Adrianna Michałowicz*

Przetwarzanie danych biometrycznych a ochrona jednostek – analiza wybranych zagadnień na tle ogólnego rozporządzenia o ochronie danych i projektu aktu w sprawie sztucznej inteligencji

Spis treści

Streszczenie

W ostatnich latach obserwujemy dynamiczny rozwój technologii opartych na przetwarzaniu danych osobowych z wykorzystaniem biometrii, czyli specjalnych technik przetwarzania danych pozwalających na jednoznaczną identyfikację osoby fizycznej. Rozwój ten w dużym stopniu jest wspierany przez coraz szersze zastosowanie sztucznej inteligencji (*artificial intelligence*) w procesach identyfikowania jednostek, pozwalające na osiąganie lepszych i bardziej dokładnych wyników przy przetwarzaniu danych biometrycznych. Stosowanie różnych technik biometrycznych w związku ze świadczeniem usług na rzecz konsumentów, w tym systemów rozpoznawania twarzy (*facial recognition*), oraz przetwarzanie w ten sposób danych na masową skalę budzi jednak wątpliwości natury prawno-etycznej, a także rodzi pytania o zasadność i konieczność sprawowania „biometrycznej kontroli" nad społeczeństwem.

Niniejszy artykuł podejmuje tematykę przetwarzania danych biometrycznych, ze szczególnym uwzględnieniem jednej z metod biometrycznego przetwarzania, jaką jest rozpoznawanie twarzy. Jest to zagadnienie rodzące wiele pytań prawnych, zwłaszcza w kontekście zakresu możliwej ingerencji w prawa podstawowe jednostek, jak i w kontekście rosnącego wykorzystywania mechanizmów sztucznej inteligencji na potrzeby tego rodzaju przetwarzania. W publikacji zaprezentowano ogólną charakterystykę celów i sposobów wykorzystywania systemów rozpoznawania

* Adwokat; doktorantka na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego w Katedrze Europejskiego Prawa Gospodarczego; kierownik projektu badawczego finansowanego przez Narodowe Centrum Nauki w ramach konkursu PRELUDIUM 20 pt. „Udostępnianie danych w interesie publicznym – filantropia danych z perspektywy prawnej" (nr umowy: UMO-2021/41/N/HS5/01490). Dwukrotna stypendystka Narodowej Agencji Wymiany Akademickiej (program PROM). Współautorka międzynarodowego bloga poświęconego tematyce prawa konsumenckiego „Recent Developments in European Consumer Law" (http://recent-ecl.blogspot.com). Ukończyła studia podyplomowe z zakresu prawa francuskiego w ramach Szkoły Prawa Francuskiego organizowanej przez Uniwersytet w Tours. Specjalizuje się w polskim i europejskim prawie gospodarczym, prawie ochrony danych osobowych, prawie własności intelektualnej i prawie nowych technologii; ORCID https://orcid.org/0000-0002-6262-2353.

twarzy, w tym zagrożeń, jakie mogą one powodować dla jednostek, a następnie analizę najczęściej obserwowanych naruszeń przepisów ogólnego rozporządzenia o ochronie danych w związku z przetwarzaniem danych biometrycznych, w tym w systemach wyposażonych w funkcje rozpoznawania twarzy. Analiza uwzględnia również projektowane regulacje dotyczące wykorzystywania w UE systemów zdalnej identyfikacji biometrycznej.

Słowa kluczowe: dane osobowe; dane biometryczne; sztuczna inteligencja; RODO; systemy zdalnej identyfikacji biometrycznej; systemy rozpoznawania twarzy.

JEL: K32

I. Wprowadzenie

Definicję legalną danych biometrycznych do unijnego porządku prawnego wprowadzono stosunkowo niedawno, bo dopiero na mocy art. 4 pkt 14 ogólnego rozporządzenia o ochronie danych[1]. Nie oznacza to, że problematyka przetwarzania danych biometrycznych nie była znana wcześniej. Wprost przeciwnie – jeszcze w okresie obowiązywania dyrektywy 95/46/WE[2] Grupa Robocza Art. 29[3] odniosła się do zagadnienia dopuszczalności przetwarzania danych biometrycznych m.in. w dokumencie roboczym dotyczącym biometrii (Grupa Robocza Art. 29, 2003) oraz w opinii w sprawie rozwoju technologii biometrycznych (Grupa Robocza Art. 29, 2012). Ramy definicyjne pojęcia „dane biometryczne" zostały zakreślone również w opinii w sprawie pojęcia danych osobowych (Grupa Robocza Art. 29, 2007). Choć prezentowane w ww. dokumentach zalecenia nie miały charakteru wiążącego, w istotny sposób przyczyniły się do kształtowania aktualnie obowiązującej definicji danych biometrycznych.

Zgodnie z art. 4 pkt 14 RODO, aby móc zakwalifikować określone dane osobowe jako dane biometryczne, muszą być spełnione trzy warunki. Po pierwsze, dane osobowe muszą dotyczyć cech fizycznych, fizjologicznych lub behawioralnych konkretnej osoby fizycznej. Cechy fizyczne lub fizjologiczne są najczęściej pozyskiwane za pomocą identyfikatorów morfologicznych, takich jak odciski palców, kształt dłoni lub twarzy, układ tęczówki i siatkówki oka, jak również analiz biologicznych, w tym analizy DNA, krwi, śliny itd. (Thales Group, 2021; Kuba, 2018). Z kolei cechy behawioralne są zwykle pobierane na podstawie analizy głosu, dynamiki podpisu, indywidualnego

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE L 119 z dn. 4.05.2016 r., str. 1 (dalej: RODO). Warto nadmienić, że definicja legalna danych biometrycznych zawarta została również w art. 3 pkt 18 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz. Urz. UE L 295 z dn. 21.11.2018 r., s. 39; dalej: rozporządzenie 2018/1725) oraz w art. 3 pkt 13 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89; dalej: dyrektywa 2016/680). Przepisy dyrektywy 2016/680 zostały implementowane do polskiego porządku prawnego mocą ustawy z dnia z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019 poz. 125; dalej: uzzp). We wszystkich ww. aktach prawnych przyjęte definicje danych biometrycznych są tożsame.

[2] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. UE L 281 z 23.11.1995, s. 31–50).

[3] Niezależna Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, powołana na mocy art. 29 nieobowiązującej już dyrektywy 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, miała charakter doradczy. W okresie obowiązywania RODO funkcję tę pełni Europejska Rada Ochrony Danych (EROD).

stylu chodzenia, charakterystycznych gestów itp. (Thales Group, 2021; Kuba, 2018). Po drugie, dane te muszą być poddane specjalnym technikom przetwarzania, tj. technikom biometrycznego przetwarzania. Ów aspekt techniczny jest kluczowym elementem, determinującym czy dochodzi do przetwarzania danych biometrycznych, czy też nie. Informacje dotyczące cech fizycznych, fizjologicznych lub behawioralnych człowieka nieprzetwarzane za pomocą specjalnych technik nie będą traktowane jako dane biometryczne, co – jak wskazuje się w literaturze – jest w pełni uzasadnione, ponieważ wiele informacji zawierających cechy biometryczne człowieka stanowi przedmiot codziennego, zwykłego obrotu, w związku z czym niecelowe byłoby stosowanie do każdego przypadku przetwarzania takich informacji regulacji dotyczących danych biometrycznych (Kuba, 2018). Wreszcie po trzecie, w wyniku takiego przetwarzania danych możliwa jest jednoznaczna identyfikacja konkretnej osoby fizycznej. Biometryczne przetwarzanie danych pozwala więc na identyfikację i uwierzytelnienie osoby fizycznej w oparciu o jej unikalne cechy, które można przypisać wyłącznie tej konkretnej osobie. W praktyce polega to na określaniu tożsamości osoby poprzez uchwycenie elementu jej danych biometrycznych (np. wizerunku twarzy lub odcisku palca), a następnie porównanie go z posiadanym przez administratora wzorcem biometrycznym (*biometric templates*), tj. zredukowaną strukturą obrazu danej biometrycznej w postaci cyfrowej (Kuba, 2018).

Dane biometryczne zostały zakwalifikowane przez prawodawcę unijnego do szczególnej kategorii danych osobowych – tzw. danych sensytywnych, zwanych też danymi wrażliwymi, których przetwarzanie podlega szczególnym obowiązkom. Wyodrębnienie tej kategorii danych osobowych podyktowane jest potrzebą zapewnienia dodatkowych środków ochronnych z uwagi na fakt, że przetwarzanie danych sensytywnych może stanowić poważną ingerencję w sferę prywatną, a nawet intymną osób fizycznych lub potencjalnie powodować znacznie większe zagrożenia niż przetwarzanie danych zwykłych (Fajgielski, 2018). Z tych przyczyn przetwarzanie danych wrażliwych, w tym m.in. danych biometrycznych, jest co do zasady zakazane. Zakaz ten został ujęty zarówno w art. 9 ust. 1 RODO, art. 10 dyrektywy 2016/680[4], jak i w art. 10 ust. 1 rozporządzenia 2018/1725, przy czym nie ma on charakteru bezwzględnego. Dopuszczalność przetwarzania szczególnej kategorii danych osobowych zależy od spełnienia warunków określonych w przepisach. O ile katalog przesłanek zawartych w art. 9 ust. 2 RODO i art. 10 ust. 2 rozporządzenia 2018/1725 jest niemal tożsamy, różnice wynikają zaś z konieczności dostosowania przesłanek do przedmiotu i zakresu stosowania poszczególnych aktów prawnych, o tyle inaczej zostały ukształtowane przesłanki dopuszczalności przetwarzania danych wrażliwych na gruncie dyrektywy 2016/680[5]. Zgodnie z art. 10 dyrektywy 2016/680 przetwarzanie szczególnej kategorii danych osobowych jest dopuszczalne jedynie wówczas, gdy jest bezwzględnie niezbędne oraz podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą. Dodatkowo, za każdym razem

[4] Na marginesie warto dodać, że konstrukcja tego przepisu jest inna niż w przypadku art. 9 ust. 1 RODO czy art. 10 ust. 1 rozporządzenia 2018/1725, gdyż nie zawiera on wprost zakazu przetwarzania szczególnych kategorii danych osobowych, a jedynie wskazuje na sytuacje, kiedy takie przetwarzanie jest „wyłącznie dozwolone". W praktyce sprowadza się to oczywiście do zakazu przetwarzania danych wrażliwych w okolicznościach innych niż opisane w przepisie, a samo przyjęcie przez prawodawcę unijnego odwrotnej konstrukcji niż na gruncie RODO i rozporządzenia 2018/1725 jest, jak się wydaje, podyktowane rodzajem aktu prawnego. Celem przyjęcia dyrektywy 2016/680 było bowiem zbliżenie przepisów państw członkowskich i zharmonizowanie zasad „ochrony i swobodnego przepływu danych osobowych przetwarzanych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom" (zob. motyw 15 dyrektywy 2016/680). W gestii państw członkowskich pozostaje ewentualna możliwość wprowadzenia wyższego standardu ochrony niż przewidzianego dyrektywą.

[5] Niniejszy artykuł nie zawiera szczegółowej analizy zagadnień dotyczących przetwarzania danych biometrycznych w kontekście zwalczania przestępczości. Kwestia ta stanowi odrębny przedmiot badań prowadzonych przez autorkę. Ich wyniki zostaną zaprezentowane w odrębnej publikacji.

musi być spełniona jedna z trzech przesłanek, tj. a) przetwarzanie takie jest dopuszczone prawem Unii lub prawem państwa członkowskiego; b) jest niezbędne dla ochrony żywotnych interesów osoby fizycznej, której dane dotyczą, lub innej osoby, lub c) dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą[6].

Mimo licznych ograniczeń prawnych ustanowionych w związku z przetwarzaniem danych biometrycznych, traktowanych jako szczególna kategoria danych osobowych i przez to wymagających podwyższonego standardu ochrony, stosowanie technik biometrycznych staje się coraz powszechniejsze, tak w życiu prywatnym, jak i publicznym. Jako konsumenci często korzystamy ze smartfonów lub komputerów, do których logujemy się po uprzednim przetworzeniu przez urządzenie naszych danych w postaci linii papilarnych lub wizerunku twarzy. Niektóre aplikacje mobilne lub usługi świadczone online oferują biometryczne metody weryfikacji użytkownika lub klienta, podnosząc w ten sposób poziom zabezpieczeń przed nieuprawnionym dostępem, ale też pozyskując dzięki temu cenne informacje o grupach swoich odbiorców, które mogą następczo wykorzystać w celach marketingowych (Fourtané, 2020)[7]. W zakładach pracy biometria jest wykorzystywana w celu zapewnienia ochrony i ograniczenia dostępu do pomieszczeń, w których przechowywane są dokumenty zawierające np. informacje objęte tajemnicą przedsiębiorstwa lub też w celu umożliwienia dostępu do strategicznych urządzeń produkcyjnych wyłącznie pracownikom posiadającym odpowiednie kwalifikacje, upoważnionym przez pracodawcę do ich obsługi oraz ponoszącym odpowiedzialność za nadzór lub prawidłowe operowanie urządzeniem. Wreszcie, do biometrycznego przetwarzania danych osobowych dochodzi również w miejscach publicznych, np. na lotniskach, dworcach, placach miejskich, gdzie jest to podyktowane potrzebą zapewnienia powszechnego bezpieczeństwa, skuteczniejszego wykrywania osób poszukiwanych, lepszą kontrolą podróżujących itp. Biometryczne przetwarzanie danych ma również miejsce w placówkach edukacyjnych, i to w odniesieniu do danych osobowych dzieci[8].

Niewątpliwie stosowanie biometrii w wielu przypadkach jest korzystne, gdyż pozwala lepiej osiągnąć cele przetwarzania, zwłaszcza gdy na jego potrzeby wykorzystywane są najnowsze techniki biometryczne. Wskazuje się, że biometryczne przetwarzanie danych mogłoby podnieść ogólny poziom bezpieczeństwa w miejscach publicznych, usprawnić procesy wykrywania zagrożeń dla bezpieczeństwa publicznego, ułatwić organom ścigania identyfikację osób podejrzanych lub poszukiwanych (Allix, 2018). Niemniej jednak, różnorodność metod biometrycznego przetwarzania danych, w połączeniu z rosnącą tendencją do ich szerokiego wykorzystywania z uwagi na osiągane rezultaty, wywołuje wątpliwości co do zakresu możliwej ingerencji w życie prywatne jednostek, w szczególności w sytuacji, gdy technologie biometryczne są elementem systemów kontroli i nadzoru stosowanych przez organy publiczne. Ponadto, nierzadko stosowanie technik biometrycznych nie wymaga zaangażowania po stronie osób, których dane są w ten sposób przetwarzane, a w wielu przypadkach podmiot danych może nawet nie mieć świadomości, że

[6] Art. 10 dyrektywy 2016/680 został implementowany do polskiego porządku prawnego poprzez art. 14 uzzp. W przepisie tym polski ustawodawca wprowadził ogólny zakaz przetwarzania danych wrażliwych (ust. 1), przewidując jednocześnie wyjątki takie same w omawianym przepisie dyrektywy 2016/680 (ust. 2).

[7] Mogą to być np. informacje o płci, wieku, stanach emocjonalnych.

[8] Przykładowo wyr. WSA w Warszawie z 07.08.2020, II SA/Wa 809/20 dotyczący biometrycznego przetwarzania danych dzieci w związku z dostępem do szkolnej stołówki; decyzję szwedzkiego organu nadzorczego nakładającą karę za naruszenie ochrony danych osobowych w związku z przetwarzaniem danych biometrycznych w celu weryfikacji obecności uczniów w szkole zob. https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv (15.10.2021).

dochodzi do przetwarzania jego danych biometrycznych[9]. Z tych przyczyn w wielu środowiskach postuluje się podjęcie publicznej debaty na temat dopuszczalnego zakresu wykorzystywania technologii biometrycznego przetwarzania danych osobowych oraz ich wpływu na funkcjonowanie jednostek i całych społeczeństw, celów, jakie mogą być w ten sposób realizowane, jak również tego, w jakich sytuacjach technologie te w ogóle nie powinny być używane (Selvadurai, 2015). Na potrzebę szerokiej dyskusji zwracają uwagę zwłaszcza krajowe organy nadzorcze oraz liczne organizacje pozarządowe[10].

II. Technologie rozpoznawania twarzy – ogólna charakterystyka w kontekście zagrożeń dla praw i wolności jednostek

Wśród różnych urządzeń opartych na biometrycznych metodach przetwarzania danych coraz szerszym zastosowaniem cieszą się urządzenia wyposażone w funkcje rozpoznawania twarzy. Współcześnie technologie te znajdują wiele zastosowań. Najczęściej wykorzystywane są w czterech celach: rozpoznania, weryfikacji, identyfikacji oraz kategoryzacji (PE, 2021). Rozpoznawanie polega na skanowaniu obrazu w celu wykrycia na nim konkretnego wizerunku twarzy, weryfikacja – na porównywaniu dwóch wzorów zawierających cechy biometryczne w celu potwierdzenia tożsamości danej osoby fizycznej, identyfikacja zaś – na porównywaniu wzoru z wizerunkiem twarzy z innymi wzorami przechowywanymi w bazie w celu sprawdzenia czy ten konkretny wzór jest również dostępny w bazie, natomiast kategoryzacja polega na ocenianiu wzorców z cechami biometrycznymi twarzy i następnie na klasyfikowaniu ich pod kątem określonych atrybutów twarzy, jak np. płeć, rasa, pochodzenie etniczne lub na szacowaniu określonych atrybutów, jak np. wiek, wyraz twarzy, stan emocjonalny (European Union Agency for Fundamental Rights, 2020; Leslie, 2020; Castelluccia i Le Métayer Inria, 2020). Dużym wsparciem w rozwoju technologii rozpoznawania twarzy są systemy oparte na sztucznej inteligencji, zwłaszcza wykorzystujące techniki głębokiego uczenia (*deep learning*) lub algorytmy widzenia komputerowego (*computer vision algorithms*), ponieważ dzięki ich zastosowaniu można w bardziej efektywny sposób realizować cele biometrycznego przetwarzania danych. Wykorzystywanie sztucznej inteligencji pozwala bowiem na osiąganie bardziej precyzyjnych wyników, w krótszym czasie, nawet mimo słabszej jakości materiału badawczego[11]. Bezspornie włączanie do technologii rozpoznawania twarzy systemów opartych na głębokim uczeniu zrewolucjonizowało metody biometrycznego przetwarzania danych, a ze względu na osiągane efekty, staje się obecnie podstawą rozwoju tego rodzaju technologii (Wang i Deng, 2020).

Mimo licznych korzyści, jakie oferuje technologia rozpoznawania twarzy, może ona powodować równie wiele zagrożeń dla praw jednostek. Tego typu przetwarzanie jest powszechnie uznawane za dość inwazyjne wkraczanie w prywatność jednostek z kilku przyczyn. Przede wszystkim, biometryczne przetwarzanie danych bazuje na wykorzystywaniu informacji mających charakter, co

[9] Przykładowo, gdy stosowane są techniki biometrycznego rozpoznawania twarzy w miejscach publicznych, dochodzi wówczas do porównania pobranego wizerunku twarzy z innymi wizerunkami dostępnymi w bazie administratora, przy czym wzory wizerunków znajdujące się w bazie mogą być tworzone w oparciu o zdjęcia dostępne w Internecie lub pozyskane z systemów monitoringu przestrzeni publicznej. Sama czynność pozyskania danych biometrycznych, np. osoby przebywającej w miejscu publicznym, nie wymaga od niej szczególnego zachowania. Poza tym, twarz jest również najbardziej widoczną częścią ciała, najtrudniejszą do ukrycia. Więcej: zob. Rada Europy, 2021.

[10] Zob. przykładowo: CNIL, 2019; Crawford i in., 2019; Castelluccia i Le Métayer Inria, 2020; La Quadrature du Net, 2020.

[11] Przykładowo, gdy analizowany wizerunek twarzy jest słabo oświetlony lub przysłonięty przez jakąś przeszkodę (zob. PE, 2021, s. 2).

do zasady, niezmienny i unikalny dla konkretnej osoby fizycznej (Grupa Robocza Art. 29, 2003)[12]. Umożliwia to z jednej strony, o czym była już mowa wcześniej, osiąganie precyzyjnych wyników przetwarzania, z drugiej zaś – powoduje, że raz pozyskane dane osoby fizycznej nie zdezaktualizują się, a sam podmiot danych nie może ich zmienić tak łatwo, jak inne dane osobowe, np. numer telefonu, adres zamieszkania. Co więcej, w przeciwieństwie do innych cech biometrycznych, które wymagają uprzedniego pobrania od podmiotu danych, w przypadku technologii rozpoznawania twarzy materiał porównawczy, potrzebny do identyfikacji osoby fizycznej, jest stosunkowo łatwy do pozyskania, gdyż obrazy twarzy są dostępne na dużą skalę w Internecie czy w bazach danych należących do podmiotów publicznych lub prywatnych, tworzonych przy okazji wykonywania zadań publicznych, monitorowania przestrzeni publicznej lub prywatnej itp. Obrazy zawierające wizerunki twarzy mogą być też pobierane „na odległość" – bez wiedzy po stronie podmiotu danych (Castelluccia i Le Métayer Inria, 2020).

Z kolei z technicznego punktu widzenia technologia rozpoznawania twarzy wciąż nie jest doskonała i pozbawiona ryzyka błędu, nawet gdy bazuje na bardzo zaawansowanych systemach przetwarzania danych (PE, 2021). Już prawie dekadę temu Grupa Robocza Art. 29 w swojej opinii wskazywała, że przetwarzanie danych osobowych za pomocą technik biometrycznych obarczone jest dwoma rodzajami błędów: 1) wynikami fałszywie pozytywnymi, polegającymi na błędnym zidentyfikowaniu osoby fizycznej i tym samym zaakceptowaniu osoby nieuprawnionej przez dany system lub 2) wynikami fałszywie negatywnymi, polegającymi na błędnym niedopasowaniu pobieranych danych do wzorca znajdującego się w systemie, a przez to błędnej odmowie akceptacji osoby uprawnionej (Grupa Robocza Art. 29, 2012). Wydajność większości systemów rozpoznawania twarzy nadal pozostaje ograniczona. Błędy pojawiają się zwłaszcza, gdy algorytmy zastosowane w oprogramowaniu nie zostały dostatecznie przeszkolone lub gdy porównywane obrazy nie są wystarczającej rozdzielczości, różnią się oświetleniem, cieniami, tłem lub innymi elementami obniżającymi jakość analizy. Błędy mogą być też pochodną różnic czasowych między utrwaleniem wizerunku tej samej osoby na porównywanych obrazach, tj. gdy zdjęcia poddane analizie przedstawiają tę samą osobę, ale w różnym wieku (PE, 2021). Co istotne, poziom błędów może być inny w zależności od tego, do jakiej populacji lub grupy społecznej należą osoby fizyczne, których wizerunki twarzy są analizowane[13]. Zdarza się, że niektóre systemy mają lepsze wyniki w przypadku osób o białej skórze niż osób o ciemnej skórze, mężczyzn niż kobiet lub osób dorosłych niż nastolatków. Tak istotne mankamenty technologiczne rodzą realne ryzyko dyskryminacji jednostek, błędów powodowanych stronniczością algorytmów (*error bias*) i przyczyniają się do rozwoju zjawisk, takich jak niesprawiedliwość dystrybucyjna lub uznaniowa (*distributive and recognitional injustice*)[14]. W rezultacie w wielu przypadkach kwestionowana jest zasadność wykorzystywania technologii rozpoznawania twarzy, ponieważ potencjalne zagrożenia dla praw

[12] Cechy, takie jak linie papilarne, DNA, obraz siatkówki oka itd., są stałe. Ulegają zmianie jedynie w wyjątkowych przypadkach, typu wypadek, uraz, operacja itp.

[13] Dostępne badania pokazują, że ryzyko dyskryminacyjnego traktowania osób o ciemnej karnacji jest większe w ramach egzekwowania prawa – np. w USA częstotliwość występowania fałszywych wyników pozytywnych ma nieproporcjonalnie duży wpływ na osoby ciemnoskóre, powodując odwrócenie ciężaru dowodu w sprawach karnych, zwłaszcza w kontekście stosowania zasady domniemania niewinności. Błędy w rozpoznawaniu twarzy powodują, że osoby podejrzane lub oskarżone muszą wykazywać, że nie są osobami, za które uważa je system. Więcej na ten temat w: Lynch, 2020; Buolamwini, Gebru, 2018; Cavazos, Phillips, Castillo, O'Toole, 2021.

[14] Niesprawiedliwość dystrybucyjna polega na tym, że członkom dyskryminowanej grupy społecznej odmawia się dostępu do korzyści, zasobów lub możliwości ze względu na ich przynależność do tej grupy, natomiast niesprawiedliwość uznaniowa przejawia się tym, że odmawia się uznania przynależności do określonej dyskryminowanej grupy społecznej, co tylko wzmacnia jej zmarginalizowaną pozycję (zob. Whittaker i in., 2018).

i wolności osób fizycznych, jakie może powodować, są większe aniżeli korzyści uzasadniające jej stosowanie.

Technologia rozpoznawania twarzy budzi także wiele wątpliwości w kontekście prawa jednostki do zachowania anonimowości w różnych miejscach lub sytuacjach. Możliwość pobierania wizerunków twarzy osób fizycznych w przestrzeni publicznej, przetwarzania za pomocą technik biometrycznych i ustalania w ten sposób ich tożsamości w oparciu o inne dane dostępne w bazie administratora powodują, że coraz częściej mówi się o istotnych zagrożeniach związanych ze stosowaniem powszechnych systemów nadzoru, skutkujących brakiem możliwości zachowania anonimowości, obawami przed wyrażeniem własnych poglądów, manifestowaniem określonych zachowań, uczestnictwem w zgromadzeniach, protestach itp. (European Union Agency for Fundamental Rights, 2020). Świadomość, że ludzie są obserwowani w przestrzeni publicznej za pomocą technologii rozpoznawania twarzy może skłaniać jednostki do zmiany zachowań, wpływać krępująco na autonomię woli jednostki czy ograniczać swobodę w korzystaniu z podstawowych praw obywatelskich poprzez zniechęcanie do partycypacji w określonych wydarzeniach, hamowanie aktywności na polu społeczno-polityczno-gospodarczym itp.

III. Stosowanie systemów opartych na przetwarzaniu danych biometrycznych, w tym umożliwiających rozpoznawanie twarzy, z perspektywy RODO

Wiele pytań o dopuszczalny zakres wykorzystywania systemów opartych na przetwarzaniu danych biometrycznych, w tym wyposażonych w funkcję rozpoznawania twarzy, można postawić z perspektywy ochrony danych osobowych. Z uwagi na wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator powinien odpowiednio przygotować się do tego rodzaju czynności przetwarzania, weryfikując nie tylko to czy dysponuje właściwą podstawą legalizującą przetwarzanie lub czy wdrożył odpowiednie środki techniczne i organizacyjne mające na celu zapewnienie zgodności przetwarzania z przepisami rozporządzenia, lecz także czy spełnia inne wymogi, w tym szczególne obowiązki nałożone na niego w związku z przetwarzaniem danych wrażliwych, jak np. obowiązek przeprowadzenia oceny skutków dla ochrony danych (*data protection impact assessment*)[15] lub uprzednich konsultacji z organem nadzorczym[16]. Co ważne, na kwestie związane z ochroną danych osobowych powinny zwracać uwagę zarówno podmioty korzystające z systemów opartych na przetwarzaniu danych biometrycznych, czyli w praktyce administratorzy i podmioty przetwarzające, jak i podmioty zajmujące się ich tworzeniem oraz produkcją urządzeń wykorzystujących techniki biometryczne, w tym technologię rozpoznawania twarzy, gdyż rozwiązania techniczne bazujące na przetwarzaniu danych osobowych, w tym danych wrażliwych, powinny być projektowane z uwzględnieniem zasad służących wzmocnieniu ochrony prywatności i minimalizacji danych, m.in. zasad *privacy by design* i *privacy by default* (EROD, 2020a).

Mimo że przetwarzanie danych biometrycznych jest dopuszczalne na mocy RODO tylko w określonych przypadkach, można zaobserwować tendencję do stopniowego rozszerzania zakresu stosowania biometrii, niestety nie zawsze w sposób zgodny z prawem ochrony danych

[15] Zob. art. 35 RODO.

[16] Zob. art. 36 RODO.

osobowych (Castelluccia i Le Métayer Inria, 2020). Wiele naruszeń w zakresie przetwarzania przez administratorów danych biometrycznych można dostrzec na tle realizacji zasad przetwarzania danych osobowych, zwłaszcza zasady minimalizacji danych oraz określania przesłanek legalizujących przetwarzanie. Wniosek taki można wyciągać, analizując decyzje wydawane przez krajowe organy nadzorcze, stwierdzające uchybienia, jakich dopuszczają się administratorzy i podmioty przetwarzające w odniesieniu do przetwarzania danych biometrycznych. W tym kontekście warto wskazać chociażby na decyzję Prezesa UODO z dnia 18 lutego 2020 r. stwierdzającą naruszenie przez szkołę podstawową w Gdańsku art. 5 ust. 1 lit. c) i art. 9 ust. 1 RODO polegające na przetwarzaniu danych biometrycznych dzieci podczas korzystania przez nie z usług stołówki szkolnej[17], co w ocenie Prezesa nie było niezbędne dla osiągnięcia celu, jakim jest identyfikacja uprawnienia dziecka do odebrania obiadu, gdyż cel ten można było realizować za pomocą środków mniej ingerujących w prywatność dziecka korzystającego z usług stołówki szkolnej. Jak podkreślił Prezes UODO, przetwarzanie danych biometrycznych powinno odbywać się ze szczególną ostrożnością i rozwagą, ponieważ ewentualny ich wyciek skutkuje dużym ryzykiem naruszenia praw i wolności osób fizycznych, zwłaszcza w przypadku dzieci, gdyż z uwagi unikalność i stałość danych biometrycznych skutki takiego naruszenia mogą okazać się niemożliwe do odwrócenia w czasie, nawet po osiągnięciu przez dziecko pełnoletności. Dodatkowo, organ dostrzegł naruszenie w postaci braku przesłanki legalizującej przetwarzanie danych biometrycznych – podstawą przetwarzania jakichkolwiek danych osobowych dzieci w związku z organizacją stołówki powinien być art. 6 ust. 1 lit. e) RODO, ponieważ przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi[18]. Szkoła więc błędnie opierała przetwarzanie danych dzieci na zgodzie uzyskanej od ich rodziców. Jak zaakcentował Prezes UODO, szkoła może przetwarzać tylko te dane osobowe ucznia, które są niezbędne do świadczenia usług stołówki szkolnej, przy czym żaden przepis prawa powszechnie obowiązującego nie zezwala szkole w takiej sytuacji na przetwarzanie danych biometrycznych. Co więcej, oprócz naruszeń z zakresu RODO, stosowanie biometrii w placówce było promowane w ten sposób, że uczniowie niekorzystający z tego systemu weryfikacji w stołówce zobowiązani byli do przepuszczenia w kolejce wszystkich pozostałych uczniów posiadających biometryczne identyfikatory, co w ocenie organu było dowodem na nierówne traktowanie uczniów[19]. Co ciekawe, decyzja Prezesa UODO została uchylona przez Wojewódzki Sąd Administracyjny w Warszawie[20] – zdaniem WSA administrator wykazał spełnienie przesłanki legalizującej przetwarzanie danych biometrycznych w postaci zgody, o której mowa w art. 9 ust. 2 lit. a) RODO, a ponadto nie naruszył zasady minimalizacji danych. Jak wskazał WSA, dokonana przez organ wykładnia zasady minimalizacji danych jest błędna, gdyż całkowicie pomija aspekt adekwatności i stosowności; wymóg adekwatności i stosowności pozwala zaś na dopuszczenie przetwarzania danych, które w istotny sposób, np. łatwiej, szybciej lub taniej, mogą pomóc osiągnąć cele przetwarzania. Administrator wykazał natomiast istnienie uzasadnionego związku między celem przetwarzania a ustalonym przez niego zakresem przetwarzanych danych, a także to, że poprzednio stosowane

[17] Dec. Prezesa UODO z 18.02.2020 r., ZSZZS.440.768.2018.

[18] Możliwość organizacji stołówki szkolnej wynika z art. 106 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz.U. 2019, poz. 1148).

[19] W tym kontekście nie bez znaczenia pozostaje też liczbowa proporcja uczniów korzystających z identyfikacji biometrycznej (ponad sześćset) i uczniów niekorzystających (łącznie sześciu).

[20] Wyr. WSA w Warszawie z 7.08.2020 r., II SA/Wa 809/20.

metody weryfikacji danych nie spełniały oczekiwań, w związku z czym decyzja o skorzystaniu z biometrycznych metod identyfikacji uczniów na stołówce była umotywowana.

Zgodność przetwarzania danych biometrycznych z RODO była przedmiotem oceny również innych organów nadzorczych. Analiza wydanych do tej pory decyzji prowadzi do wniosku, że organy nadzorcze dość restrykcyjnie podchodzą do kwestii dopuszczalności przetwarzania danych biometrycznych, traktując je rzeczywiście w kategoriach wyjątku. Przykładowo, szwedzki organ nadzorczy w sprawie przedmiotowo podobnej do tej, która była prowadzona przez Prezesa UODO, zaprezentował analogiczne podejście, uznając że przetwarzanie danych biometrycznych dzieci na potrzeby weryfikacji obecności na zajęciach szkolnych nie może być oparte na zgodzie rodziców jako przesłance legalizującej przetwarzanie ze względu na brak równowagi pomiędzy administratorem a podmiotem danych[21]. Podobnie szwedzki organ ocenił w tym kontekście naruszenie zasady minimalizacji danych, stwierdzając, że wykorzystywanie biometrii do sprawdzania obecności prowadzi do gromadzenia danych w sposób nadmiarowy i nieproporcjonalny względem celu przetwarzania. Co istotne, takie stanowisko zaaprobował sąd rozpoznający środek zaskarżenia od decyzji szwedzkiego organu[22]. Podobny pogląd w kwestii przetwarzania danych biometrycznych dzieci w ramach pilotażowego programu rozpoznawania twarzy uczniów w szkole wyraził francuski organ nadzorczy oraz Sąd Administracyjny w Marsylii (za Rapcewicz, 2020)[23], natomiast w kontekście przetwarzania danych biometrycznych pracowników – niderlandzki i rumuński organ nadzorczy[24].

Coraz częściej uwagę organów nadzorczych przykuwają także systemy oparte na przetwarzaniu danych biometrycznych stosowane w miejscach publicznych, np. w supermarketach. Przykładowo, hiszpański organ nadzorczy nałożył karę na sieć supermarketów, w których wprowadzono monitoring wizyjny wyposażony w funkcję rozpoznawania twarzy osób przebywających na terenie sklepów. Według wyjaśnień złożonych przez administratora, system rozpoznawania twarzy stosowano w celu zapewnienia bezpieczeństwa w sklepach poprzez wykrywanie osób, wobec których orzeczono zakaz zbliżania się, np. po napaści na pracownika sklepu, lub które zostały ukarane za incydent w sklepie[25]. W ten sposób przetwarzane były jednak wizerunki wszystkich osób wchodzących do sklepów, w tym dzieci oraz pracowników. W ocenie organu administrator niezasadnie powoływał się na art. 6 ust. 1 lit. e) RODO i art. 9 ust. 2 lit. g) RODO jako podstawy przetwarzania danych osobowych, ponieważ nie spełnił warunków wymienionych w tych przepisach. Organ wskazał też na brak związku pomiędzy stosowanymi przez administratora środkami bezpieczeństwa a interesem publicznym, gdyż wykorzystywanie monitoringu z funkcją rozpoznawania twarzy służyło realizacji prywatnych interesów administratora i nie uzasadniało masowego przetwarzania danych wszystkich osób wchodzących na teren sklepów[26]. W decyzji podkreślono

[21] Zob.: https://www.imy.se/en/about-us/arkiv/nyhetsarkiv/facial-recognition-in-school-renders-swedens-first-gdpr-fine/ (5.12.2021). Brak równowagi sił pomiędzy administratorem a podmiotem danych, który udziela zgody na przetwarzanie jego danych osobowych, jest traktowany jako czynnik uniemożliwiający wyrażenie zgody w sposób dobrowolny, a tym samym uniemożliwiający oparcie przetwarzania na tej przesłance (zob. więcej: EROD, 2020b).

[22] Zob.: https://techlaw.se/wp-content/uploads/2021/06/KamR.pdf (5.12.2021).

[23] Zob. też: https://www.engage.hoganlovells.com/knowledgeservices/news/facial-recognition-challenged-by-french-administrative-court (5.12.2021).

[24] Zob. https://autoriteitpersoonsgegevens.nl/en/news/company-fined-processing-employees'-fingerprint-data; https://edpb.europa.eu/news/national-news/2019/romanian-supervisory-authority-issues-two-fines-each-23893-lei-eur-5000_ro (5.12.2021). Organy w swoich decyzjach podkreśliły m.in., że biometryczne przetwarzanie danych pracowników w związku z kontrolą obecności lub na potrzeby rejestracji czasu pracy jest zbyt inwazyjnym wkroczeniem w prywatność i nie jest niezbędne z perspektywy celu przetwarzania, gdyż cel ten może być osiągnięty innymi sposobami (zob. więcej w: Bielecki i Rapcewicz 2020).

[25] Zob. https://www.aepd.es/es/documento/ps-00120-2021.pdf (5.12.2021).

[26] Zob.: https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS/00120/2021&mtc=today (5.12.2021).

również naruszenie zasady minimalizacji poprzez przetwarzanie danych osobowych w zakresie większym aniżeli było to konieczne do osiągnięcia celów przetwarzania, a także sam fakt, że cele te mogły być osiągnięte innymi, mniej ingerującymi w prywatność, środkami. Warto w tym miejscu dodać, że podobny system rozpoznawania twarzy w celu zapewnienia bezpieczeństwa w sklepie miał być zastosowany w jednym z supermarketów w Holandii – w tym przypadku niderlandzki organ nadzorczy wysłał formalne ostrzeżenie do administratora z informacją o zakazie stosowania tego rodzaju technologii w sklepach[27]. Jak można przeczytać w oficjalnym komunikacie organu, rozwiązania oparte na przetwarzaniu danych biometrycznych i systemach rozpoznawania twarzy stanowią istotne zagrożenie dla konsumentów, ponieważ powodują, że „wszyscy stajemy się chodzącymi kodami kreskowymi" – nasze wizerunki są skanowane w różnych miejscach publicznych, przechowywane w bazach, mogą być łączone z innymi dostępnymi danymi, np. poprzez porównanie utrwalonego wizerunku z obrazami umieszczonymi na profilach społecznościowych, wreszcie są podstawą do podejmowania zautomatyzowanych decyzji wobec konkretnych osób, np. kwalifikowania ich jako osoby stanowiące zagrożenie dla bezpieczeństwa w sklepie lub przeciwnie – jako osoby, które warto sprofilować i monitorować ich zachowania zakupowe[28].

Oprócz uchybień dotyczących zasady minimalizacji danych, naruszenia można obserwować także na tle realizowania zasady ograniczenia celu przetwarzania[29]. Zdarzają się bowiem przypadki, gdy w trakcie przetwarzania danych biometrycznych dochodzi do zmiany celu przetwarzania, a w konsekwencji do przekroczenia dopuszczalnego zakresu przetwarzania tych danych (Castelluccia i Le Métayer Inria, 2020). Może to mieć miejsce przykładowo w sytuacji, gdy system oparty na technologii biometrycznej jest poddawany aktualizacjom poprzez dodawanie nowych funkcji, a przez to zwiększanie zakresu przetwarzania danych biometrycznych. Dochodzi wówczas do zmiany kontekstu przetwarzania, co skutkuje koniecznością ponownej weryfikacji po stronie administratora czy przetwarzanie jest zgodne z prawem[30]. Wskazuje się jednak, że nierzadko takie działania stanowią element z góry zaplanowanej strategii (PE, 2021). Co więcej, stopniowe rozszerzanie zastosowań tych systemów nie wywołuje z reguły masowego sprzeciwu społeczeństwa, lecz jest traktowane jako naturalna ewolucja technologiczna (Castelluccia i Le Métayer Inria, 2020).

Przetwarzanie danych biometrycznych niewątpliwie wymaga zastosowania podwyższonych standardów ochrony, gdyż wiąże się ze zwiększonym ryzykiem naruszenia praw i wolności podmiotów danych. Ryzyko to materializuje się zwłaszcza w kontekście zjawiska dyskryminacji, o którym była mowa powyżej, choć nie tylko. Z uwagi na specyfikę tej kategorii danych oraz to, że zawierają informacje pozwalające na jednoznaczną identyfikację osoby fizycznej, w dodatku informacje o charakterze trwałym i zasadniczo niepodatne na zmiany, ewentualne naruszenie ochrony takich danych osobowych może wywołać nieodwracalne skutki dla podmiotu danych. Z tego względu tak ważne jest prawidłowe zapewnienie właściwego poziomu ochrony danych biometrycznych oraz przyjęcie przez administratora takich rozwiązań, które zminimalizują ryzyko wystąpienia naruszeń. Wiele ważnych wskazówek w tym zakresie zawarła EROD w wydanych wytycznych

[27] Zob.: https://edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_en (5.12.2021).

[28] Zob.: https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-issues-formal-warning-supermarket-use-facial-recognition-technology (5.12.2021).

[29] Art. 5 ust. 1 lit. b) RODO.

[30] Zmiana m.in. celów i kontekstu przetwarzania aktualizuje obowiązek przeprowadzenia analizy ryzyka – zob. art. 24 i 32 RODO.

3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo. Europejska Rada Ochrony Danych zwróciła uwagę na dwie kluczowe, moim zdaniem, kwestie. Po pierwsze, stosowanie biometrii na potrzeby monitoringu wizyjnego, w tym w systemach rozpoznawania twarzy, w większości przypadków wymaga uzyskania wyraźnej zgody wszystkich osób, których dane mają być przetwarzane[31]. Co warto podkreślić, zgoda jako przesłanka legalizująca przetwarzanie danych wrażliwych musi przyjąć formę wyraźnego działania potwierdzającego, nie może być zaś wywodzona z określonego zachowania podmiotu danych, np. z faktu wejścia na teren monitorowany, mimo oznaczenia, że system monitoringu wykorzystuje technologie biometryczne[32]. Poza tym, oprócz spełnienia innych przesłanek warunkujących ważność udzielonej zgody, administrator powinien pamiętać o zapewnieniu alternatywnego rozwiązania, nieopartego na biometrii, np. w postaci osobnego wejścia do budynku dla osób, które nie wyrażają zgody na przetwarzanie danych biometrycznych[33]. Jest to istotne też z perspektywy osób, które ze względu na ograniczenia urządzeń wykorzystujących technologię biometryczną nie mogą z nich korzystać, jak np. osoby niepełnosprawne. Po drugie, EROD akcentuje, że nie zawsze stosowanie systemów monitoringu wizyjnego wyposażonych w technologię biometryczną będzie wchodziło w zakres stosowania art. 9 RODO. Jeśli administrator nie tworzy szablonów biometrycznych w celu jednoznacznego zidentyfikowania osób fizycznych, a zamiast tego odczytuje określone cechy fizyczne (np. wiek, płeć) jedynie w celu przypisania danej osoby do konkretnej grupy, a następnie dostarczania jej spersonalizowanych reklam, tj. reklam przewidzianych dla grupy, do której została zakwalifikowana, to nie przetwarza danych biometrycznych[34]. W mojej ocenie można mieć jednak wątpliwości czy takie stanowisko jest słuszne. Należy bowiem pamiętać, że już samo zestawienie ze sobą różnych informacji, do których administrator może mieć dostęp, jak choćby wieku, płci, lokalizacji, czasu przebywania w danym miejscu czy preferencji zakupowych, może sprawić, że określona osoba fizyczna stanie się co najmniej możliwa do zidentyfikowania. W takich sytuacjach, biorąc też pod uwagę tempo rozwoju technologii biometrycznych, granica pomiędzy przetwarzaniem danych wrażliwych a przetwarzaniem danych zwykłych może być trudna do ustalenia.

IV. Systemy zdalnej identyfikacji biometrycznej w świetle projektu aktu w sprawie sztucznej inteligencji

W kwietniu 2021 r. KE opublikowała projekt aktu w sprawie sztucznej inteligencji[35]. Proponowana regulacja ma na celu stworzenie ram prawnych dla rozwoju inwestycji i innowacji w dziedzinie sztucznej inteligencji, skoordynowanie europejskiego podejścia w tym zakresie oraz stworzenie warunków dla rozwoju godnej zaufania sztucznej inteligencji poprzez niwelowanie zagrożeń związanych z niektórymi zastosowaniami tej technologii, a jednocześnie promowanie stosowania sztucznej inteligencji w sposób bezpieczny, zgodny z prawem i z poszanowaniem praw podstawowych i na

[31] Mogą zachodzić też inne wyjątki z art. 9 ust. 2 RODO, jednak podstawą przetwarzania danych biometrycznych na potrzeby prywatnego monitoringu wizyjnego najczęściej będzie art. 9 ust. 2 lit. a) RODO.

[32] Zob. pkt 46 wytycznych 3/2019.

[33] Zob. pkt 86 wytycznych 3/2019.

[34] Zob. pkt 80 wytycznych 3/2019.

[35] Wniosek – rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, COM(2021) 206 final, Bruksela, dn. 21.4.2021 r. (dalej: projekt rozporządzenia lub akt w sprawie sztucznej inteligencji).

rzecz polepszenia dobrostanu społeczeństwa[36]. Projekt rozporządzenia, oprócz wprowadzenia definicji pojęcia „system sztucznej inteligencji"[37] czy klasyfikacji systemów sztucznej inteligencji z uwzględnieniem tzw. podejścia opartego na ryzyku[38], zawiera także regulację dotyczącą przetwarzania danych biometrycznych[39].

W myśl art. 5 ust. 1 lit. d) projektu rozporządzenia wykorzystywanie systemów zdalnej identyfikacji biometrycznej[40] w czasie rzeczywistym[41] w przestrzeni publicznej[42] do celów egzekwowania prawa powinno być co do zasady zakazane. Systemy te zakwalifikowano jako systemy wysokiego ryzyka z uwagi na wysoki stopień ingerencji w życie prywatne społeczeństwa, podatność na błędy techniczne, możliwość dostarczania nieobiektywnych wyników, a w konsekwencji – przyczyniania się do dyskryminacji jednostek[43]. Komisja Europejska postuluje jednak wprowadzenie kilku wyjątków, kiedy to wykorzystanie tego typu systemu jawi się jako „absolutnie niezbędne" i ma służyć realizacji jednego z trzech celów, a mianowicie: (i) poszukiwania konkretnych potencjalnych ofiar przestępstw, w tym zaginionych dzieci; (ii) zapobiegnięcia konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu, lub (iii) wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy przestępstwa lub podejrzanego o popełnienie przestępstwa, o którym mowa w art. 2 ust. 2 decyzji ramowej w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi[44]. Skorzystanie z któregoś z wyjątków powinno być poprzedzone zarówno wszechstronną analizą sytuacji powodującej konieczność zastosowania systemu zdalnej identyfikacji biometrycznej w czasie rzeczywistym[45], jak i konsekwencji wykorzystania systemu dla praw i wolności wszystkich zainteresowanych osób, w tym wagi, prawdopodobieństwa i skali tych konsekwencji[46]. Każdorazowe wykorzystanie systemu zdalnej identyfikacji biometrycznej

[36] Zob. uzasadnienie projektu rozporządzenia, s. 1–3.

[37] Zob. art. 3 pkt 1 projektu rozporządzenia, zgodnie z którym za system sztucznej inteligencji uważa się „oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję". KE proponuje, aby definicja ta była odpowiednio elastyczna i neutralna technologicznie. Na marginesie warto dodać, że tak szeroka definicja jest krytykowana (zob. Ebers i in., 2021).

[38] Z uwagi na różne stopnie ryzyka i rodzaje zagrożeń, jakie mogą wywoływać niektóre systemy sztucznej inteligencji, KE proponuje wprowadzenie zakazu stosowania niektórych praktyk jako sprzecznych z unijnymi wartościami, takimi jak poszanowanie godności ludzkiej, wolności, równości, demokracji i praworządności, oraz z prawami podstawowymi, w tym z prawem do niedyskryminacji, ochrony danych i prywatności oraz z prawami dziecka – zob. motyw 15 i nast. oraz art. 5 projektu rozporządzenia. Ponadto, w projekcie rozporządzenia wyróżniono kategorię w postaci systemów sztucznej inteligencji wysokiego ryzyka, których stosowanie wymaga spełnienia odpowiednich obowiązków – zob. tytuł III projektu rozporządzenia.

[39] Projekt rozporządzenia w art. 3 pkt 33 zawiera również autonomiczną definicję pojęcia „dane osobowe". Definicja ta jest jednak tożsama z definicją przyjętą na gruncie RODO.

[40] Samo pojęcie systemu zdalnej identyfikacji biometrycznej zostało zdefiniowane w art. 3 pkt 36 projektu rozporządzenia jako „system sztucznej inteligencji służący do identyfikacji osób fizycznych na odległość poprzez porównanie danych biometrycznych danej osoby z danymi biometrycznymi zawartymi w referencyjnej bazie danych, bez uprzedniej wiedzy użytkownika systemu sztucznej inteligencji, czy dana osoba będzie w nim figurować i czy może zostać zidentyfikowana".

[41] Należy odróżnić systemy zdalnej identyfikacji biometrycznej w czasie rzeczywistym od systemów *post factum*, o czym mowa w motywie 8 oraz art. 3 pkt 37 i 38 projektu rozporządzenia. W przypadku tych pierwszych, pobranie danych biometrycznych, porównanie i identyfikacja następują natychmiast, a przynajmniej bez znacznego opóźnienia; poza tym, systemy te wykorzystują materiał rejestrowany „na żywo" lub „w czasie zbliżonym do rzeczywistego", np. poprzez kamerę wideo. Z kolei systemy identyfikacji *post factum* działają w oparciu o dane biometryczne wcześniej pobrane, przez co porównanie danych i identyfikacja osoby fizycznej następują ze znacznym opóźnieniem.

[42] Za przestrzeń publiczną uważa się, zgodnie z motywem 9 i art. 3 pkt 39 projektu rozporządzenia, każde miejsce fizyczne, które jest dostępne dla ogółu osób, niezależnie od tego czy mają zastosowanie określone warunki dostępu (np. czy jest własnością prywatną czy publiczną).

[43] Zob. motyw 18 i 33 projektu rozporządzenia.

[44] Decyzja ramowa Rady z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między Państwami Członkowskimi (Dz. Urz. UE L 190 z dn. 18.07.2002 r., s. 1). Artykuł 2 ust. 2 tejże decyzji wymienia przestępstwa, takie jak: terroryzm, handel ludźmi, seksualne wykorzystywanie dzieci, nielegalny handel środkami odurzającymi, substancjami psychotropowymi, bronią, amunicją i materiałami wybuchowymi itd. Dodatkowo, zgodnie z art. 5 ust. 1 lit. d) pkt (iii) projektu rozporządzenia warunkiem zastosowania przewidzianego w nim wyjątku jest to, aby dane przestępstwo, według prawa państwa członkowskiego, było zagrożone karą pozbawienia wolności lub podlegało środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej trzy lata.

[45] W szczególności w analizie powinno się uwzględnić powagę, prawdopodobieństwo i skalę szkody wyrządzonej w przypadku niewykorzystania systemu zdalnej identyfikacji biometrycznej w czasie rzeczywistym.

[46] Art. 5 ust. 2 projektu rozporządzenia.

w czasie rzeczywistym w przestrzeni publicznej do celów egzekwowania prawa powinno też, zgodnie z projektem rozporządzenia, następować za uprzednim zezwoleniem odpowiedniego organu sądowego lub administracyjnego; jedynie w nagłych i uzasadnionych przypadkach można skorzystać z systemu bez zezwolenia, lecz wówczas trzeba wystąpić z wnioskiem o następcze zatwierdzenie stosowania systemu[47]. Dodatkowo, w projekcie przewidziano możliwość dla państw członkowskich wprowadzenia w prawie krajowym zezwolenia, pełnego lub częściowego, na korzystanie z systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów egzekwowania prawa[48].

Zgodnie z projektem rozporządzenia inne zdalne systemy identyfikacji biometrycznej, tj. niewykorzystywane w celu egzekwowania prawa, również powinny być kwalifikowane jako systemy wysokiego ryzyka, a w konsekwencji powinny spełniać wymogi dla nich przewidziane, i to niezależnie od tego czy systemy te przetwarzają dane w czasie rzeczywistym, czy *post factum*[49]. W odniesieniu do przetwarzania danych biometrycznych lub innych danych osobowych w przestrzeni publicznej, ale w celach innych niż egzekwowanie prawa, a także bez wykorzystania systemów przetwarzających dane w czasie rzeczywistym, konieczne jest nadal spełnienie wymogów wynikających z art. 9 ust. 2 RODO, art. 10 ust. 1 rozporządzenia 2018/1725 lub art. 10 dyrektywy 2016/680[50]. Ponadto, w projekcie rozporządzenia mowa jest także o systemach kategoryzacji biometrycznej, które służą do przypisywania osób fizycznych, na podstawie ich danych biometrycznych, do określonych kategorii, jak np. płeć, wiek, kolor włosów, kolor oczu, pochodzenie etniczne, orientacja seksualna lub polityczna[51]. Systemy te nie zostały zakwalifikowane jako systemy wysokiego ryzyka, w związku z czym mają podlegać jedynie obowiązkom informacyjnym i w zakresie przejrzystości[52].

Propozycja regulacji dotyczącej przetwarzania danych biometrycznych w systemach sztucznej inteligencji budzi sporo zastrzeżeń. Kwestionowana jest przykładowo zasadność rozróżniania zdalnych systemów identyfikacji biometrycznej w czasie rzeczywistym od tych *post factum*, podobnie jak systemów służących do biometrycznej identyfikacji od tych przeznaczonych do kategoryzacji. Zarówno w przypadku systemów identyfikacji biometrycznej w czasie rzeczywistym, jak i tych *post factum* negatywny wpływ na podstawowe prawa jednostek może być taki sam – podobnie mogą one oddziaływać na swobodę decyzji jednostek, np. co do udziału w zgromadzeniach czy podejmowania innych aktywności w przestrzeni publicznej. Ponadto, systemy te w równym stopniu podatne są na ryzyko popełniania błędów w procesie identyfikacji osób fizycznych (Kind, 2021). Co więcej, użyte w definicjach systemów pojęcia nieostre, jak „bez znacznego opóźnienia" czy „niewielkie opóźnienie", powodują realne obawy, że w praktyce granica pomiędzy odróżnianiem systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym od tych *post factum* będzie się zacierać, co z kolei potencjalnie powoduje ryzyko nadużyć ze strony organów publicznych,

47 Art. 5 ust. 3 projektu rozporządzenia.

48 Art. 5 ust. 4 projektu rozporządzenia.

49 Motyw 33 projektu rozporządzenia oraz Załącznik III do projektu rozporządzenia, pkt 1 lit. a). W odniesieniu do wymogów, jakie należy spełnić – zob. art. 8–29 projektu rozporządzenia.

50 Motyw 24 projektu rozporządzenia.

51 Art. 3 pkt 35 projektu rozporządzenia.

52 Z tym zastrzeżeniem, że obowiązki te nie mają zastosowania, gdy systemy kategoryzacji biometrycznej są zatwierdzone z mocy prawa do celów wykrywania przestępstw, przeciwdziałania przestępstwom i prowadzenia dochodzeń/śledztw w związku z przestępstwami – zob. art. 52 ust. 2 projektowanego rozporządzenia.

które takie systemy mogłyby stosować. Zwraca się też uwagę na to, że systemy kategoryzacji biometrycznej w niektórych przypadkach pozwalają na identyfikację osoby fizycznej, zwłaszcza gdy osoba ta posiada jakieś cechy charakterystyczne w wyglądzie zewnętrznym (Kind, 2021).

Wśród głosów krytycznych nie brakuje też opinii, że ogólny zakaz wykorzystywania systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym podlega zbyt szeroko zakreślonym wyjątkom, w praktyce zaś i tak nie będzie obejmować różnych podmiotów, które już teraz stosują tego rodzaju systemy na szeroką skalę (Chander i Jakubowska, 2021; Ebers i in., 2021). Obecnie systemy identyfikacji biometrycznej są przede wszystkim wykorzystywane przez podmioty prywatne, które nie realizują w ten sposób interesu dobra publicznego, lecz swoje własne, komercyjne (Ebers i in., 2021). Zakaz przyjęty w art. 5 ust. 1 lit. d) projektu rozporządzenia nie wpłynie zatem ani na ograniczenie stosowania w miejscach publicznych systemów wykorzystujących biometrię, ani na zwiększenie ochrony osób fizycznych przed negatywnymi skutkami ich stosowania. Wobec tego, postuluje się odejście od podziału różnych form zdalnych systemów identyfikacji biometrycznej na te, które są zakazane i dopuszczalne, na rzecz ustanowienia ogólnego zakazu stosowania jakichkolwiek form masowego nadzoru w przestrzeni publicznej – w odniesieniu zarówno do podmiotów publicznych, jak i do prywatnych (Chander i Jakubowska, 2021). Rekomendację taką zaprezentowali również Europejski Inspektor Ochrony Danych Osobowych i Europejska Rada Ochrony Danych we wspólnym stanowisku, wzywając m.in. do wprowadzenia zakazu wykorzystywania systemów opartych na sztucznej inteligencji i biometrycznym przetwarzaniu danych do automatycznego rozpoznawania cech ludzkich w publicznie dostępnych miejscach lub do kategoryzacji osób na grupy ze względu na pochodzenie etniczne, płeć, orientację polityczną lub seksualną lub z innych względów, gdyż takie podziały mogą przyczyniać się do rozwoju zjawiska dyskryminacji (EROD i EIOD, 2021)[53].

V. Podsumowanie

Na tle biometrycznego przetwarzania danych, w tym stosowania technologii rozpoznawania twarzy, ujawnia się wiele sprzecznych i trudnych do pogodzenia interesów – z jednej strony podmiotów danych, które są takiemu przetwarzaniu poddawane, z drugiej – podmiotów chcących korzystać z tego rodzaju rozwiązań zarówno w sektorze publicznym, jak i w prywatnym. Przyzwolenie na dalszy dynamiczny rozwój technologii, zwłaszcza opartych na sztucznej inteligencji, bez ustanowienia ścisłych ram regulacyjnych może spowodować, że jako społeczeństwo stracimy kontrolę nad tym, jak, gdzie, przez kogo i w jakich celach są przetwarzane nasze dane osobowe, w tym dane wrażliwe. Nie ulega przy tym wątpliwości, że rozwój technologii jest zarówno nieunikniony, jak i pożądany ze względów gospodarczych, jednak nie powinien być z pewnością realizowany kosztem podstawowych praw jednostek.

Przywołane w artykule stanowiska organów nadzorczych odnoszące się do przetwarzania danych biometrycznych, choć jak dotąd jeszcze nieliczne, ukazują utrwalającą się tendencję do ścisłego i restrykcyjnego interpretowania przepisów ogólnego rozporządzenia o ochronie danych, zwłaszcza gdy przetwarzanie danych z wykorzystaniem technik biometrycznych może mieć

[53] Wezwanie do wprowadzenia zakazu wykorzystywania sztucznej inteligencji do automatycznego rozpoznawania cech ludzkich w publicznie dostępnych przestrzeniach EROD powtórzyła również w stanowisku z 18.11.2021 r. w sprawie pakietu usług cyfrowych i strategii w zakresie danych, zob.: https://edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf (5.12.2021).

charakter masowy. Krajowe organy zwracają przede wszystkim uwagę na aspekt proporcjonalności przyjmowanych przez administratorów środków względem celów przetwarzania, jakie mają być osiągnięte. Jeśli w określonym przypadku cele przetwarzania mogą być osiągnięte innymi sposobami, administrator powinien z nich skorzystać. Wydaje się, że bez znaczenia w takiej sytuacji jest argument, iż zastosowanie technik biometrycznych pozwala łatwiej, taniej lub szybciej realizować interes administratora albo że przyczynia się do osiągnięcia bardziej precyzyjnych efektów przetwarzania. Co do zasady tego rodzaju argumenty, w ocenie organów nadzorczych, nie uzasadniają tak inwazyjnej ingerencji w prywatność osób fizycznych, gdyż wiążą się z dużym ryzykiem dla praw i wolności podmiotów danych. Ryzyko to może zmaterializować się np. jeśli dojdzie do naruszenia bezpieczeństwa przetwarzanych danych, poufności i integralności danych, przechowywania ich przez czas dłuższy niż konieczny dla realizacji celów przetwarzania itp. Warto jednak podkreślić, że praktyka krajowych organów w tym zakresie, mimo wielu podobnych rozstrzygnięć, nie jest jeszcze w pełni ukształtowana. Ponadto, co pokazuje *casus* przetwarzania danych biometrycznych przez szkołę podstawową w Gdańsku, może być kwestionowana przez sądy rozpoznające środki zaskarżenia od wydawanych decyzji.

Regulacje przyjmowane na poziomie UE sprzyjają wzmocnieniu ochrony jednostek przed negatywnymi skutkami stosowania różnych technologii ingerujących w życie prywatne osób fizycznych, ustanawiając, chociażby na mocy RODO, liczne obowiązki na podmioty przetwarzające dane osobowe. Mimo to, wydaje się, że nie są one wystarczające. Bezspornie krokiem w dobrym kierunku byłoby przyjęcie kompleksowych przepisów odnoszących się do kwestii wykorzystywania technologii zbudowanych na systemach sztucznej inteligencji, w tym technologii wykorzystywanych na potrzeby biometrycznej identyfikacji osób fizycznych. Zaproponowany przez KE w kwietniu br. projekt rozporządzenia, pomimo że – słusznie moim zdaniem – wprowadza podejście oparte na ryzyku, nie jest jednak pozbawiony wad i wymaga doprecyzowania wielu kwestii w toku prac legislacyjnych, aby faktycznie mógł realizować cele, o których mowa w motywie 1 projektu rozporządzenia, takie jak zapewnienie wysokiego poziomu ochrony zdrowia, bezpieczeństwa i praw podstawowych.

Bibliografia

Allix, G. (2018). *Comment des villes « hyper connectées » contrôlent l'espace public*. Pozyskano z: https://www.lemonde.fr/economie/article/2018/12/19/au-nom-de-la-smart-city-des-villes-sous-surveillance_5399527_3234.html (15.10.2021).

Bielecki, D. i Rapcewicz, A. (2020). Biometryczne metody weryfikacji tożsamości. *Magazyn ODO,* (13), 2–5.

Buolamwini, J. i Gebru, G. (2018). Gender shades: intersectional accuracy disparities in commercial gender classification. *Machine Learning Research*, (81).

Castelluccia, C. i Le Métayer Inria, D. (2020). *Impact Analysis of Facial Recognition: Towards a Rigorous Methodology*. Centre for Data Ethics and Innovation, s. 6–7.

Cavazos, J.G., Phillips, P.J., Castillo, C.D. i O'Toole, A.J. (2021). *Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?.* Cornell University. Pozyskano z: https://arxiv.org/abs/1912.07398 (20.10.2021).

Chander, S. i Jakubowska, E. (2021). *EU's AI law needs major changes to prevent discrimination and mass surveillance*. EDRI. Pozyskano z: https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/ (20.10.2021).

CNIL. (2019). *Facial recognition: for a debate living up to the challenges*. Pozyskano z: https://www.cnil.fr/en/facial-recognition-debate-living-challenges (16.10.2021).

Crawford, K., Dobbe, R., Dryer, T., Fried, G., Green, B., Kaziunas, E., Kak, A., Mathur, W., McElroy, E., Nill Sánchez, A., Raji, D., Rankin, J. L., Richardson, R., Schultz, J., Myers West, S. i Whittaker, M. (2019). *AI Now 2019 Report*. Nowy Jork. Pozyskano z: https://ainowinstitute.org/AI_Now_2019_Report.html (16.10.2021).

Ebers, M., Hoch, V. R. S., Rosenkranz, F., Ruschemeier, H. i Steinrötter, B. (2021). The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS), *J, 4*(4), 589–603. https://doi.org/ 10.3390/j4040043.

European Union Agency for Fundamental Rights. (2020). *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, s. 7–8. Pozyskano z: https://op.europa.eu/en/publication-detail/-/publication/0de97f99-10db-11ea-8c1f-01aa75ed71a1/language-en.

EROD. (2020a). *Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo*. *Wersja 2.0.* European Data Protection Board. Pozyskano z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pl.pdf.

EROD (2020b). *Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679*. *Wersja 1.1.* European Data Protection Board. Pozyskano z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pl.

EROD, EIOD (2021). *EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. European Data Protection Supervisor. Pozyskano z: https://edps.europa.eu/node/7140_en.

Fajgielski, P. (2018). *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*. Warszawa: Wolters Kluwer.

Fourtané, S. (2020). *AI Facial Recognition and IP Surveillance for Smart Retail, Banking, and the Enterprise*. Pozyskano z: https://interestingengineering.com/ai-facial-recognition-and-ip-surveillance-for-smart-retail-banking-and-the-enterprise (15.10.2021).

Grupa Robocza Art. 29. (2003). *Working document on biometrics*. WP80. Pozyskano z: https://www.uodo.gov.pl/3.

Grupa Robocza Art. 29. (2007). *Opinia 4/2007 w sprawie pojęcia danych osobowych*, WP136. Pozyskano z: https://www.uodo.gov.pl/3.

Grupa Robocza Art. 29. (2012). *Opinion 3/2012 on developments in biometric technologies*, WP193. Pozyskano z: https://www.uodo.gov.pl/3.

Kind, C. (2021). *Containing the canary in the AI coalmine – the EU's efforts to regulate biometrics. Exploring the gaps and risks relating to biometrics in the EU's draft AI regulation*. Pozyskano z: https://www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics/ (18.10.2021).

Kuba, M. (2018). Artykuł 4 pkt 14. W: E. Bielak-Jomaa, D. Lubasz (red.), *RODO Ogólne rozporządzenie o ochronie danych Komentarz*, s. 273–277. Warszawa: Wolters Kluwer.

La Quadrature du Net. (2020). *Our legal action against the use of facial recognition by the French police*. Pozyskano z: https://www.laquadrature.net/en/2020/09/21/our-legal-action-against-the-use-of-facial-recognition-by-the-french-police/ (16.10.2021).

Leslie, D. (2020). *Understanding bias in facial recognition technologies*. The Alan Turing Institute.

Lynch, J. (2020). *Face Off: Law Enforcement Use of Face Recognition Technology*. Pozyskano z: https://www.eff.org/pl/wp/law-enforcement-use-face-recognition (17.10.2021).

PE. (2021). *Regulating facial recognition in the EU*. Bruksela: European Parliamentary Research Services.

Rada Europy. (2021). *Guidelines on facial recognition*. Pozyskano z: https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html.

Rapcewicz, A. (2020). Stosowanie mechanizmów rozpoznawania twarzy w świetle wytycznych Europejskiej Rady Ochrony Danych i stanowisk organów nadzorczych. *Magazyn ODO*, (12), 63–66.

Selvadurai, N. (2015). Not just a face in the crowd: addressing the intrusive potential of the online application of face recognition technologies. *International Journal of Law and Information Technology*, (23), 187–218. https://doi.org/10.1093/ijlit/eav006.

Thales Group. (2021). *Biometrics: definition, use cases and latest news*. Pozyskano z: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (15.10.2021).

Wang, M. i Deng, W. (2020). Deep Face Recognition: A Survey. *Neurocomputing,* 429, 215–244. https://doi.org/10.1016/j.neucom.2020.10.081.

Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, W., Richardson, R., Schultz, J., Myers West, S. i Schwartz, O. (2018). *AI Now Report 2018*. Nowy Jork. Pozyskano z: https://ainowinstitute.org /AI_Now_2018_Report.pdf (17.10.2021).