Rozdział 3. Dane osobowe w wybranych ustawach o ochronie danych osobowych

§ 1. Definicja danych osobowych w RODO i w wybranych ustawach o ochronie danych osobowych

Wspólnym rdzeniem w definicji danych osobowych w RODO (art. 1 RODO, definicja z art. 4 pkt 1 RODO oraz motyw 14 RODO) i we wszystkich analizowanych tu ustawach o ochronie danych osobowych, opartych na europejskim modelu[1], są trzy kryteria:

1) to, że są to „wszelkie informacje";
2) dane osobowe dotyczą wyłącznie osób fizycznych (ustawy obejmujące ochroną również dane osób prawnych są nielicznymi wyjątkami); oraz
3) to, że identyfikują lub umożliwiają w określonym kontekście identyfikację osoby, której dane dotyczą.

Analogiczną konstrukcję definicji danych osobowych („wszystkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej") przyjęto też m.in. w: art. 4 PIPL (个人信息)[2], art. 5 LGPD[3], art. 3 ust. 1 lit. d KVKK, art. 3 pkt 1 rosyjskiej ustawy federalnej Nr 152-FZ z 27.7.2006 r. o danych osobowych, sekcji 96 DPA 2012[4].

---

[1] Tj. opartych na RODO albo dyrektywie 95/46/WE, ponieważ podobieństwa ustaw w państwach pozaeuropejskich do modelu europejskiego niekoniecznie należy postrzegać w kontekście RODO. W wielu przypadkach te analogie dotyczą wcześniejszej dyrektywy, choćby ze względu na datę uchwalenia ustawy, która następnie nie była gruntownie nowelizowana.

[2] Merytorycznie zbieżne definicje zawierają także CSL i Kodeks cywilny Chińskiej Republiki Ludowej, zgodnie z którymi dane osobowe to informacje, które mogą zidentyfikować osobę fizyczną bezpośrednio lub w połączeniu z innymi informacjami.

[3] Brazylijska ogólna ustawa o ochronie danych osobowych z 14.8.2018 r., Lei Geral de Proteção de Dados Pessoais, Nr 13.709, https://lgpd-brazil.info/ (dostęp: 5.3.2025 r.).

[4] Ghańska ustawa o ochronie danych osobowych z 10.5.2012 r., Data Protection Act of 2012, Act 843, https://nita.gov.gh/wp-content/uploads/2017/12/Data-Protection-Act-2012-Act-843.pdf (dostęp: 5.3.2025 r.).

Również w kalifornijskiej CCPA [sekcja § 1798.140(v)(1)] dane osobowe to informacje, które identyfikują (w przepisie także: odnoszą się, opisują) oraz które można w uzasadniony sposób powiązać bezpośrednio lub pośrednio z konkretnym konsumentem (a więc odpowiada to informacjom o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej z art. 4 pkt 1 RODO). Istotną różnicą w stosunku do tego modelu dominującego w wielu regionach świata jest, po pierwsze, ograniczenie podmiotowe – konsument jest mieszkańcem Kalifornii, a po drugie – komponent „gospodarstwa domowego" w kalifornijskiej w definicji danych osobowych (dane osobowe to informacje, które identyfikują lub które można powiązać z konsumentem lub gospodarstwem domowym). Ponieważ nawet osoba fizyczna mieszkająca samotnie może stanowić gospodarstwo domowe, definicja[5] nie wskazuje kryterium odróżniającego osobę w gospodarstwie domowym od konsumenta w definicji danych osobowych[6]. Osoby tworzące gospodarstwo domowe są jednocześnie konsumentami w rozumieniu CCPA, więc „gospodarstwo domowe" w CCPA powiela znaczenie „konsumenta" w definicji danych osobowych. Nowelizacja wprowadzona przez CPRA, która wprowadziła definicję z sekcji § 1798.140(q) CCPA, nie daje powodu do zmiany tej krytycznej opinii, ponieważ podtrzymuje definicję gospodarstwa domowego (*household*) jako zidentyfikowanej grupy konsumentów mieszkającej pod tym samym adresem i wspólnie użytkującej wspólne urządzenia lub usługi[7]. Natomiast ustawa wyłącza w sekcji § 1798.140(p) CCPA prawa do usunięcia, korekty i dostępu do danych wobec danych gospodarstw domowych, co ma niwelować skutki tego elementu definicji danych osobowych, który ją zaburza.

Jednak w definicji „unikalnego identyfikatora" (*unique identifier or unique personal identifier*), którym jest m.in. plik cookie (ponadto adres IP, beacons, pixele), ustawa nie posługuje się już pojęciem gospodarstwa domowego (*household*), lecz rodziny (*family*) – odnosi się do identyfikatora umożliwiającego rozpoznanie konsumenta, rodziny lub urządzenia, które jest powiązane z konsumentem lub rodziną, w różnych usługach [sekcja § 1798.140(aj) CCPA].

Inną widoczną różnicą między RODO i CCPA jest to, że definicja danych osobowych w CCPA [sekcja § 1798.140(v)(2) CCPA] nie obejmuje informacji publicznie dostępnych ani uzyskanych zgodnie z prawem prawdziwych in-

[5] Sekcja § 999.301(k) CCPA: *'Household' means a person or group of people who*: *(1) reside at the same address*, *(2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier*.

[6] *M. Krzysztofek*, The Interpretation of 'Household' in the Definition of Personal Information in the CCPA, s. 38–43, https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/2.1/GPLR2021005 (dostęp: 7.2.2025 r.).

[7] Sekcja § 1798.140(q) CCPA: (…) *a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common devices or services*.

formacji, które stanowią przedmiot zainteresowania opinii publicznej (*publicly available information or lawfully obtained, truthful information that is a matter of public concern*)[8]. Przepis definiuje „publicznie dostępne" informacje jako udostępnione zgodnie z prawem z rejestrów władz federalnych, stanowych lub lokalnych, lub informacje, co do których administrator ma uzasadnione podstawy sądzić, że zostały zgodnie z prawem udostępnione ogółowi społeczeństwa przez konsumenta lub media o szerokim zasięgu, lub informacje udostępnione przez osobę, której konsument je ujawnił, jeżeli konsument nie ograniczył ich do określonego grona odbiorców. „Publicznie dostępne" nie oznaczają informacji biometrycznych zebranych przez administratora nt. konsumenta bez wiedzy konsumenta. To wyłączenie z zakresu danych osobowych w CCPA zbliża w tym przypadku tę ustawę do podstawy przetwarzania danych z art. 13 ust. 6 PIPL (gdy dane osobowe zostały ujawnione przez podmiot danych lub ujawnione zgodnie z prawem), jednak odróżnia od RODO, bo RODO nie pomija danych w zależności od ich źródła (do danych wrażliwych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą – art. 9 ust. 2 lit. e RODO – odniosłem się w rozdziałach 3 i 6 tej monografii).

Uwagę zwraca, że CCPA posługuje się określeniami „informacje osobowe" (w definicji danych osobowych – tłumaczę je jako dane osobowe, aby zachować spójność z RODO) oraz „dane". „Dane" są interpretowane jako „surowe", nieprzetworzone[9]. To np. dane lokalizacyjne (*geolocation data*). Chociaż wydaje się, że słabością tej interpretacji są np. informacje biometryczne (*biometric information*), które spełniają przecież ten sam warunek, nie są przetworzone. Z pewnością w CCPA „informacje" i „dane" (*information*, *data*) nie są synonimami. W definicji danych osobowych w CCPA *'personal information' means information* (...)" te określenia nie są stosowane alternatywnie, natomiast w definicji danych osobowych w RODO przeciwnie – „«dane osobowe» oznaczają informacje (...)".

Unijne RODO ogranicza zakres danych osobowych do informacji dotyczących osób fizycznych (art. 1 RODO, definicja z art. 4 pkt 1 RODO), definicje danych osobowych w PIPL i CCPA – również.

---

[8] Tak również – teza o braku gwarancji dla prawa do prywatności w prawie USA w przypadku danych, które znajdują się w sferze publicznej (gdy w UE obowiązuje odwrotna zasada, konieczność wykazania podstawy przetwarzania również dla danych znajdujących się w sferze publicznej): *D. Kuźnicka-Błaszkowska*, Uznanie adekwatności modelu ochrony danych osobowych, s. 367; *B.C. Newell*, *S. de Conca*, *K. Thomasen*, Survailance and Privacy in North America public spaces, s. 226; *Katz v. United States*, 389 U.S. 347 (1967), https://supreme.justia.com/cases/federal/us/389/347/ (dostęp: 7.2.2025 r.).

[9] *B.M. Wheeler*, California Privacy Law Update, https://www.aalrr.com/Business-Law-Journal/california-privacy-law-update-the-ccpa-and-cpra-amended (dostęp: 7.2.2025 r.).

Na przykładzie RODO zakres nie obejmuje osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej (motyw 14 RODO), choć RODO nie wyłącza ochrony wobec osób fizycznych prowadzących działalność gospodarczą.

Przykładami ustaw, których definicje danych osobowych obejmują również osoby prawne, są południowoafrykańska POPIA (sekcja 1), definiująca dane osobowe jako informacje dotyczące możliwej do zidentyfikowania żyjącej osoby fizycznej oraz w niektórych przypadkach (*where applicable*) możliwej do zidentyfikowania istniejącej osoby prawnej, oraz PDPL[10] (rozdział I, sekcja 2), w której dane osobowe zostały zdefiniowane jako wszelkiego rodzaju informacje dotyczące osób fizycznych lub prawnych, zidentyfikowanych lub możliwych do zidentyfikowania.

§ 2. Katalog danych osobowych

Definicja danych osobowych w RODO (art. 4 pkt 1 RODO) wskazuje otwarty katalog informacji umożliwiających identyfikację osoby fizycznej, której dotyczą, do których należą w szczególności imię i nazwisko, numer identyfikacyjny, lokalizacja, identyfikator internetowy, lub czynniki określające fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Odzwierciedla to m.in. wyr. TS z 29.1.2008 r. [*Productores de Música de España (Promusicae) v. Telefónica de España SAU*][11], który wskazuje dane bezpośrednio i pośrednio identyfikujące, jak imię i nazwisko, numer identyfikacyjny, datę urodzin, adres zamieszkania, w powiązaniu z informacjami o charakterze biometrycznym lub innymi cechami, jak płeć, kolor oczu, waga, wzrost oraz w powiązaniu z poglądami.

To również dane kontaktowe, do których należy numer telefonu (w powiązaniu z innymi danymi)[12], a także np. numer rejestracyjny samochodu[13] – tu najczęściej właściciela pojazdu, bo identyfikacja innych osób korzystających

[10] Argentyńska ustawa o ochronie danych osobowych z 4.10.2000 r., Nr 25.326, Personal Data Protection Law, https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm (dostęp: 5.3.2025 r.).

[11] Wyr. TS z 29.1.2008 r., *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, C-275/06, EU:C:2008:54.

[12] Wyr. WSA w Warszawie: z 25.11.2022 r., II SA/Wa 710/22, Legalis; wyr. WSA w Warszawie z 13.4.2021 r., II SA/Wa 1898/20, Legalis.

[13] Wytyczne 01/2020, https://www.edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_pl.pdf (dostęp: 5.3.2025 r.).

z pojazdu będzie utrudniona [TSUE[14] odniósł się ponadto do numeru VIN (Vehicle Identification Number)].

Analogiczny przykładowy katalog kategorii danych osobowych zawiera CCPA (otwarty i wyjątkowo obszerny). Definicja danych osobowych [sekcja § 1798.140(v)(1) CCPA] obejmuje w niej w szczególności imię i nazwisko, alias, dane kontaktowe, numer ubezpieczenia społecznego, numer prawa jazdy, numer paszportu, dane biometryczne, dane genetyczne, dane o lokalizacji, numery kont, informacje o zatrudnieniu, informacje o wykształceniu, historię zakupów, identyfikatory online i urządzeń oraz historię wyszukiwania i przeglądania oraz inne działania online, jeśli takie informacje są powiązane lub możliwe do utworzenia powiązania z określonym konsumentem (który jest definiowany jako mieszkaniec Kalifornii) lub gospodarstwem domowym. Innym przykładem ustawy, która zawiera przykładowy katalog kategorii danych osobowych, jest południowoafrykańska POPIA (sekcja 1), wymieniająca m.in. informacje dotyczące rasy, płci, ciąży, stanu cywilnego, pochodzenia narodowego, etnicznego lub społecznego, orientacji seksualnej, wieku, zdrowia, religii, przekonań, wykształcenia, historii kredytowej, karalności, przebiegu zatrudnienia, numer identyfikacyjny, adres e-mail, adres fizyczny, numer telefonu, informacje o lokalizacji, identyfikator internetowy lub inne, dane biometryczne, osobiste opinie osoby lub nt. osoby, prywatną korespondencję wysłaną przez osobę lub dalszą korespondencję, która ujawniłaby treść oryginalnej korespondencji, nazwisko osoby.

Przykładem przeciwnym definicji danych osobowych, która nie zawiera katalogu osobowych, a określa je tylko jako „wszelkiego rodzaju informacje dotyczące zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych", jest art. 4 PIPL (aby być ścisłym, należy powiedzieć, że nie zawiera go główna definicja danych osobowych, ponieważ otwarty katalog danych wrażliwych, również będących przecież danymi osobowymi, znajduje się w art. 28 PIPL) (przykłady danych osobowych różnych kategorii, m.in. dane identyfikacyjne, kontaktowe, lokalizacyjne, zawiera jednak nieobligatoryjna, zalecana norma krajowa[15], a także art. 76 ust. 5 CSL, gdzie znajduje się niewyczerpujący katalog danych osobowych, który obejmuje w szczególności imię i nazwisko, datę

[14] Wyr. TS z 9.11.2023 r., *Gesamtverband Autoteile-Handel e.V. v. Scania CV AB*, C-319/22, EU:C:2023:837.

[15] Pkt 3.1, s. 1 i Załącznik A, GB/T 35273–2020 [National Standard of the People's Republic of China, Information security technology – Personal information (PI) security specification z 6.3.2020 r., (信息安全技术 个人信息安全规范), State Administration for Market Supervision of the People's Republic of China Standardization Administration of the People's Republic of China, https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf (dostęp: 7.2.2025 r.)].

urodzenia, numer dokumentu tożsamości, dane biometryczne, adres, numer telefonu).

Podobna uproszczona konstrukcja została zastosowana w ustawach brazylijskiej (LGPD), argentyńskiej (PDPL) i rosyjskiej (ustawy federalnej Nr 152-FZ z 27.7.2006 r. o danych osobowych). Uważam jednak, że brak otwartego katalogu lub ograniczony katalog danych osobowych (w porównaniu do innej ustawy) nie wpływa na możliwość uznania informacji za dane osobowe, skoro we wszystkich analizowanych ustawach wspólnymi kryteriami są kwestie, że dane osobowe to „wszelkie informacje" oraz że identyfikują lub umożliwiają w określonym kontekście identyfikację osoby, której dane dotyczą.

Tak więc niezależnie od tego, czy przepis wymienia np. identyfikatory internetowe (jak w motywie 30 RODO[16]: adresy IP, identyfikatory plików cookie – generowane przez urządzenia, aplikacje, narzędzia i protokoły czy też inne identyfikatory, generowane np. przez etykiety RFID, lub inne, takie jak pseudonimy używane na forach internetowych przez użytkowników; podobny katalog znajduje się również w definicji danych osobowych w kalifornijskiej CCPA: *online identifier*, *Internet Protocol address*, *e-mail address*, *account name*) czy nie zawiera takiego wyliczenia (jak w chińskiej PIPL lub w ww. ustawie rosyjskiej), stanowią dane osobowe, jeżeli umożliwiają identyfikację osoby fizycznej. Danymi osobowymi są także nagrania obrazu lub głosu, w tym uzyskane przez monitoring (wyr. TS z 11.12.2014 r., *František Ryneš v. Úřad pro ochranu osobních údajů*)[17].

W definicji danych osobowych, niezależnie od obszerności katalogu informacji stanowiących dane osobowe, wymienienie wszystkich nie jest możliwe, katalog zawsze ma charakter otwarty i przykładowy, a zmieniające się okoliczności, jak nowe technologie przetwarzania, mogą powodować powstawanie nowych (i tak było w ostatnich latach) kategorii danych osobowych[18].

Jeżeli więc informacja umożliwia identyfikację osoby fizycznej (np. adres e-mail, numer identyfikacyjny w elektronicznym systemie ewidencji ludności, numer dokumentu tożsamości, imiona i nazwiska rodziców, imię i nazwisko żony/męża, numer rejestracyjny pojazdu, numer rachunku bankowego, numer karty kredytowej, identyfikator internetowy, lokalizacja, dane biometryczne, historia kredytowa itd.), to jest daną osobową na podstawie definicji z każdej z analizowanych tu ustaw, niezależnie od tego, czy zawiera ona przykładowy ka-

[16] Wyr. TS z 24.11.2011 r., *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, EU:C:2011:771, uznaje adres IP za dane osobowe w przypadku dostawcy usługi dostępu do Internetu.

[17] Wyr. TS z 11.12.2014 r., *František Ryneš v. Úřad pro ochranu osobních údajů*, C-212/13, EU:C:2014:2428.

[18] *P. Fajgielski*, Ogólne rozporządzenie o ochronie danych, s. 106.

talog danych osobowych. Z drugiej strony, żadna kategoria informacji odnoszących się bezpośrednio lub pośrednio do osoby fizycznej nie stanowi „danej osobowej" z samej swojej natury, ponieważ poza kontekstem, bez dodatkowych informacji dotyczących danej osoby, może nie powstać możliwość powiązania jej z tą osobą (ani uzasadnione prawdopodobieństwo, że informacja zostanie wykorzystana przez administratora w celu identyfikacji ze względu na koszt czy technologię, którą dysponuje). Analizowane pozaeuropejskie ustawy są więc m.zd. zbieżne w tym aspekcie z RODO.

Nieprawdziwe informacje i opinie o osobie, np. subiektywne, czy wręcz zniesławiające, również są danymi osobowymi, jeżeli można je przypisać konkretnej osobie fizycznej[19]. Dotyczy to także samych danych osobowych, np. informacje dotyczące zadłużenia osoby, które zostały opublikowane w rejestrze kredytowym i nie zostały zaktualizowane po spłacie zadłużenia, a tym samym błędnie wskazują, że dana osoba jest nadal dłużnikiem, są danymi osobowymi, które należy sprostować.

W południowoafrykańskiej POPIA (sekcja 1) wprost sprecyzowano, że opinie o osobie należą do danych osobowych (*the views or opinions of another individual about the person*), należy więc założyć, że również nieprawdziwe, skoro ocena ich prawdziwości może zależeć np. od odmiennych perspektyw osoby, która je formułuje i podmiotu danych oraz nowych informacji nieznanych wcześniej. Ustawa australijska, tj. Privacy Act 1988[20] (obecnie trwają prace nad jej nowelizacją[21]), jeszcze wyraźniej podkreśla, że do danych osobowych należy m.in. opinia lub informacja, bez względu na ich prawdziwość (*whether the information or opinion is true or not*).

§ 3. Dane wrażliwe

Zamkniętym (w art. 9 ust. 1 RODO, choć nie w każdym analogicznym przepisie innych ustaw jest to zbiór zamknięty) podzbiorem danych osobowych są „szczególne kategorie danych osobowych" – dane wrażliwe.

Ta kategoria danych została wyodrębniona i objęta wzmocnioną ochroną w porównaniu ze zwykłymi danymi osobowymi (a więc innymi niż ujęte w ka-

[19] Tak również *D. Lubasz*, w: *tenże* (red.), Ochrona danych osobowych, s. 78.

[20] Australijska ustawa o ochronie prywatności z 21.12.1988 r. ze zm., Privacy Act 1988, https://www.legislation.gov.au/C2004A03712/latest/text (dostęp: 5.3.2025 r.).

[21] 12.9.2024 r. Prokurator Generalny przedstawił Parlamentowi projekt ustawy (pierwszą część tej reformy, poprzedzającą konsultacje dotyczące drugiej części) reformującej ustawę o ochronie prywatności [Privacy Act; Law reform in the age of AI, https://ministers.ag.gov.au/media-centre/speeches/law-reform-age-ai-17-10-2024 (dostęp: 7.2.2025 r.)].

talogu danych wrażliwych) ze względu na ich szczególne znaczenie dla ochrony prawa do prywatności oraz zagrożenia dla podstawowych praw i wolności.

Dane wrażliwe należą do sfery nie tylko prywatnej, ale intymnej. Ich ujawnienie może narazić osobę, której dane dotyczą, na istotną i nieodwracalną szkodę poprzez naruszenie jej godności, napiętnowanie jej lub narażenie jej na ostracyzm w jej środowisku. Może również prowadzić do dyskryminacji podmiotu danych, wywoływać negatywne skutki prawne lub mieć inny istotny wpływ, np. na decyzje dotyczące zatrudnienia, kredytowania czy ubezpieczenia na życie.

Tę naturę danych wrażliwych wskazuje chińska PIPL w art. 28 (w ten sposób jako jedyna spośród analizowanych tu ustaw), określając je jako dane, które ujawnione lub bezprawnie wykorzystane, mogą łatwo naruszyć godność osób fizycznych lub poważnie zaszkodzić bezpieczeństwu osobistemu lub majątkowemu[22], co uzasadnia pośrednio potrzebę wyodrębnienia ich jako podkategorii danych osobowych.

Przewodnik dotyczący wrażliwych danych osobowych (Guide for Sensitive Personal Information Identification) wydany przez Krajowy Komitet Techniczny ds. Standaryzacji Bezpieczeństwa Informacji (TC260, National Information Security Standardization Technical Committee) we wrześniu 2024 r., mocno akcentuje to kryterium. Wprowadza test „ryzyka szkody" i jego prymat nad listą kategorii danych wrażliwych z art. 28 PIPL – wytyczne mówią, że informacja może nie mieć wrażliwego charakteru, jeżeli nie wyrządza szkód wskazanych w art. 28 PIPL, a więc nie spełnia kumulatywnie warunków z tego przepisu. To duża różnica w stosunku do RODO, skoro jego przepisy nie stopniują poziomu ochrony danych wrażliwych w zależności od ich wpływu na prywatność podmiotu danych, np. informacje dotyczące zdrowia są wrażliwe niezależnie od ich kontekstu, wpływu na podmiot danych, ewentualnego odbioru przez osoby trzecie (por. pkt 51 wyr. TS z 6.11.2003 r.[23]).

Zamknięty katalog danych wrażliwych w art. 9 ust. 1 RODO obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, a także dane genetyczne, dane biometryczne jednoznacznie identyfikujące osobę fizyczną oraz dane dotyczące zdrowia, seksualności lub orientacji seksualnej (art. 9 ust. 1 RODO).

Przepis określa dane wrażliwe jako „ujawniające" niektóre cechy wymienione w art. 9 ust. 1 RODO, jednak w przypadku innych cech – jako „dane dotyczą-

[22] Art. 28 PIPL: (…) *once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security*.

[23] Wyr. TS z 6.11.2003 r., *Bodil Lindqvist*, C-101/01, EU:C:2003:596.

ce" ich, np. ujawniające pochodzenie rasowe, ale dotyczące zdrowia. Zgadzam się z opinią, że „dane ujawniające" to kategoria szersza, bo obejmuje też informacje, z których można wnioskować o istnieniu tych cech, a nie tylko informacje wprost dotyczące tych cech, np. z treści recept wystawianych systematycznie przez lekarza na nazwisko pacjenta można wnioskować o określonej chorobie[24], z wpłat na określony kościół o przekonaniach religijnych. Jednak to, że w przypadku zdrowia, seksualności i orientacji seksualnej danymi wrażliwymi są „dane dotyczące", a nie „ujawniające", wprowadza niekonsekwencję. To zróżnicowanie mogłoby uzasadniać wątpliwość czy zakres danych wrażliwych odnoszących się do zdrowia, seksualności lub orientacji seksualnej nie jest węższy niż pozostałych kategorii z art. 9 ust. 1 RODO. Jednak z wyr. TS z 1.8.2022 r.[25] wynika, że nie. Trybunał Sprawiedliwości Unii Europejskiej dokonał szerokiej interpretacji zakresu danych wrażliwych w rozumieniu art. 9 RODO, uznając, że są nimi również dane partnera (w tym przypadku w postępowaniu na podstawie litewskiego prawa antykorupcyjnego), skoro można z nich pośrednio wywnioskować orientację seksualną podmiotu danych. Szeroka wykładnia zakresu danych wrażliwych, która zmierza do zapewnienia wysokiego poziomu ochrony tej kategorii danych, wynika też z pkt 50 ww. wyr. TS z 6.11.2003 r.

Warto podkreślić, że nie tylko art. 9 ust. 1 RODO, ale też np. kalifornijska CCPA [w sekcji § 1798.140(ae)(1) CCPA] – *personal information that reveals* – i argentyńska PDPL (w sekcji 2 PDPL) odnoszą się do danych „ujawniających" poszczególne kategorie danych wrażliwych, a więc nie tylko informacji wprost wrażliwych, ale też prowadzących pośrednio do ich ustalenia. Przykładem może być geolokalizacja, która jest bezpośrednio informacją wrażliwą w kalifornijskiej CCPA i chińskiej PIPL, lecz nie w RODO, ale która np. w historii nawigacji samochodowej może umożliwić ustalenie adresów, które mogą wskazywać np. na regularne wizyty lekarskie właściciela samochodu w gabinecie o określonym profilu. Natomiast art. 6 ust. 1 KVKK wprost zalicza do danych wrażliwych również ubiór, ponieważ może on ujawniać wyznanie.

Zgodnie z art. 26 PIPL systemy rozpoznawania twarzy w miejscach publicznych mogą służyć wyłącznie do celów ochrony bezpieczeństwa publicznego, chyba że zostanie uzyskana odrębna zgoda podmiotu danych[26]. Kilka chińskich

[24] *P. Fajgielski*, Ogólne rozporządzenie o ochronie danych, s. 198.

[25] Wyr. TS z 1.8.2022 r., *OT v. Vyriausioji tarnybinės etikos komisja*, C-184/20, EU:C:2022:601.

[26] Tak również Najwyższy Sąd Ludowy Chin w wytycznych dla sądów z 28.7.2021 r. dotyczących stosowania przepisów o technologii rozpoznawania twarzy znajdujących się w chińskim Kodeksie cywilnym, CSL, chińskiej ustawie o ochronie praw konsumentów, chińskiej ustawie o handlu elektronicznym; *M. Torres*, China's Supreme People's Court sets rules, https://www.garrigues.com/en_GB/new/chinas-supreme-peoples-court-sets-rules-facial-recognition-technology (dostęp: 7.2.2025 r.).

miast, np. Tianjin, Nanjing i Xuzhou, ograniczyło lub zakazało stosowania technologii rozpoznawania twarzy[27].

Dostawca oprogramowania AI do rozpoznawania twarzy, Clearview AI, został ukarany przez kilka unijnych organów ochrony danych, między innymi m.in. włoski, francuski i grecki, za trenowanie swoich algorytmów rozpoznawania twarzy zdjęciami pozyskiwanymi przez technikę „web scrappingu", czyli przeczesywaniea Internetu, w szczególności mediów społecznościowych, jak Facebook, Youtube czy Instagram w poszukiwaniu tych danych. Są w tej sytuacji danymi biometrycznymi z art. 4 pkt 14 RODO, więc podstawą przetwarzania danych nie mógł być uzasadniony interes, a organy ochrony danych wykazały, że administrator danych nie miał innej.

Pozyskiwanie zdjęć użytkowników bez podstawy prawnej (poza innym naruszeniami) było także powodem nałożenia 21.7.2022 r. poważnej administracyjnej kary pieniężnej w wysokości 8,026 mld RMB (około 1,2 mld USD) przez chińską CAC na firmę Didi Chuxing[28].

Model zamkniętego katalogu danych wrażliwych powielają również definicje danych wrażliwych w innych analizowanych w tym rozdziale ustawach, np. w argentyńskiej PDPL (sekcja 2 PDPL), DPA 2012 (art. 37 ust. 1 DPA 2012), kalifornijskiej CCPA [sekcja § 1798.140(ae) CCPA], przy czym należy zaznaczyć, że CCPA pierwotnie nie definiowała danych wrażliwych, w południowoafrykańskiej POPIA (sekcja 26 POPIA), w tureckiej KVKK (art. 6 KVKK).

Co więcej, kategorie danych wrażliwych w tych ustawach są w znacznym stopniu zbieżne z art. 9 ust. 1 RODO, np. definicje w ustawach: brazylijskiej LGPD, australijskiej Privacy Act 1988, tureckiej KVKK, południowoafrykańskiej POPIA, kalifornijskiej CCPA, ghańskiej ustawie o ochronie danych osobowych z 10.5.2012 r. i argentyńskiej PDPL obejmują m.in. dane dotyczące zdrowia, wyznania i życia seksualnego.

Na tym tle odróżnia się chińska PIPL (art. 28 PIPL), w której katalog danych wrażliwych jest otwarty i wprawdzie zawiera kategorie, takie jak dane dotyczące zdrowia i wyznanie, to zbieżność listy danych wrażliwych z RODO może wynikać ewentualnie z wykładni art. 28 PIPL, oceny czy ujawnienie poszczególnych danych narusza godność osób fizycznych lub poważnie zagraża ich bezpieczeństwu osobistemu lub majątkowemu, bo sama lista tych danych w przepisie nie jest zbieżna z RODO. Listę chińskich danych wrażliwych wskazuje też krajo-

[27] *Y. Chen*, Tianjin Bans the Collection of Facial Recognition Data, https://www.chinajusticeobserver.com/a/tianjin-bans-the-collection-of-facial-recognition-data (dostęp: 7.2.2025 r.).

[28] *G. Webster*, Chinese Authorities Announce $1.2B Fine in DiDi Case, https://digichina.stanford.edu/work/translation-chinese-authorities-announce-2b-fine-in-didi-case-describe-despicable-data-abuses/ (tekst w języku angielskim) (dostęp: 7.2.2025 r.), http://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (tekst w języku chińskim) (dostęp: 7.2.2025 r.).

wy standard[29] (National Standard, 国标, GB/T 35273–2020, nieobligatoryjny, zalecana norma krajowa), w tym niebędących takimi w RODO, jak informacje o koncie bankowym, informacje o nieruchomościach, informacje kredytowe, informacje o miejscu pobytu oraz dane osobowe dzieci do 14 lat.

Przepisy te nie stopniują poziomu ochrony danych w zależności od ich wpływu na prywatność podmiotu danych, np. dotyczących zdrowia – informacje o bezpłodności lub nosicielstwie niektórych wirusów są szczególnie intymne, natomiast informacja o krótkiej kontuzji sportowej zapewne neutralna w odbiorze otoczenia. Jednak w pkt 51 wskazanego powyżej wyr. TS z 6.11.2003 r. Trybunał stwierdził, że „informacja, iż dana osoba doznała urazu stopy i przebywa na zwolnieniu lekarskim w niepełnym wymiarze, stanowi dane osobowe dotyczące zdrowia w rozumieniu art. 8 ust. 1 dyrektywy 95/46". Informacje o uzależnieniach dotyczą zdrowia[30], a więc są danymi wrażliwymi[31], dodatkowym uzasadnieniem tego charakteru tych danych jest też ryzyko negatywnych skutków prawnych lub innego istotnego wpływu na osobę, której dotyczą.

Z tymi ustawami kontrastuje prawo Kazachstanu, które nie zawiera definicji wrażliwych danych osobowych, a jedynie ogranicza dostęp do niektórych informacji będących przedmiotem tajemnic zawodowych np. tajemnicy lekarskiej lub telekomunikacyjnej (dane osobowe abonentów).

Definicja danych wrażliwych z art. 9 ust. 1 RODO nie uwzględnia wszystkich kategorii, które w powszechnym odczuciu mogłyby zostać określone jako dane o dużej wrażliwości, również w krajach, które nie podlegają RODO. Przykładem są dane o sytuacji finansowej, w tym np. o stanie rachunku bankowego, które w RODO nie wchodzą w zakres danych wrażliwych (w RODO tożsamość ekonomiczna, a więc sytuacja finansowa, należy do definicji zwykłych danych osobowych), mimo że nieuprawnione ujawnienie lub dostęp do takich danych może narazić osobę, której dane dotyczą, na istotną lub nieodwracalną szkodę (w niektórych przypadkach podlegają ochronie np. jako tajemnica bankowa, jednak nie we wszystkich przypadkach dane o sytuacji majątkowej muszą

[29] Pkt 3.2, s. 2 i Załącznik B, GB/T 35273–2020 [National Standard of the People's Republic of China, Information security technology – Personal information (PI) security specification z 6.3.2020 r., (信息安全技术 个人信息安全规范), State Administration for Market Supervision of the People's Republic of China Standardization Administration of the People's Republic of China, https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf (dostęp: 7.2.2025 r.)].

[30] Uzależnienie jest definiowane jako nabyty stan zaburzenia zdrowia psychicznego i fizycznego, który charakteryzuje się okresowym lub stałym przymusem wykonywania określonej czynności lub zażywania psychoaktywnej substancji chemicznej, a diagnozowanie uzależnień odbywa się m.in. w oparciu o klasyfikacje chorób ICD-10 i DSM IV; „Uzależnienie", https://pl.wikipedia.org/wiki/Uzale%C5%BCnienie (dostęp: 7.2.2025 r.).

[31] *P. Fajgielski*, Ogólne rozporządzenie o ochronie danych, s. 133; *M. Kuba*, w: *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO, s. 279.

znajdować się na rachunkach bankowych). Dane tego rodzaju spełniają również kryterium poważnego zagrożenia dla bezpieczeństwa osobistego lub majątkowego, wyraźnie wskazane w art. 28 PIPL. Warto wspomnieć o publicznym dostępie do zeznań podatkowych wszystkich podatników w Finlandii i Norwegii, a więc możliwości sięgnięcia do informacji o dochodach sąsiadów lub znajomych w bazach danych organów podatkowych, a w Finlandii, w tzw. dniu zazdrości narodowej nawet w mediach, w przypadku 10 tys. najlepiej zarabiających w kraju Finów, np. celebrytów, gwiazd[32] (po wejściu RODO w życie, tj. od 2019 r., podatnicy osiągający przychód co najmniej 100 tys. EUR mogą zażądać zaprzestania udostępniania mediom danych o ich zarobkach[33]). Natomiast w Chinach funkcjonują tzw. ekrany wstydu – publikowanie wizerunków dłużników lub sprawców wykroczeń na monitorach na ulicach lub w transporcie publicznym oraz współpraca między sądami (sąd w Nanning w Guangxi) i TikTokiem polegająca na wyświetlaniu wizerunków osób z czarnej listy[34].

Dane finansowe (login do konta klienta, numer konta, karty debetowej lub karty kredytowej w połączeniu z dowolnym środkiem zabezpieczającym lub kodem dostępu, hasłem lub danymi uwierzytelniającymi umożliwiającymi dostęp do konta) zostały natomiast zaliczone do danych wrażliwych w kalifornijskiej CCPA [sekcja § 1798.140)(ae)(1)(B) CCPA] oraz w ustawie indyjskiej[35] (informacje finansowe, takie jak dane konta bankowego lub karty kredytowej lub debetowej lub inne dane instrumentu płatniczego). Ale CCPA w sekcji § 1798.145(d)(1) wyłącza stosowanie przepisów tej ustawy do przetwarzania danych dotyczących oceny zdolności kredytowej i analizy ryzyka kredytowego konsumenta zdefiniowanych w powoływanych już ustawach: Gramm Leach Bliley Act (GLBA) (15 U.S. Code § 6802 i n.) oraz Fair Credit Reporting Act (FCRA). Kalifornijska CCPA wyłącza ze swojego zakresu również przetwarzanie danych medycznych, które podlega ustawom Confidentiality of Medical Information Act (CMIA)[36] i powoływanej już ustawie – Health Insurance Portability and Accountability Act [sekcja § 1798.145(c)(1) CCPA].

---

[32] *A. Doyle*, *A. Scrutton*, Privacy, what privacy?, https://www.reuters.com/article/idUSKCN0X91S0/ (dostęp: 7.2.2025 r.).

[33] *M. Kucharczyk*, *P. Vänttinen*, Finlandia, https://www.euractiv.pl/section/praca-i-polityka-spoleczna/news/finlandia-jak-w-praktyce-wyglada-jawnosc-zarobkow-najbogatszych/ (dostęp: 7.2.2025 r.).

[34] *S. Ahmed*, The Messy Truth About Social Credit, https://logicmag.io/china/the-messy-truth-about-social-credit/ (dostęp: 7.2.2025 r.); *T.F. Chan*, Debtors in China are placed on a blacklist, https://www.businessinsider.com/chinas-tax-blacklist-shames-debtors-2017-12?IR=T (dostęp: 7.2.2025 r.).

[35] Indyjska ustawa o ochronie danych osobowych z 9.8.2023 r., Digital Personal Data Protection Act, https://www.meity.gov.in/content/digital-personal-data-protection-act-2023 (dostęp: 5.3.2025 r.).

[36] Amerykańska federalna ustawa dotycząca ochrony poufności informacji medycznych z 1.1.1981 r., Confidentiality of Medical Information Act (CMIA), https://consumercal.org/about-

Innym przykładem kategorii danych, które nie są zaliczone do danych wrażliwych w RODO ani analogicznych ustawach, są dane takie jak numery PESEL i ich odpowiedniki w innych państwach. W USA numerowi PESEL odpowiada numer ubezpieczenia społecznego [Social Security Number (SSN)], który należy do zakresu danych wrażliwych [sekcja § 1798.140(ae)(1)(A) CCPA].

Poza danymi finansowymi powyżej i numerem ubezpieczenia społecznego definicja danych wrażliwych z CCPA z 1798.140(ae) obejmuje też dane dotyczące prawa jazdy, stanowego dowodu osobistego lub numer paszportu, dokładną geolokalizację konsumenta, treść poczty, e-maili i wiadomości tekstowych konsumenta, z wyjątkiem skierowanych do administratora danych. Jest to więc zakres znacznie szerszy niż ten z art. 9 ust. 1 RODO.

W chińskiej PIPL dane osobowe dzieci w wieku poniżej 14 lat są danymi wrażliwymi (art. 28 PIPL) niezależnie od charakteru tych danych, a więc ich faktycznej wrażliwości albo neutralności[37].

Warto zwrócić uwagę na różnice, które mogą wynikać z kontekstu historycznego – np. pochodzenie rasowe zostało zakwalifikowane do danych wrażliwych we wszystkich analizowanych tu ustawach, a w motywie 51 RODO zaznaczono, że „użycie w niniejszym rozporządzeniu terminu «pochodzenie rasowe» nie oznacza, że Unia akceptuje teorie sugerujące istnienie osobnych ras ludzkich", to w RPA (choć apartheid został zniesiony w 1994 r.) obywatele podlegają ustawowej ewidencji wg tego kryterium (*African*, *Indian*, *colored*, *white*)[38] np. w statystykach demograficznych, przy dystrybucji funduszy publicznych czy w edukacji.

Unijne RODO nie zalicza do wrażliwych danych osobowych dotyczących wyroków skazujących i naruszeń prawa (art. 10 RODO).

§ 4. Dane genetyczne i biometryczne

Unijne RODO wprowadziło definicje danych genetycznych – jako danych osobowych dotyczących odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pocho-

-cfc/cfc-education-foundation/cfceducation-foundationyour-medical-privacy-rights/confidentiality-of-medical-information-act/?form=MG0AV3 (dostęp: 5.3.2025 r.).

[37] *L. Zhang*, *K. Kollnig*, Theory and practice, s. 37–52, https://doi.org/10.1093/idpl/ipad017 (dostęp: 7.2.2025 r.).

[38] *M. Plaut*, South Africa's Enforced Race Classification Mirrors Apartheid, https://www.fairobserver.com/region/africa/martin-plaut-south-africa-racial-groups-minorities-south-african-history-apartheid-23801/ (dostęp: 7.2.2025 r.).

dzącej od tej osoby fizycznej (art. 4 pkt 13 RODO). Danymi osobowymi są więc próbki krwi i innych tkanek. Konieczne jest jednak uwzględnienie kryterium subiektywnej identyfikowalności, zgodnie z którym identyfikacja jest możliwa w określonych okolicznościach dotyczących danego administratora, takich jak technologie i budżet, którymi dysponuje. Na przykład nie należy traktować zmieszanych włosów klientów na podłodze zakładu fryzjerskiego jako próbek biologicznych, choć mogą się nimi stać w specjalistycznych laboratoriach diagnostyki genetycznej.

Unijne RODO zawiera również definicję danych biometrycznych jako danych osobowych, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby (np. wizerunek twarzy, dane daktyloskopijne, a w przypadku biometrii behawioralnej np. sposób poruszania kursorem myszy lub przesuwania palcem po monitorze telefonu). Danymi osobowymi są więc np. wykorzystywane w paszportach biometrycznych odciski palców zapisywane w formie elektronicznej w czipach, skany siatkówki oka czy nagrania głosu wykorzystywane do identyfikacji w bankach – do dostępu do rachunku przez klienta lub do pomieszczeń chronionych przez pracowników.

Skoro zgodnie z definicją i motywem 51 RODO dane biometryczne wynikają ze „specjalnego przetwarzania technicznego" i jednoznacznie identyfikują osobę, to np. zdjęcia są danymi biometrycznymi w paszportach biometrycznych (ponieważ można je odczytać maszynowo na lotniskach), ale nie w albumach pamiątkowych.

Uzupełnienie RODO o definicje danych genetycznych i biometrycznych należy traktować jako doprecyzowanie, ponieważ ich brak w otwartym katalogu danych nie oznacza, że nie są danymi osobowymi, jeżeli umożliwiają identyfikację osoby fizycznej. Analogicznie, mimo że nie wszystkie ustawy państw trzecich wyraźnie wskazują te kategorie danych, uważam, że we wszystkich ustawach są one danymi osobowymi, pod warunkiem że identyfikują osobę fizyczną.

Południowoafrykańska POPIA (sekcja 1 POPIA) definiuje biometrię, w ramach danych wrażliwych, jako technikę indywidualnej identyfikacji opartej na charakterystyce fizycznej, fizjologicznej lub behawioralnej, w tym grupie krwi, odciskach palców, analizie DNA, skanach siatkówki oka i rozpoznawaniu głosu, a więc choć nie wymienia danych genetycznych jako odrębnej kategorii, zawiera elementy danych genetycznych (DNA) wśród danych biometrycznych.

W kalifornijskiej CCPA, w której dane biometryczne i genetyczne również są danymi wrażliwymi, informacje biometryczne ustawa definiuje [sekcja § 1798.140(c) CCPA] jako fizjologiczne, biologiczne lub behawioralne cechy danej osoby (np. wzorce lub rytmy naciśnięć klawiszy telefonu lub komputera, je-

żeli mogą posłużyć do identyfikacji), w tym informacje dotyczące DNA, obrazy tęczówki, siatkówki, odcisków palców, twarzy, dłoni, wzorów żył, nagrania głosu[39]; definicja podkreśla kryterium identyfikacji tożsamości[40]. Gubernator Kalifornii zatwierdził 28.9.2024 r. nowelizację CCPA rozszerzającą od 25.1.2025 r. katalog danych wrażliwych o dane neuronowe (*neural data*)[41].

U.S. Consumer Financial Protection Bureau zakwestionowało praktykę stosowania monitoringu, w szczególności opartego na systemach AI, do pomiaru wydajności pracowników, z wykorzystaniem ich danych osobowych, w tym danych biometrycznych, bez ich zgody. Consumer Financial Protection Bureau uznało się za właściwe w tej sprawie, bo podniosło, że Fair Credit Reporting Act ma zastosowanie do wykorzystania tej technologii i że jednym z celów tej ustawy jest zapobieganie potencjalnie krzywdzącemu profilowaniu pracowników bez ich zgody. Jeszcze bardziej wrażliwe mogą być tego rodzaju praktyki w sektorze ochrony zdrowia, ponieważ jak zwróciło uwagę Michigan Nurses Association, narzędzia nadzoru wykorzystujące systemy AI (należałoby dodać, że nie tylko systemy AI) umieszczone w identyfikatorach pielęgniarek wpływają również na ochronę prywatności pacjentów[42].

Na marginesie – to zbieżność z zakazem wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemów AI do wyciągania wniosków nt. emocji osoby fizycznej w miejscu pracy, z wyjątkiem przypadków, w których system AI ma zostać wdrożony lub wprowadzony do obrotu ze względów medycznych lub bezpieczeństwa (art. 5 ust. 1 lit. f rozp. 2024/1689), jednak w miejscu pracy (i w instytucjach edukacyjnych) zostało to uznane za nieakceptowalne ryzyko i zakazaną praktykę w zakresie AI. Choć poza nimi systemy AI wykorzystujące biometrię przy rozpoznawaniu emocji są systemami wysokiego ryzyka (załącznik III pkt 1 lit. c rozp. 2024/1689 oraz motyw 54 rozp. 2024/1689), a z tym poziomem ryzyka wiążą się określone obowiązki, ale nie zakaz ich stosowania (np. obowiązek informacyjny z art. 50 ust. 3 rozp. 2024/1689).

---

[39] Podobnie w pkt 5.4, s. 6, GB/T 35273–2020 [National Standard of the People's Republic of China, Information security technology – Personal information (PI) security specification z 6.3.2020 r. (信息安全技术 个人信息安全规范), State Administration for Market Supervision of the People's Republic of China Standardization Administration of the People's Republic of China, https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf (dostęp: 7.2.2025 r.)].

[40] *D.L. Buresh*, Should Personal Information and Biometric Data Be Protected Under a Comprehensive Federal Privacy Statute, s. 31.

[41] California: Bill to amend CCPA definition, https://www.dataguidance.com/news/california-bill-amend-ccpa-definition-sensitive-data-3 (dostęp: 7.2.2025 r.).

[42] *L. White*, US agencies take stand against AI-driven employee monitoring, https://iapp.org/news/a/cfpb-takes-on-enforcement-measures-to-prevent-employee-monitoring (dostęp: 5.3.2025 r.).

Ustawa rosyjska (art. 11 ust. 1 rosyjskiej ustawy federalnej Nr 152-FZ z 27.7.2006 r. o danych osobowych) definiuje dane biometryczne jako informacje dotyczące cech fizjologicznych i biologicznych osoby umożliwiające jej identyfikację i wykorzystywane przez administratora do ustalenia tożsamości osoby, której dane dotyczą; ich przetwarzanie wymaga pisemnej zgody podmiotu danych[43] z wyjątkiem przypadków takich jak określone w przepisach służących zapewnieniu bezpieczeństwa narodowego i publicznego, czy prowadzenia postępowań sądowych. Ustawa rosyjska nie wspomina natomiast o danych genetycznych.

Brazylijska LGPD (art. 5 ust. II LGPD) i turecka KVKK (art. 6 KVKK) wymieniają dane biometryczne i genetyczne w katalogu danych wrażliwych, ale szerzej ich nie definiują. Brak informacji o aspektach przetwarzania oraz zgody na stosowanie biometrii (odcisków palców) jako autoryzacji wstępu do pomieszczeń, ze względu na wrażliwy charakter danych biometrycznych, był powodem sankcji nałożonej przez turecki KVKK decyzją z 7.7.2022 r., Nr 2022/662.

Również chińska PIPL (art. 28 PIPL) wymienia dane biometryczne wśród danych wrażliwych, nie definiując ich, natomiast nie zawiera kategorii danych genetycznych, ale można przyjąć, że dane genetyczne też należą do danych wrażliwych, bo spełniają warunek ryzyka naruszenia godności lub spowodowania poważnych szkód dla bezpieczeństwa osobistego lub majątkowego w razie wycieku lub nielegalnego wykorzystania. Dane biometryczne i identyfikacyjne dane osobowe muszą być przechowywane oddzielnie, a ponadto zasadą jest wyjątkowe przechowywanie danych biometrycznych identyfikujących osobę[44].

Wytyczne wydane przez Najwyższy Sąd Ludowy Chin 28.12.2022 r. (Guiding Cases Nr 35) dotyczące postępowania karnego odnoszą się m.in. do rozpoznawania twarzy. Podobnie jak w RODO dane zbierane przez stosowanie tej technologii są danymi biometrycznymi[45].

---

[43] Sąd Najwyższy Federacji Rosyjskiej uznał fotografie za dane biometryczne i podkreślił wymóg pisemnej zgody pracodawcy na system dostępu oparty na identyfikacji pracowników na podstawie zdjęć (post. Sądu Najwyższego Federacji Rosyjskiej z 5.3.2018 r., 307-KG18-101).

[44] Pkt 6.3, s. 9, GB/T 35273–2020 [National Standard of the People's Republic of China, Information security technology – Personal information (PI) security specification z 6.3.2020 r. (信息安全技术 个人信息安全规范), State Administration for Market Supervision of the People's Republic of China Standardization Administration of the People's Republic of China, https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf (dostęp: 7.2.2025 r.)].

[45] Supreme Court Clarifies Scope Of Criminal Personal Information Violations, https://www.mondaq.com/china/data-protection/1286686/supreme-court-clarifies-scope-of-criminal-personal-information-violations (dostęp: 7.2.2025 r.).