



PRAWNE I ETYCZNE ASPEKTY BIOMETRII

AUTOR: MARTA KOZIOŁ

WROCŁAW, 13.01.2021

AGENDA:

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



DANE BIOMETRYCZNE



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

Norma ISO/IEC 2382:2015 Information technology – Vocabulary

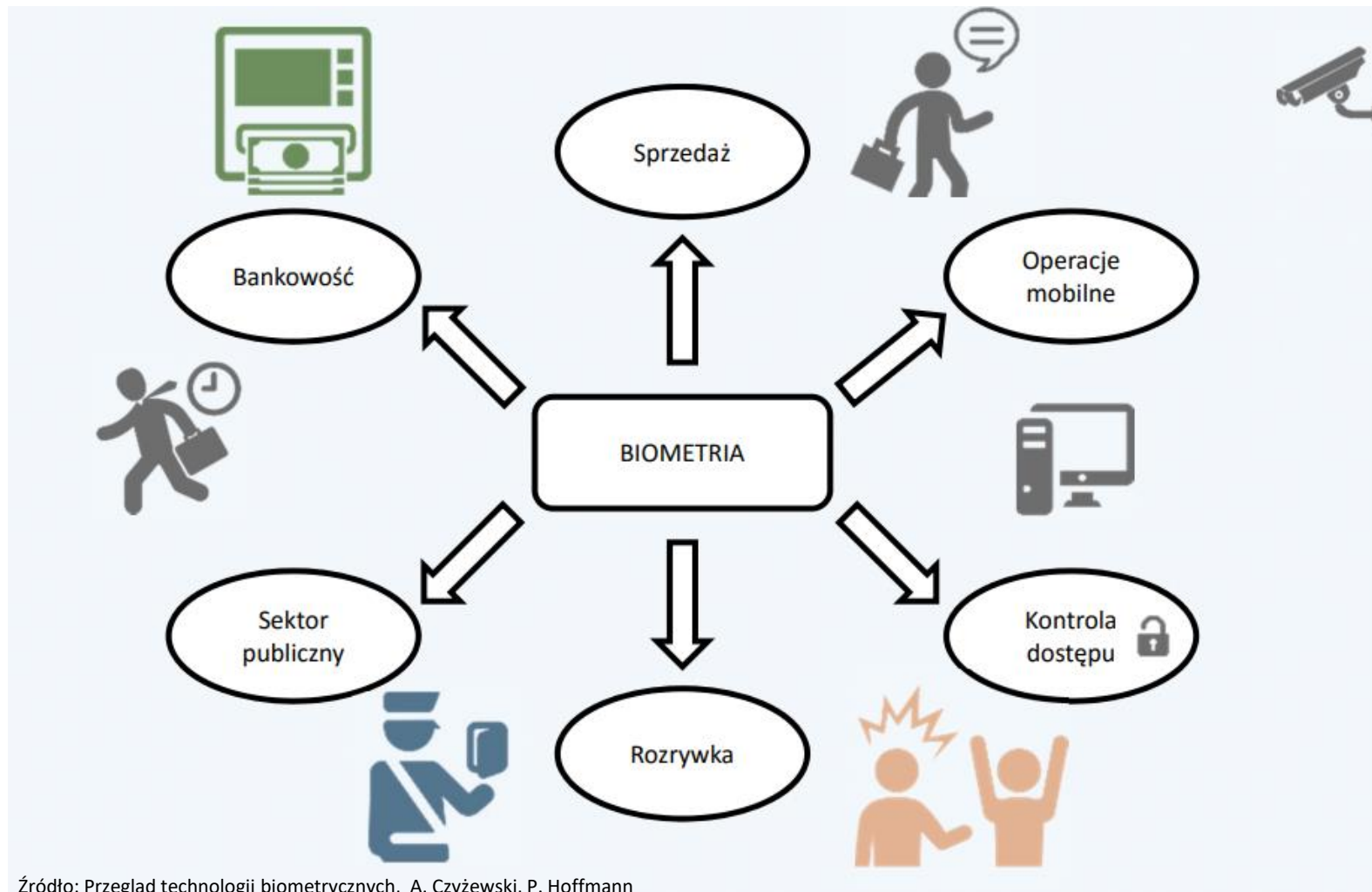


system, którego zadaniem jest automatyczne rozpoznanie lub uwierzytelnienie osoby fizycznej na podstawie jej cech biologicznych lub behawioralnych.

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

BIOMETRIA

SYSTEM BIOMETRYCZNY



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

OBSZARY ZASTOSOWAŃ BIOMETRII



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

DANE BIOMETRYCZNE

FORMY WYSTĘPOWANIA DANYCH BIOMETRYCZNYCH

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

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

The background of the slide is a dark, abstract composition. It features numerous thin, white, wavy lines that flow across the frame, creating a sense of motion and depth. Interspersed among these lines are many small, bright white dots and larger, fainter circular bokeh-like shapes. The overall effect is reminiscent of a digital or scientific visualization, such as a particle simulation or a data flow map. On the left side, there is a solid dark red vertical bar that serves as a container for the title text.

TECHNOLOGIE BIOMETRYCZNE

TECHNOLOGIE BIOMETRYCZNE

należy rozumieć jako obejmujące 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

TECHNIKI BIOMETRYCZNE

*Biometria
odcisku palca*

*Biometria
tęczówki*

*Biometria
siatkówki*

*Biometria
podpisu*

*Biometria
głosowa*

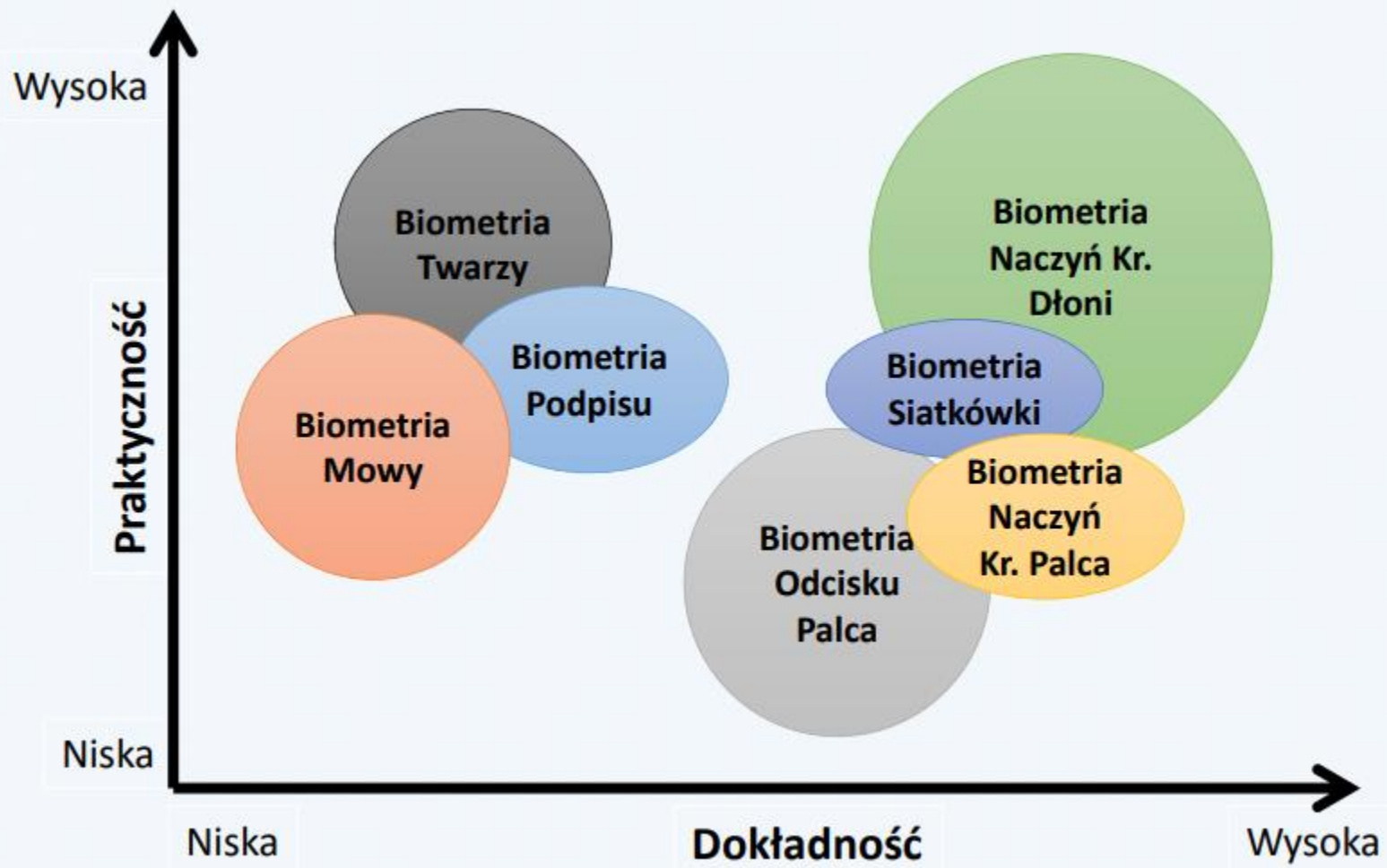
*Biometria
kształtu ucha*

*Biometria
kształtu
twarzy*

*Biometria
chodu*

*Biometria
układu żył*

DNA



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

KLASYFIKACJA CECH BIOMETRYCZNYCH

TECHNOLOGIE BIOMETRYCZNE

Dane biometryczne można podzielić na różne sposoby, jednym z nich jest podział 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.

Ludzie nie są już potrzebni do przechwytywania, przetwarzania i porównywania identyfikatorów biometrycznych, umożliwiając czysto automatyczną identyfikację.

TECHNOLOGIE BIOMETRYCZNE

Powszechny jest podział na **pierwszą i drugą generację** technologii biometrycznych.

Technologie biometryczne **pierwszej generacji**:

- Koncentrowały się 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
- Od tego czasu biometria pierwszej generacji stała się bardziej niezawodna i zaawansowana, dzięki czemu znacznie zmniejszono liczbę błędów udoskonalonej technologii komputerowej (zwłaszcza w technologiach rozpoznawania twarzy)
- 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

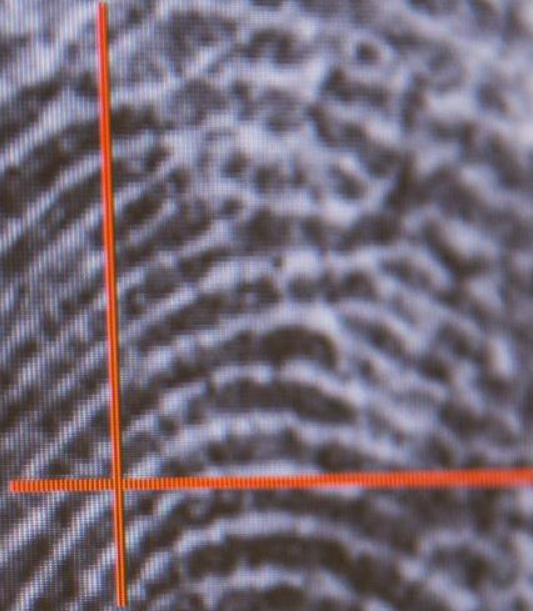
TECHNOLOGIE BIOMETRYCZNE

Technologie biometryczne **drugiej generacji**:

- Skupiają 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 oraz diagnostyka medyczna
- Oferuje nowe możliwości organom ścigania i kontroli granicznej, umożliwiając m.in. w celu wykrycia 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
ORAZ
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
(1:N)



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

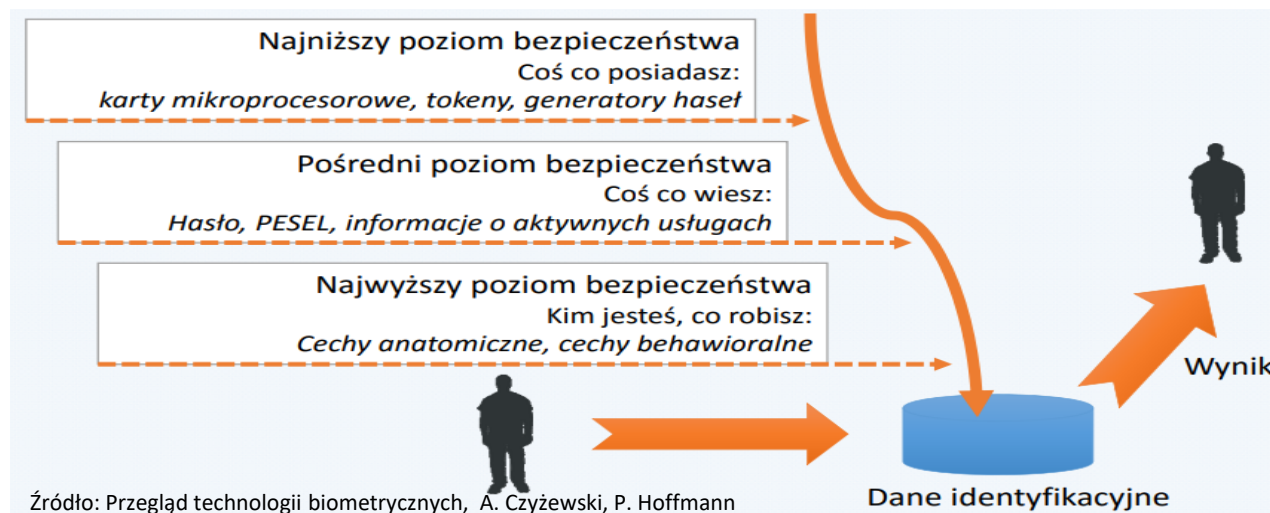
analiza cech użytkownika, a następnie porównanie ich ze wszystkim dostępnymi wzorcami w bazie

WERYFIKACJA

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

UWIERZYTELNIANIE

proces weryfikacji tożsamości użytkownika, sprawdzenie, kontrola zgodności z prawdą, określenie autentyczności, stwierdzenie, poświadczenie prawdziwości również z uwzględnieniem określonego prawdopodobieństwa



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

KATEGORYZACJA BIOMETRYCZNA

- Jest terminem mniej powszechnym niż *identyfikacja biometryczna*, ponieważ wzrost technik kategoryzacji biometrycznej nastąpił dopiero wraz ze wzrostem wykorzystania technologii biometrycznych słabych i miękkich
- 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 lub stan zdrowia
- 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



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

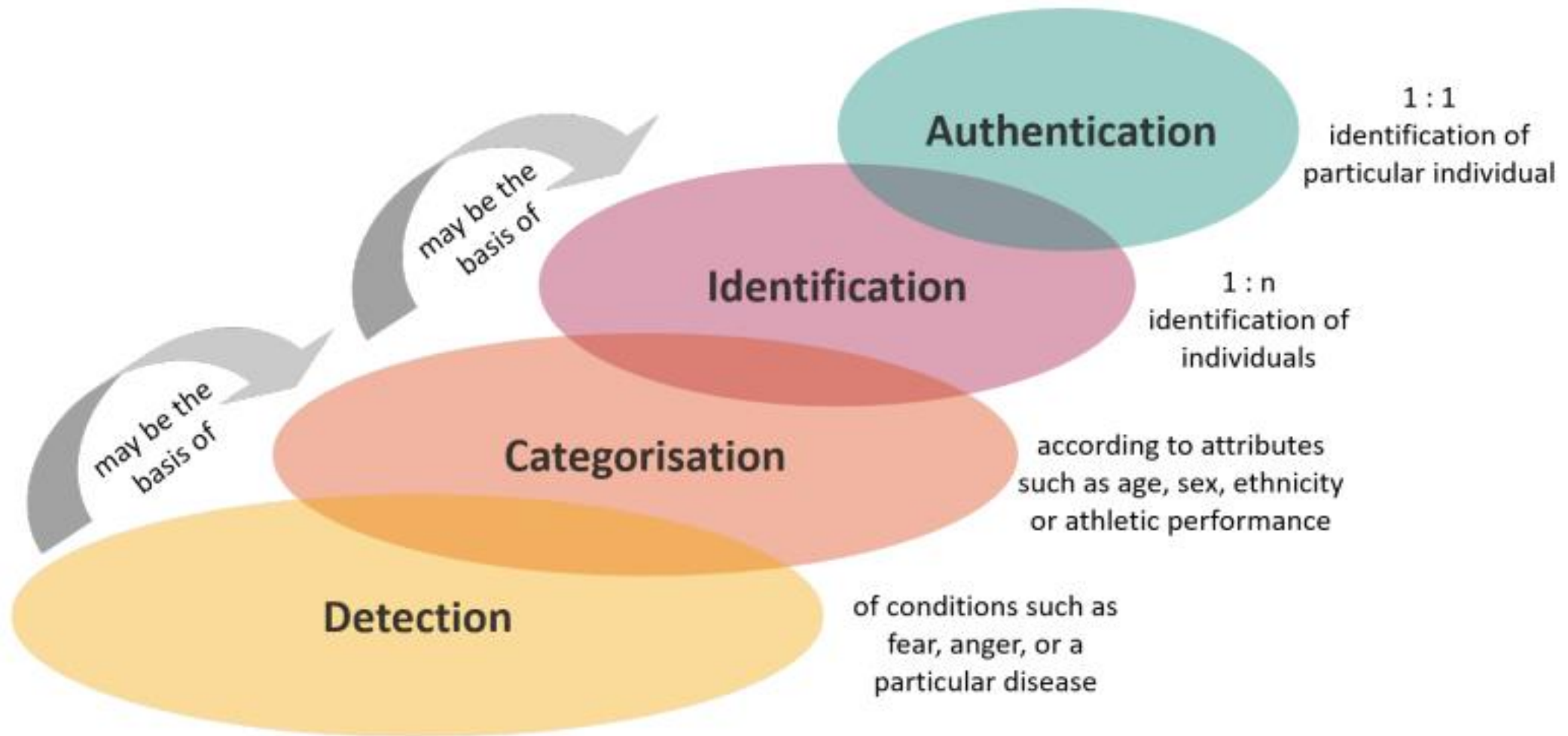


Ostatnio pojawiły się systemy rozpoznawania emocji, czyli systemy identyfikacji lub wnioskowania z emocji, myśli lub intencji osób na podstawie biosygnatów, które wiążą się z szeregiem problemów etycznych



Wraz z rosnącym wykorzystaniem słabej i/lub miękkiej biometrii oraz coraz szerszej gamy biosygnatów 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

WYKRYWANIE BIOMETRYCZNE



Source: Christiane Wendehorst

„BIOMETRYCZNY”

oznacza pewien stopień
niezmiennność, 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 -
USTAWODASTWO**



PRAWNE ASPEKTY BIOMETRII - 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

Projekt rozporządzenia w
sprawie sztucznej inteligencji
w UE (AIA)

EUROPEJSKA KONWENCJA PRAW CZŁOWIEKA (EKPC)

- W odniesieniu do technik biometrycznych w EKPC szczególnej uwagi wymagają: 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
- Stosowanie technik biometrycznych do celów nadzoru może dodatkowo 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)

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

KARTA PRAW PODSTAWOWYCH UNII EUROPEJSKIEJ (KPP UE)

- W kontekście obowiązującego prawodawstwa UE regulującego techniki biometryczne, prawo do poszanowania życia prywatnego i ochrona danych osobowych są szczególnie godne uwagi, ponieważ 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”
- Godność człowieka jest również wymieniona w art. 2 Traktatu o Unii Europejskiej (TUE) wraz z wolnością, demokracją, równością, praworządnością i poszanowaniem praw człowieka jako wartości, na której opiera się UE
- 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
- W przeciwieństwie do art. 14 EKPC zakaz dyskryminacji na podstawie art. 21 KPP UE nie jest powiązany z innymi podstawowymi prawami KPP UE

ROZPORZĄDZENIE O OCHRONIE DANYCH OSOBOWYCH (RODO)

- Zgodnie z RODO prawodawca unijny nie tylko wprowadził definicję „danych biometrycznych”, ale także nałożył surowe wymagania dotyczące przetwarzania danych biometrycznych
- Zgodnie z RODO dane biometryczne *„oznaczają dane osobowe wynikające” z określonego przetwarzania technicznego związanego z cechami fizycznymi, fizjologicznymi lub behawioralnymi a osoba fizyczna, które umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby fizycznej, np. obraz twarzy lub dane daktyloskopijne*
- Fotografie powinny podlegać definicji danych biometrycznych tylko wówczas, gdy fotografia ulega „podczas przetwarzania za pomocą określonych środków technicznych pozwalających na niepowtarzalność” identyfikacji lub uwierzytelnieniu osoby
- Dane biometryczne mogą być przetwarzane tylko wtedy, gdy zachodzi jedna z podstaw określonych w art. 6 ust. 1 RODO. Przetwarzanie jest m.in. uzasadnione, jeżeli osoba, której dane dotyczą wyraziła na to zgodę lub jeżeli: przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku przetwarzania
- Przetwarzanie danych biometrycznych może stwarzać poważne zagrożenia dla praw podstawowych osób, których dane dotyczą, a art. 9 ust. 1 RODO 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

ROZPORZĄDZENIE O OCHRONIE DANYCH OSOBOWYCH (RODO)

- RODO ogranicza również stosowanie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach (profilowanie)
- Art. 22 ust. 1 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 (i) jest to konieczne do zawarcia lub wykonania umowy, (ii) dozwolone na mocy prawa Unii lub prawa państwa członkowskiego, lub (iii) 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: wyrazi na to wyraźną zgodę lub jeśli 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 nie daje podstaw do zgodnego z prawem przetwarzania danych osobowych, a jedynie ustawia ogólne zasady dla organów ścigania
- Zgodnie z art. 10 LED 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: (i) być dozwolone na mocy prawa Unii lub prawa państwa członkowskiego, (ii) chronić żywotne interesy osoby, której dane dotyczą, lub innej osoby fizycznej, lub (iii) dotyczyć danych, które: zostały w sposób oczywisty upublicznione przez osobę, której dane dotyczą
- Jeżeli przetwarzanie narusza Artykuł 10 LED, dane podmiotom przysługuje prawo żądania usunięcia dotyczących ich danych

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

- Zgodnie z art. 11 LED, wykorzystanie zautomatyzowanego podejmowania decyzji opartych 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, w tym: poufność i aktualny stan wiedzy, zwłaszcza w zakresie szczególnych kategorii danych osobowych jak dane biometryczne.
- 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

- Zgodnie z art. 1 ust. 2 rozporządzenia paszporty i dokumenty podróży wydane przez Państwa członkowskie 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
- Artykuł 1 lit. b) wyjaśnia, że tylko personel krajowego organu odpowiedzialnego za wydawanie paszportów są upoważnione 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

- W kontekście kontroli granic i bezpieczeństwa istnieje kilka przepisów UE, które pozwalają na zbieranie, przechowywanie i udostępnianie danych biometrycznych
- Najbardziej godne uwagi jest rozporządzenie w sprawie systemu wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich (EES rozporządzenie), które stanowi centralny element Pakietu Smart Border Komisji Europejskiej
- Również warte uwagi, w związku z wykorzystaniem technik biometrycznych do zabezpieczenia granic są: rozporządzenia tworzące System Informacyjny Schengen (SIS), decyzja z Prüm, System EURODAC (European Dactyloscopy), który był pierwszą ogółouropejską biometryczną bazą danych umożliwiającą porównanie odcisków palców osób ubiegających się o azyl

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 dowolnego państwa trzeciego obywateli przekraczających granicę strefy Schengen. Informacje te są łączone z danymi daktyloskopijnymi, a wizerunek twarzy i informacje w dokumencie 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 danych zgodnie z KPP UE i EKPC
- Europejskie Inspektor Ochrony (EIOD) wskazał, że system EES stanowi znaczną ingerencję z art. 7 i 8 KPP UE, ponieważ przetwarza dane wrażliwe i ma wpływ na dużą liczbę osób
- 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 Prüm decyzja 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 są Norwegia, Szwajcaria i Islandia

PROJEKT ROZPORZĄDZENIA W SPRAWIE SZTUCZNEJ INTELIGENCJI W UE

- Wiosną 2021 r. Komisja Europejska opublikowała wniosek dotyczący rozporządzenia określającego zasady dotyczące sztucznej inteligencji, tzw. akt o sztucznej inteligencji (AIA).
- Komisja zdecydowała się na podejście oparte na ryzyku, a zatem rozróżnia zastosowania sztucznej inteligencji, które tworzą (i) i niedopuszczalne ryzyko, (ii) wysokie ryzyko oraz (iii) niskie lub minimalne ryzyko. W zależności od klasyfikacji ryzyka
- AIA dotyczy w szczególności systemów identyfikacji biometrycznej i wykorzystania sztucznej inteligencji do przetwarzania danych biometrycznych
- Przetwarzanie danych biometrycznych jest wymienione w załączniku III do AIA jako wysokiego ryzyka system. Oznacza to, że ich użycie nie jest zabronione, ale podlega szeregowi obowiązkowych wymogów
- Wymagania te obejmują m.in. wdrożenie systemu zarządzania ryzykiem oraz odpowiednie praktyki zarządzania danymi i zarządzania, a także zapewnienie przejrzystości i odpowiedni nadzór ludzki
- Dostawca sztucznej inteligencji wysokiego ryzyka musi przestrzegać bardziej rygorystycznych procedur oceny zgodności, z udziałem jednostki notyfikowanej, chyba że system jest w pełni zgodny z normami zharmonizowanymi. W tym ostatnim przypadku procedura oceny zgodności oparta na wewnętrznych kontroli jest wystarczająca

PROJEKT ROZPORZĄDZENIA W SPRAWIE SZTUCZNEJ INTELIGENCJI W UE

- Wykorzystanie sztucznej inteligencji do zdalnych systemów identyfikacji biometrycznej „w czasie rzeczywistym” w miejscach publicznie dostępnych dla prawa celów egzekwowania prawa jest uważane za „niedopuszczalne ryzyko” i dlatego jest zabroniona
- Natomiast stosowanie sztucznej inteligencji do zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” jest bezwzględnie konieczne w poszukiwaniu ofiar przestępstw, zapobieganiu konkretnemu bezpośredniemu zagrożeniu życia lub poszukiwaniu sprawcy określonych przestępstw
- Należy wziąć pod uwagę wagę, prawdopodobieństwo i skalę szkody, gdyby system nie został wykorzystany, a także konsekwencje dla prawa i wolności osób poszkodowanych
- Zdalna identyfikacja biometryczna „w czasie rzeczywistym” musi przestrzegać niezbędnych i proporcjonalnych zabezpieczeń i warunków w związku z użytkowaniem, w szczególności w zakresie ograniczeń czasowych, geograficznych i osobistych. Kolejnym warunkiem jest obowiązkowy uprzednie zezwolenie wydane przez sąd lub niezależny organ administracyjny, które może być w należycie uzasadnionych pilnych sytuacjach

PRAWNE ASPEKTY
BIOMETRII -
ORZECZNICTWO



PRAWNE ASPEKTY BIOMETRII - ORZECZNICTWO

Orzecznictwo
Europejskiego
Trybunału Praw
Człowieka (ETPCz)

Orzecznictwo
Trybunału
Sprawiedliwości Unii
Europejskiej (TSUE)

Orzecznictwo
polskie - WSA i NSA

ORZECZNICTWO EUROPEJSKIEGO TRYBUNAŁU PRAW CZŁOWIEKA (ETPCz)

- Pierwsza sprawa, dotycząca przechowywania danych biometrycznych, związana jest z **przechowywaniem zdjęć skazanych terrorystów w Irlandii**. ETPCz uznał, że przechowywanie i przetwarzanie 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**. Według ETPCz zdolność profilu DNA do dostarczania środków do identyfikacji genetycznych w relacji między jednostkami jest sama w sobie wystarczająca do stwierdzenia, że ich przechowywanie narusza prawo do życia prywatnego jednostek.
- 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 zwrócono się do TSUE z pytaniem, czy art. 1 ust. 2 rozporządzenia nr 2252/2004, który zobowiązuje organy państwowe do pobierania i przechowywania odcisków palców przy wydawaniu paszportu, narusza prawa osoby do poszanowanie życia prywatnego i ochrona danych osobowych?
- TSUE stwierdził, że **przetwarzanie odcisków palców** nie wykracza poza to, co jest konieczne do osiągnięcia celu rozporządzenia, jakim jest ochrona przeciwko nielegalnemu używaniu paszportów.
- TSUE wyraźnie wspomniał, że niezgodność między odciskami palców posiadacza paszportu, a danymi w tym dokumentie 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
- TSUE podkreślił, że rozporządzenie nr 2252/2004 daje również wystarczające gwarancje, że dane nie są wykorzystywane do żadnych innych celów niż weryfikacja autentyczności paszportu i tożsamości jego posiadacza
- W sprawie Burgemeester zwrócono się do TSUE z pytaniem, czy art. 7 i 8 KPP UE wraz z rozporządzeniem nr 2252/2004 nakładają na państwa członkowskie obowiązek zagwarantowania, że dane biometryczne gromadzone i przechowywane zgodnie z tym rozporządzeniem nie będą zbierane, przetwarzane i wykorzystywane do celów innych niż wydawanie paszportów?
- 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

ORZECZNICTWO TRYBUNAŁU SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ (TSUE)

- Prawa podstawowe gwarantowane przez KPP UE mają zastosowanie tylko tam, gdzie prawodawstwo krajowe nie spełnia wymogów w zakresie prawa Unii Trybunał nie mógł ustalić, czy przechowywanie i wykorzystywanie danych biometrycznych do celów innych niż wydawanie paszportów są zgodne z art. 7 i 8 KPP UE. Do sądów krajowych należałoby dokonanie oceny, czy środki krajowe odnoszące się do używania i przechowywanie danych biometrycznych są zgodne
- 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 podkreślił, że przepisy krajowe ograniczają dostęp do danych biometrycznych i korzystanie z nich w centralnym zbiorze danych, który jest ograniczony do urzędników organów krajowych odpowiedzialnych za wdrożenie ustawodawstwa krajowego dotyczącego cudzoziemców w celu ustalenia lub weryfikacji tożsamość obywateli państw trzecich
- 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 nadzoruje osoby 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 niezmiennie. Ataki mające na celu uzyskanie nieautoryzowanego dostępu do szablonów biometrycznych mogą być skierowane przeciwko biometrii bazy danych systemu lub przy przekazywaniu wzorców biometrycznych

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- 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
- Ze względu na swoją wyjątkowość szablony biometryczne pozwalają wydajnie identyfikować i śledzić bez ograniczeń czasowych i 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. Do na przykład biometryczny szablon odcisku palca może być użyty do stworzenia sztucznych palców z tym samym cechy daktyloskopijne

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
- Mogą się pojawić problemy etycznych, które są zazwyczaj 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 wyzwać 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

- Kwestią często podnoszona w dyskusjach etycznych dotyczących stosowania identyfikacji biometrycznej jest brak dokładności oprogramowania do identyfikacji czarnoskórych twarzy
- 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
- Polityki decyzyjne i prawo jednostki do zakwestionowania identyfikacji mają ogromne znaczenie dla ochrony osób przed naruszeniami ich praw podstawowych
- Wszelkie niedociągnięcia w tym zakresie mogą prowadzić do poważnej niesprawiedliwości, a nawet do masowej dyskryminacji, w tym z powodów rasowych lub etnicznych, oraz do podważania praw proceduralnych, w tym dostępu do wymiaru sprawiedliwości i prawa do rzetelnego procesu sądowego

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
- 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
- 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

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 e-mail
- 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
- Aby zapobiec naruszeniom danych i niezamierzonemu udostępnianiu szablonów, należy zapewnić silne zabezpieczenia: konieczne jest zagwarantowanie technicznej solidności każdego systemu identyfikacji biometrycznej w dowolnym momencie
- Zmniejszenie zagrożenia dla praw podstawowych, jakie stwarza przechowywanie i tworzenie szablonów biometrycznych, można ograniczyć poprzez powiązania między szablonem a innymi danymi osobowymi do niezbędnego minimum, a dodatkowe techniki deidentyfikacji mogą zapobiec identyfikacji po naruszeniu danych
- Jeśli szablony można tworzyć na podstawie różnych punktów odniesienia niektórych identyfikatorów biometryczny, osoby, których to dotyczy, powinny mieć możliwość złożenia wniosku o utworzenie nowego szablonu

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 jednostki, w czasie rzeczywistym, w przestrzeni publicznej, bez jakiejkolwiek współpracy ze strony jednostek zidentyfikowane
- Ataki terrorystyczne drastycznie zwiększyły rozmieszczenie telewizji przemysłowej w miejscach publicznych w połączeniu z identyfikacją biometryczną

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- Centralną kwestią masowej inwigilacji jest to, że ingeruje ona w autonomię i samostanowienie jednostki, ponieważ nieustannie muszą się obawiać, że ich zachowanie jest oceniane i analizowane. Monitorowanie społeczeństwo jest pierwszym krokiem do kontrolowania społeczeństwa
- Po pierwsze, 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
- Skutki, jakie całkowity nadzór może mieć na zachowanie całej populacji stają się szczególnie widoczne, gdy patrzy się na chiński system oceny kredytowej, karze się obywateli za nieprzestrzeganie norm społecznych

ETYCZNE ASPEKTY ZWIĄZANE Z IDENTYFIKACJĄ BIOMETRYCZNĄ

- Nie można zaprzeczyć, że identyfikacja biometryczna otwiera ogromne możliwości wielkoskalowego nadzoru, co zwiększa zagrożenia dla praw podstawowych, należy zauważyć, że podobne skutki może również wynikać z inwigilacji za pomocą innych środków
- 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

**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, pozwalając 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

- Troski etyczne jednak 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 może już dotyczyć konstrukcji kategorii. Ten wykorzystanie zautomatyzowanego podejmowania decyzji dodaje kolejną warstwę problemów etycznych
- 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”)
- Również mniej drastyczne i częściej używane kategorie mogą być kontrowersyjne z etycznego punktu widzenia, np. kategoria „rasa” jest wyraźnie zakorzeniona w myśleniu i musi być postrzegane w świetle historycznej i współczesnej dyskryminacji rasowej

ETYCZNE ASPEKTY ZWIĄZANE Z KATEGORYZACJĄ BIOMETRYCZNĄ

- 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
- Ryzyko błędnej kategoryzacji przez systemy algorytmiczne jest znacznie bardziej niebezpieczne niż błędna kategoryzacja przez ludzi z uwagi na skalowalność
- W przypadku, 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, w związku z tym osoby są narażone na ryzyko dyskryminacji i błędnej klasyfikacji
- 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
- Fakt, że jednostka ma niewielką kontrolę nad swoim sygnałami fizycznym, fizjologicznymi lub behawioralnymi, z których wiele będzie podświadomych, mogą posłużyć do wykryć warunków o szczególnym wymiarze etycznym
- 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

ETYCZNE ASPEKTY ZWIĄZANE Z WYKRYWANIEM BIOMETRYCZNYM

- Wykrywanie biometryczne będzie połączone z pewnego rodzaju automatyczną kategoryzacją opartą na wnioskach i predyktach, takich jak „potencjalny agresor” lub „potencjalne zagrożenie”
- 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
- Rozróżnienie między biometrią behawioralną a innymi zachowaniami nie są jednoznaczne i często będą łączone, aby zapewnić jeszcze bardziej kompleksową analizę intencji jednostki
- 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

ETYCZNE ASPEKTY ZWIĄZANE Z WYKRYWANIEM BIOMETRYCZNYM

- Techniki wykrywania 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 mrozący 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

DZIĘKUJĘ ZA UWAGĘ!

Marta Kozioł

koziolm21@gmail.com

Wrocław, 13.01.2022 r.

