowych. W związku, z czym dzieci i kobiety, a także osoby reprezentujące inne rasy mogą spotkać się z niesprawiedliwym osądem AI.

Inny problem polega na tym, że AI najlepiej działa kiedy osoby przedstawione na zdjęciach patrzą się na wprost, ich oczy są otwarte, usta zamknięte, a ciało zatrzymane w ruchu. Co często jest trudne do osiągnięcia, gdyż zdjęcia osób poszukiwanych są kompletnym przeciwieństwem tego, z czym AI pracuje się najlepiej.

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

Case: w 2023 r. **badacze z Columbia Engineering Undergraduate** stworzyli model AI, który miał za zadanie przeanalizowanie olbrzymiej bazy danych odcisków palców. W sumie AI miała do zbadania ok. 60 tys. linii papilarnych.

Okazało się, że były przypadki, gdy para linii należała do tej samej osoby, ale do różnych palców, a niekiedy do dwóch zupełnie innych osób.

Recenzenci uznali, że baza danych jest zbyt mała, żeby podważyć tezę o unikalności linii papilarnych. Zespół nie poddał się i zebrał więcej danych oraz usprawnił model AI, aby otrzymane wyniki były jeszcze dokładniejsze. W końcu udało się i praca inżynierów z Columbii doczekała się publikacji w wydaniu „Science Advances".

Odkrycie może sprawić, że skazani mogą zostać uniewinnieni w wyniku błędnego porównywania linii papilarnych.

W badaniu czytamy, że AI wykorzystała zupełnie nowe podejście do analizy linii papilarnych, a dokładność wynosi ok. 77%. AI skupiała się głównie na kwestiach związanych z kątami i krzywiznami wiru i pętli na środku odcisku palca.

Problemem mogą być potencjalne uprzedzenia modelu AI. Chodzi m.in. o płeć i rasę, żeby uniknąć tych komplikacji, AI musi mieć do dyspozycji dużo mniej ograniczoną bazę danych.

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- Tworzenie unikalnych szablonów oznacza **przekształcanie unikalnych cech fizycznych człowieka w dane cyfrowe**, co prowadzi do **datafikacja ludzi**
- Uprzedmiotawia to człowieka i daje innym możliwość wykorzystania unikalne cech fizycznych dla własnych celów, **nawet jeśli cele te są sprzeczne z interesem osoby, której dane dotyczą**

Case: **PimEyes** to płatna wyszukiwarka pozwalająca odnaleźć wszystkie zdjęcia danej osoby na podstawie jednego zdjęcia załadowanego na stronę. Zdjęcia wykorzystywane przez PimEyes zaczerpnięte są ze stron internetowych, takich jak: blogi, studia fotograficzne, serwisy newsowe, zrzuty zdjęć z Zoom'a czy witryny z recenzjami lokali gastronomicznych, a nawet serwisy pornograficzne.

Wyszukiwanie działa bardzo dokładnie, docierając nawet do tych rejonów sieci, o jakich dawno już nikt nie pamięta i wyciągając na światło dzienne zdjęcia, które trudno odnaleźć nawet przy pomocy Google'a. Potencjalnie może być zatem bardzo niebezpieczne i wykorzystywane jako łatwy oręż do walki z prywatnością np. byłych partnerów czy współpracowników.

W 2018 r. firma chwaliła się przeanalizowaniem 1 terabajta zdjęć oraz przechowywaniem w swojej bazie danych biometrycznych ponad 100 mln twarzy. Rok później baza obejmowała 500 mln twarzy, a w 2020 r. było to już 900 mln twarzy, a obecnie – 2 miliardy (!)

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- Biorąc pod uwagę fakt, że szablon biometryczny digitalizuje ludzkie ciało i reprezentuje cechy ciała, to argumentowano nawet, że zbieranie identyfikatorów biometrycznych nie tylko ingeruje w życie prywatne i prawo do ochrony danych, ale **także w integralność ciała osoby**

Case: **Facebook** (obecnie Meta) i dawna funkcja "*Tag Suggestions*", czyli mechanizmu sugerowania, kto jest na danym zdjęciu. Każde zdjęcie przesłane do serwisu jest skanowane przez kilka różnych systemów.

Część algorytmów szuka na zdjęciach treści nielegalnych, drażliwych i niedostosowanych dla dzieci. Wliczają się w to np. krwawe sceny, czy choćby nagość. Inne algorytmy dużo bardziej ingerowały w prywatność, bo na każdym zdjęciu skanowały twarze wszystkich osób uwiecznionych na fotce. To dlatego Facebook mógł proponować oznaczanie znajomych.

Funkcja ta okazała się być sprzeczna m.in. z przepisami gwarantującymi prywatność (tzw. *biometric privacy law*) w Illinois za co FB/Meta został ukarany 500 mln $

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- Powszechnie uważa się, że **z uwagi na bezpieczeństwo publiczne** organy ścigania mogą co do zasady, uzasadniać pewne naruszenia życia prywatnego, uznając, że należy zachować równowagę między prawami jednostki a interesami ogółu społeczeństwa i pod pewnymi warunkami
- W swojej rezolucji Parlament Europejski uznaje sztuczną inteligencję, techniki biometryczne i powiązane technologie za **mogące zwiększyć bezpieczeństwo publiczne** w obszarze egzekwowania prawa i kontroli granic

Case: **Centrum Biometryczne Interpolu (BioHub)** uruchomione w październiku 2023 r. umożliwiło policji po raz pierwszy aresztowania już w połowie listopada 2023 r. po wykorzystaniu zdalnego sprawdzania danych biometrycznych Interpolu w celu identyfikacji podejrzanego przemytnika.

Poszukiwany za handel ludźmi od 2021 r. mężczyzna został zatrzymany podczas kontroli policyjnej w Sarajewie w Bośni i Hercegowinie. Podał fałszywe dane osobowe i użył nieprawdziwych dokumentów, próbując przedostać się do Europy Zachodniej.

Centrum Biometryczne Interpolu, umożliwiło porównanie danych biometrycznych osoby z globalną bazą danych BioHub dotyczącą odcisków palców oraz rozpoznawania twarzy. Po przesłaniu zdjęcia przemytnika do Centrum Biometrycznego od razu potwierdzono, że jest on poszukiwany w innym kraju europejskim

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- Urządzenia elektroniczne są odblokowywane za pomocą rozpoznawania twarzy i skanowania odcisków palców, a te metody identyfikacji mogą być dalej wykorzystywane do uzyskiwania dostępu do aplikacji bankowych lub kont email
- **Im więcej istnieje identyfikatorów biometrycznych jako klucz dostępu i jest w obiegu, tym jest to mniej bezpieczne i tym mniejszą kontrolę ma się nad tym, kto ma dostęp do zablokowanych przedmiotów**
- Hasła można zmienić, jeśli zostały naruszone, biometrycznych identyfikatorów nie można zmienić. W związku z tym dana osoba może nie być już w stanie bezpiecznie korzystać z uwierzytelniania biometrycznego

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

Case: **TikTok w USA** łamał federalne przepisy dotyczące prywatności i cyberbezpieczeństwa, pobierając dane dotyczące cech fizycznych i behawioralnych umożliwiających identyfikację użytkowników. Wrażliwe informacje były gromadzone z użyciem technik rozpoznawania twarzy, w celu określenia m.in. pochodzenia etnicznego, płci i wieku użytkowników. TikTok zawarł na początku 2021 r. ugodę na kwotę 92 mln $.

Case: **TikTok w USA** zmiany w polityce aplikacji dot. automatycznego zbierania danych biometrycznych, takich jak skany twarzy i próbki głosu (zwane przez TikTok: "*faceprints*" i "*voiceprints*") z treści publikowanych przez użytkowników na platformie. TikTok może także kolekcjonować dane o naturze dźwięku i treści słów wypowiadanych przez użytkownika. Te informacje zaś mają służyć do umożliwienia moderowania publikowanych na platformie filmów.

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

Case: **Clearview AI** to firma, która zasłynęła z przechwałek, że posiada największą bazę biometrycznych obrazów twarzy na świecie.

Clearview AI istotnie zgromadziła zbiór, w którym znalazło się **ponad 30 mld!,** choć firma podaje na swojej stronie **50 mld zdjęć (w styczniu 2023 było to 20 mld, a cel to 100 mld zdjęć!)** wykorzystywanych do uczenia algorytmów i zasilania baz danych skanów twarzy wiązanych z tożsamością, które wykorzystywane są m.in. przez systemy rozpoznawania twarzy.

Clearview AI dysponuje bazą danych zdjęć, które są gromadzone z mediów społecznościowych, takich jak Instagram i Facebook, a także z innych źródeł internetowych, w tym stron osobistych, zawodowych i artykułów prasowych. **Spółka pobiera te zdjęcia z Internetu, a następnie przekształca je w unikalne kody biometryczne dla każdej twarzy**.

Głównym produktem sprzedawanym przez firmę Clearview AI jest dostęp do jej baz danych. Kupują go rozmaite podmioty – od prywatnych spółek z całego świata, po organy ścigania chcące korzystać z zasobów firmy do usprawniania swojego korzystania z systemów rozpoznawania twarzy.

Clearview AI została ukarana najwyższą karą za naruszenia RODO. Karę w wysokości 30,5 miliona euro! nałożył na Clearview AI Holenderski Organ Ochrony Danych Osobowych decyzją z dnia 16 maja 2024 roku. Ponad to Organ ostrzegł Clearview AI przed możliwością nałożenia kolejnej kary w wysokości do 5,1 miliona euro za dalsze nieprzestrzeganie przepisów dotyczących ochrony danych osobowych, jeśli Spółka nie zaradzi istniejącym naruszeniom. Główny zarzut to brak podstawy prawnej do gromadzenia zdjęć twarzy, tworzenie baz danych zawierającej zdjęcia, unikalne kody biometryczne oraz inne powiązane informacje.

Clearview AI ma na swoim koncie już inne kary m.in. karę finansową w wysokości 20 mln euro nałożoną przez francuski organ ochrony danych osobowych CNIL w związku z nielegalnym gromadzeniem danych obywateli tego kraju.

Brytyjski ICO nałożył na Clearview AI w 2022 r. karę wynosząca ponad 9 milionów dolarów w związku z nielegalnym gromadzeniem zdjęć osób i tworzeniem na ich podstawie baz danych dla systemu rozpoznawania i identyfikowania twarzy.

Natomiast Clearview AI wygrała w 2023 r. apelację przeciwko brytyjskiemu organowi ochrony danych osobowych i prawdopodobnie uniknie kary. Zdaniem Trybunału, działalność firmy z USA nie podlega brytyjskiemu prawu o ochronie danych osobowych, a ICO „nie może działać eksterytorialnie”. Jeśli ICO nie odwoła się teraz od tej decyzji, grzywna z maja 2022 roku zostanie oficjalnie uchylona.

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- Przy zwiększonych możliwościach komputerów i nowych technik analizy danych, możliwe jest pozyskanie informacji z dużych zbiorów danych z bezprecedensową szybkością i w połączeniu z innymi danymi osobowymi, tym samym **intensyfikuje się ryzyko dla prywatność związane z nadzorem na dużą skalę**
- **Zdalna identyfikacja biometryczna** jest jedną z tych możliwości technologicznych, które zwiększyły **obawy etyczne dotyczące nadzoru na dużą skalę**.
- Pozwala ona na identyfikację dużej liczby jednostek, w czasie rzeczywistym, w przestrzeni publicznej, **bez jakiejkolwiek współpracy ze strony jednostek zidentyfikowanych**.
- Ataki terrorystyczne drastycznie zwiększyły rozmieszczenie telewizji przemysłowej w miejscach publicznych w połączeniu z identyfikacją biometryczną

Case: **PimEyes** zostało wykorzystane przez dziennikarzy śledczych pracujących nad materiałami dotyczącymi ataku na Kapitol w Waszyngtonie, do którego doszło 06.01.2021 r., kiedy tłum osób rozwścieczonych przegraną Donalda Trumpa w wyborach prezydenckich w USA wtargnął do budynków rządowej administracji federalnej. PimEyes posłużyło wówczas do identyfikacji konkretnych osób widocznych na zdjęciach z tych wydarzeń.

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

Case: w 2022 r. Mistrzostwa Świata w Piłce Nożnej w Katarze - film Mateusza Chroboka na YouTube: https://www.youtube.com/watch?v=s0f8LvdKxIY

Case: Chiny i polityka „zero covid” tj. masowe testowanie, doraźne i długotrwałe lockdowny, które poważnie ograniczają wolność i prawa obywateli; wymogi masowego i systematycznego testowania oraz kwarantanny, a także nieproporcjonalnych i poważnych ograniczeń swobody przemieszczania się w obrębie Chin. Ograniczenia te doprowadziły również do niedoboru podstawowych towarów, w tym żywności, do ograniczonego dostępu do opieki zdrowotnej oraz do wzrostu bezrobocia młodzieży. Ze względu na ścisłe egzekwowanie lockdownów dochodziło do odgradzania całych budynków, w tym wyjść ewakuacyjnych.

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- **Całkowity nadzór** może skutecznie **wyeliminować podstawowe prawa** do wolności słowa i zgromadzeń, które zapewniają udział w życiu politycznym i gwarantują skuteczność opozycji w systemie demokratycznym
- Na podstawie szczegółowych profili osób w połączeniu z dużymi analizą danych, **można nawet przewidzieć opinie polityczne**, a sprzeciw wobec rządu może być wyeliminowany z wyprzedzeniem

Case: **Cambridge Analytica** w USA prowadziła działania na rzecz kampanii prezydenckiej Donalda Trumpa w 2016 r. i uzyskała dostęp do danych osobowych z ponad 87 milionów (!) kont na Facebooku w celu profilowania wyborców i ich targetowania, Facebook (obecnie Meta) nie przyznał się do winy, ale zawarł ugodę na kwotę 725 mln $

Case: film na Netflix: ***Hakowanie świata*** opowiada o ww. aferze uznanej za jedną z najważniejszych afer ostatnich lat tj. Cambridge Analytica. Dokument odsłaniania wpływ zbierającej dane korporacji na kampanię prezydencką Donalda Trumpa i próbuje dowieść jej zaangażowania w Brexit. Pokazuje, jak prowadzi się w sieci wielką politykę, prezentując precyzyjne mechanizmy targetowania, które umożliwiają namierzenie osób nieprzekonanych, ustalenie cech ich osobowości, określenie, na co najlepiej zareagują i wysyłanie specjalnie pod nich skrojonego przekazu

Case: książka **Brittany Kaiser *Dyktatura danych*** również o Cambridge Analytica z punktu widzenia sygnalisty

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- Coraz więcej **urządzeń naszego codziennego użytku jest wyposażonych z czujnikami, które stale gromadzą dane o ich użytkownikach**, takie jak zachowanie, preferencje czy lokalizacja. Dzięki łączności tych urządzeń dane z różnych źródeł można ze sobą łączyć i połączone **w celu tworzenia profili użytkowników**
- Podobnie jak identyfikacja biometryczna, **monitorowanie odbywa się bez żadnej współpracy ze strony użytkowników** urządzeń lub nawet **bez wiedzy** tych użytkowników
- **Zagrożenia dla wolności i godności jednostek** mogą również powstać i bez użycia technologii biometrycznych. Śledzenie ruchów ludzi, rejestrowanie ich rozmów, analiza korzystania przez nich z podłączonych urządzeń, takich jak samochody i lodówki, aby narysować ingerencje dotyczące ich zachowania i osobowości dotyczą aspektów życia ludzkiego i głębokiej prywatności

Case: **Google** w 2019 r. potwierdził doniesienia o podsłuchiwaniu użytkowników przez urządzenia z Asystentem Google, który faktycznie nagrywał i wysyłał na serwery dźwięki otoczenia, w tym prywatne rozmowy, gdzie później były przesłuchiwane przez pracowników Google i pracowników zewnętrznych firm.

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

Case: **Revolut w USA** użytkownicy wnieśli pozew przeciwko fintechowi, że nielegalnie gromadził, przechowywał i wykorzystywał dane biometryczne swoich klientów wykorzystywane w procesie zakładania konta (użytkownik musi zeskanować swoją twarz i przesłać do porównania zdjęcie dokumentu tożsamości).

Zdaniem klientów ze stanu Illinois (USA), nie byli oni właściwie informowani o całym procesie gromadzenia i przetwarzania danych. W efekcie zdecydowano się wnieść pozew o naruszenie prywatności. Poszkodowani powołują się na obowiązującą w tym stanie ustawę o biometrii (BIPA - Biometric Information Privacy Act). Regulacje zawarte w BIPA przewidują odszkodowania w wysokości do 5000 dolarów za każde naruszenie prywatności. Oznacza to, że Revolutowi może grozić nawet kilka milionów kary. Firma nie odniosła się szczegółowo do stawianych zarzutów.

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

Case: **Worldcoin** projekt oficjalnie uruchomiony w lipcu 2023 r. i finansowany przez inwestorów z Doliny Krzemowej, który zbiera dane biometryczne za obietnicę wynagrodzenia w kryptowalucie (**58 tokenów! Kurs na dzień 17.12.2024 to 2,85 USD, czyli ok. 165 USD/670 PLN**). Jego współzałożycielem jest Sam Altman, dyrektor generalny OpenAI, czyli spółki stojącej za ChatGPT.

Koncepcja projektu polega na zapewnieniu ludzkości dochodu podstawowego w postaci cyfrowej waluty WLD. Zdaniem Altmana AI wyeliminuje w najbliższych latach wiele zawodów, a worldcoin to sposób, by podzielić się ze społeczeństwem pieniędzmi wygenerowanymi podczas tej rewolucji. Żeby zweryfikować, że środki trafiają do ludzi, a nie do botów, twórcy projektu wymyślili, że dołączanie do niego będzie odbywać się poprzez skanowanie tęczówki. Zdjęcie wykonuje urządzenie w kształcie kuli o nazwie Orbs. Projekt twierdzi, że gwarantuje użytkownikom zachowanie anonimowości, dzięki wykorzystaniu technologii blockchain. Urzędnicy z kilku państw mają co do tego wątpliwości. Firma posiada **15 milionów użytkowników!**, którzy zweryfikowali już swoją tożsamość za pomocą Orba

Francuski organ ds. prywatności (CNIL) sonduje Worldcoin podobnie jak regulatorzy z Niemiec i Wielkiej Brytanii. Wątpliwości budzi mechanizm zakładania portfeli, opierający się na skanowaniu oka w celu potwierdzenia tożsamości.

Hiszpański sąd wydał w 2024 r. orzeczenie zakazujące sprzedaży danych biometrycznych obywateli. Decyzja sądu jest werdyktem w sprawie firmy Worldcoin, która wytoczyła proces Hiszpańskiej Agencji Danych Osobowych (AEPD), kiedy ta zakazała spółce nabywania za kryptowalutę danych biometrycznych obywateli.

W trakcie rozprawy potwierdzono, że spółka Worldcoin pozyskiwała dane dotyczące tęczówki oka, a także twarzy. Nie zawsze, jak ustalono, osoby przekazujące swoje dane w zamian za kryptowalutę wyrażały zgodę na obrót swoimi danymi.

Hiszpański sąd potwierdził też, że doszło do przypadków pozyskiwania danych biometrycznych od nieletnich, a także od osób nieświadomych tego, że ich dane będą w przyszłości przekazywane innym podmiotom.

Według szefostwa Worldcoin skanowanie tęczówek i twarzy osób służy stworzeniu tzw. paszportu ludzkości, który ma pozwolić odróżnić ludzi od sztucznej inteligencji w Internecie, zaś opłaty w kryptowalutach były jedynie formą wynagradzania wolontariuszy.

W październiku 2024 r. ogłoszono, że Worldcoin, przechodzi rebranding. Od teraz jest to po prostu „World” lub „World Network” i wprowadza na rynek nową wersję Orba, swojego narzędzia skanującego tęczówkę oka.

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

Case: **CupCut**, ByteDance (firma-matka TikToka), została pozwana w Illinois. Według zarzutów, firma ta miała korzystać bez uprawnień z danych **ponad 200 milionów użytkowników!** popularnej aplikacji, CapCut, której także jest twórcą. To stanowi poważne oskarżenie dotyczące naruszenia prywatności.

Pozew wynika z tego, że CapCut nie dostarczał użytkownikom wystarczających informacji dotyczących sposobu gromadzenia i wykorzystania danych.

Obawy o prywatność związane z CapCut skupiają się na fakcie, że jest to produkt chińskiej firmy, co mogłoby wiązać się z udostępnianiem danych rządowi chińskiemu przez amerykańską firmę-matkę ByteDance.

Proces bazuje na oświadczeniu byłego pracownika ByteDance z maja 2023 roku, który wskazywał na możliwość dostępu chińskiego rządu do danych użytkowników. Roszczenia zawarte w pozwie obejmują **również nielegalne gromadzenie danych biometrycznych**.

CapCut celowo tworzył mylącą i niejasną politykę prywatności, potencjalnie wprowadzając użytkowników w błąd i zachęcając ich do wyrażenia zgody na praktyki wykorzystujące ich dane.

CapCut miał gromadzić: zdjęcia, filmy, lokalizację, płeć, datę urodzenia oraz szczegóły urządzenia, które miały służyć reklamom i rozwojowi sztucznej inteligencji. Tak więc, aplikacja służąca do edycji treści musi być szczególnie dokładnie zbadana, ponieważ to tam trafiają wideo i zdjęcia w oryginalnej formie - które często nie są publikowane.

ETYCZNE ASPEKTY ZWIĄZANE Z KATEGORYZACJĄ BIOMETRYCZNĄ

ETYCZNE ASPEKTY ZWIĄZANE Z KATEGORYZACJĄ BIOMETRYCZNĄ

- Główne kwestie etyczne podnoszone przez kategoryzację biometryczną jednostek ludzkich (np. przydział do grup ryzyka w ramach systemu bezpieczeństwa lotniska, ocena kandydatów do pracy) są związane z **rozwojem i konkretnym wykorzystaniem** systemów kategoryzacji
- **Problemy etyczne pojawiają się w związku z definicją kategorii**, powiązanymi założeniami i wnioskami lub reakcjami wywołanymi przez system, prowadząc do zagrożeń takich jak: **dyskryminacja, stygmatyzacja i wyciąganie niewłaściwych wniosków.** Dalsze ryzyko obejmuje **manipulację i wykorzystywanie luk w zabezpieczeniach**
- Podczas gdy, identyfikacja biometryczna zwykle wykorzystuje „silne” identyfikatory biometryczne w celu jednoznacznej identyfikacji osób, **systemy kategoryzacji biometrycznej mogą również wykorzystywać „miękką” biometrię**, pozwala tylko na przypisanie osoby fizycznej do określonej grupy lub kategorii osób
- Takie kategorie mogą być związane z funkcjami, które normalnie byłyby wyraźnie widoczne dla człowieka, takie jak: pochodzenie etniczne, płeć, niepełnosprawność lub wiek.
- Kategorie mogą być również znacznie bardziej wyrafinowane, na przykład odnoszące się do konkretnego kontekstu regionalnego, konkretnej grupy ryzyka lub pewnej cechy osobowości

ETYCZNE ASPEKTY ZWIĄZANE Z KATEGORYZACJĄ BIOMETRYCZNĄ

- Problemy etyczne nie tylko odnoszą się **do działań dyskryminacyjnych** w oparciu o ustalone kategorie (takie jak odfiltrowywanie kandydatów do pracy na podstawie ich pochodzenia etnicznego lub płci), ale mogą też dotyczyć **konstrukcji kategorii**.
- **Definiowanie** niektórych kategorii **może być rażąco nieetyczne** już na początku, jeśli opiera się **na nienaukowych, dyskryminujących przekonaniach i poglądach** (np. jeśli ludzie są klasyfikowani jako „lepsi” i „gorsi”)
- Kategorie **mogą być same w sobie kontrowersyjne** z etycznego punktu widzenia, np. kategoria „rasa”, która jest wyraźnie zakorzeniona w myśleniu i musi być postrzegane w świetle historycznej i współczesnej dyskryminacji rasowej
- Wykorzystanie **zautomatyzowanego podejmowania decyzji** dodaje kolejną warstwę problemów etycznych
- Stosowanie systemów rozpoznawania biometrycznego do automatycznej kategoryzacji ludzi niesie ze sobą również ryzyko, że **błędna kategoryzacja może stanowić podstawę decyzji naruszających prawa podstawowe,** np. odmowa azylu

ETYCZNE ASPEKTY ZWIĄZANE Z KATEGORYZACJĄ BIOMETRYCZNĄ

Case: film na Netflix ***Dylemat społeczny***, w którym pojawia się teza, że to algorytmy social mediów wpływają na polaryzację społeczeństwa.

Jeśli ktoś pasjami ogląda społecznie zaangażowane, lewicowe treści, to właśnie te będą mu podsuwały Facebook czy Twitter. Dostanie powiadomienia o protestach w obronie praw kobiet oraz propozycje dołączenia do grup osób o podobnych zainteresowaniach.

Z kolei jeśli ktoś ogląda vlogi antyszczepionkowców czy lajkuje posty, które dowodzą, że pandemia koronawirusa to zwykły blef, to algorytmy wyszukają mu treści właśnie tego typu. Nacjonalistyczne strony, antycovidowe grupy, skrajnie prawicowe filmy – YouTube czy Google nie pomogą mu poszerzyć horyzontów, bo wcale nie zaproponują mu innych materiałów.

Dokument Netflixa alarmuje więc, że "żyjemy w bańce poglądów".

„Skoro nie płacisz za produkt, to sam jesteś produktem”

ETYCZNE ASPEKTY ZWIĄZANE Z KATEGORYZACJĄ BIOMETRYCZNĄ

- Ryzyko błędnej kategoryzacji przez systemy algorytmiczne jest znacznie bardziej niebezpieczne niż błędna kategoryzacja przez ludzi z uwagi na skalowalność
- Gdy sztuczna inteligencja i inne systemy algorytmiczne są wykorzystywane w celu przypisania osób do określonych kategorii ze względu na ich cechy fizyczne, fizjologiczne lub behawioralne, to osoby są narażone na ryzyko dyskryminacji i błędnej klasyfikacji

Case: **System zaufania społecznego w Chinach,** czyli zakrojony na ogólnokrajową skalę projekt realizowany na przestrzeni ostatnich lat przez ChRL. Polega na stworzeniu systemu oceny społecznej, który na podstawie danych zbieranych na przestrzeni ostatnich dziesięcioleci i przechowywanych w sposób analogowy w państwowych archiwach jak i docelowo z pomocą najnowszych technologii, w tym technologii przesyłania danych w czasie rzeczywistym 5G, technologii rozpoznawania twarzy *face recognition* oraz sztucznej inteligencji, będzie tworzył profile obywateli ChRL i firm działających na terytorium Chin.

- Prawo kwestionowania przez osobę automatycznej kategoryzacji przewidzianej w art. 22 RODO jest podstawowym zabezpieczeniem zapewnienia przynajmniej pewnego rodzaju kontroli nad decyzjami związanymi z kategoryzacją

ETYCZNE ASPEKTY ZWIĄZANE Z WYKRYWANIEM BIOMETRYCZNYM

ETYCZNE ASPEKTY ZWIĄZANE Z WYKRYWANIEM BIOMETRYCZNYM

- Podczas gdy techniki identyfikacji i kategoryzacji zadają pytania *„Kim jesteś?”* lub *„Do której grupy należysz*?”, techniki wykrywania pytają *„Jak się masz*?” i *„Co zamierzasz zrobić*?”.
- Kwestie etyczne podnoszone przez biometryczne wykrywanie stanów ludzkich (np. zamiar popełnienia przestępstwa, strachu, zmęczenia lub choroby) wynikają z **potencjalnie natrętnego charakteru, często analizującego bardzo intymne cechy, niektóre z nich poza świadomością jednostki**
- Większość problemów etycznych związanych z zastosowaniem wykrywania biometrycznego nie odnosi się konkretnie do samego faktu, że **dane biometryczne są wykorzystywane** do wnioskowania o stanie, ale **do wykrycia tego stanu jako takiego**
- Faktem jest, że **jednostka ma niewielką kontrolę nad swoim sygnałami** fizycznym, fizjologicznymi lub behawioralnymi, z których wiele będzie podświadomych
- W zakresie wykrywania biometrycznego to **systemy wykrywające ludzkie emocje, myśli i intencje** zasługują na szczególną uwagę z uwagi na perspektywę etyczną i regulacyjną, taką jak **prawo do prywatności i integralności psychicznej**
- Wykrywanie biometryczne będzie połączone z pewnego rodzaju automatyczną kategoryzacją opartą na wnioskach i predykatach, takich jak „potencjalny agresor” lub „potencjalne zagrożenie”

ETYCZNE ASPEKTY ZWIĄZANE Z WYKRYWANIEM BIOMETRYCZNYM

- Identyfikatory te generalnie pozwalają na wyciąganie wniosków na temat ludzkich zachowań, mają szerokie pole do zastosowania, takie jak marketing ukierunkowany lub obliczanie składek ubezpieczeniowych i nie ograniczają się tylko do egzekwowania prawa i celów bezpieczeństwa
- Cechą charakterystyczną jest to, że chociaż ludzie mogą być w stanie ćwiczyć jakiś rodzaj kontroli nad tymi identyfikatorami, to są **one w większości sytuacji kontrolowane przez podświadomość**
- Wiele danych biometrycznych, takich jak chód czy dynamika mimiki, nie wymaga kontaktu lub partycypacji ze strony jednostki, a nawet może być uchwycony z dystansu, zwiększając ryzyko, że osoby są analizowane bez ich wiedzy

Case: **Chiny i opaska EEG.** Uczniowie w 2019 r. w jednej ze szkół nakładali opaski z EEG na głowy podczas rozpoczęcia lekcji. Urządzenia mierzyły sygnały fal mózgowych i w ten sposób pokazywały, czy uczniowie w odpowiednim stopniu skupiają się na przyswajaniu wiedzy. Poziom skupienia jest sygnalizowany kolorową diodą na opasce oraz w formie wykresów przesyłanych do komputera na biurku nauczyciela, ale również do rodziców, którzy mogą śledzić wyniki np. na smartfonie. Dane trafiają też do rządowych agencji badawczych.

ETYCZNE ASPEKTY ZWIĄZANE Z WYKRYWANIEM BIOMETRYCZNYM

- **Techniki wykrywanie mogą ujawniać wysoce prywatne informacje**, takie jak osobiste problemy zdrowotne i niepełnosprawności, które nie były wcześniej znane odpowiednim osobom
- Analiza identyfikatorów biometrycznych **może dostarczyć wskazówek o zamiarach człowieka, jego wewnętrznej motywacji lub planowanych działaniach**, ale nigdy nie może być twardym dowodem
- Oparcie decyzji na danych biometrycznych behawioralnych gromadzonych w przestrzeni publicznej może mieć poważny i mrożący wpływ na społeczeństwo, ponieważ ludzie mogą poprzez swoje zachowania zostać zaklasyfikowani jako podejrzani przez biometryczne systemy wykrywania i mogą zmieniać swoje zachowania w miejscach publicznych
- Również zawodność techniki wykrywania biometrycznego **zwiększa ryzyko umieszczania osób w kategoriach stygmatyzujących**, gdy informacja zostanie upubliczniona, tego rodzaju stygmatyzacja może trwać, nawet jeśli błąd zostanie naprawiony
- Niezwykle ważne jest, aby **profile biometryczne były chronione wysokimi standardami bezpieczeństwa i były regularnie przeglądane i aktualizowane**

ETYCZNE ASPEKTY ZWIĄZANE Z WYKRYWANIEM BIOMETRYCZNYM

Case: **Technika PrintListener,** zespół naukowców ze Stanów Zjednoczonych i Chin wykazał, że **wyłącznie na podstawie dźwięków przesuwania palcem po ekranie dotykowym** udało się uzyskać aż 27,9% częściowych i 9,3% kompletnych odcisków palców w ciągu pięciu prób przy najwyższym ustawieniu bezpieczeństwa systemu.

W jednym na cztery ataki technika, którą nazwano PrintListener była w stanie skutecznie złamać system automatycznej identyfikacji odcisków palców (AFIS) przy użyciu częściowych odcisków palców, a w prawie jednym na dziesięć przypadków przy użyciu całych odcisków palców.

Algorytmy używane do wygenerowania odcisku palca na podstawie izolowanych dźwięków tarcia, wmieszanych w hałas tła są niezwykłe skomplikowane. Należy wziąć pod uwagę również czynniki fizjologiczne i behawioralne, ponieważ mogą one wpływać na dźwięk wydawany przez palec na ekranie. Wykorzystane techniki identyfikują poszczególne fragmenty odcisku palca na podstawie charakterystyki dźwięku tarcia, które można następnie wykorzystać do wygenerowania syntetycznych odcisków palców.

Źródłem dźwięków przesuwania palcem mogą być popularne aplikacje, takie jak Discord, Skype, WeChat, FaceTime czy każda dowolna aplikacja do czatowania, w której użytkownicy bezmyślnie przesuwają palcem po ekranie, gdy mikrofon urządzenia jest włączony. W zasadzie każde nasze użytkowanie smartfonów w całości polega na przesuwaniu po nim palcami. W związku z tym dźwięki tarcia palca mogą z dużym prawdopodobieństwem zostać przechwycone przez osoby atakujące w Internecie.

Szacuje się, że do 2032 r. rynek uwierzytelniania odcisków palców będzie wart prawie 100 miliardów dolarów. Liczne firmy wykorzystujące te metody oraz sami użytkownicy sprzętu musza być coraz bardziej świadomi, że grupy przestępcze mogą spróbować ukraść ich odciski palców.

„Biometria (…) zmienia w sposób nieodwracalny stosunek pomiędzy ciałem a tożsamością: cechy ciała ludzkiego stają się przedmiotem odczytu maszynowego i mogą być dalej wykorzystywane.

Nawet jeśli cechy biometryczne nie są rozpoznawalne dla ludzkiego oka, to można je zawsze odczytać i wykorzystać przy zastosowaniu odpowiednich narzędzi, bez względu na miejsce przebywania danej osoby”

Opinia Europejskiego Inspektora Ochrony Danych Osobowych z dnia 23 marca 2005 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Systemu Informacji Wizowej (VIS) oraz wymiany danych pomiędzy Państwami Członkowskimi na temat wiz krótkoterminowych

„Skoro nie płacisz za produkt, to sam jesteś produktem”

Cytat z filmu *Dylemat Społeczny*

DZIĘKUJĘ ZA UWAGĘ!

Marta Kozioł

koziolm21@gmail.com

Wrocław, 18.12.2024 r.