Katolicki Uniwersytet Lubelski Jana Pawła II
Wydział Prawa, Prawa Kanonicznego i Administracji
Instytut Nauk Prawnych

mgr Katarzyna Agnieszka Janczewska
Numer albumu 118617

Ochrona danych osobowych dziecka w związku ze świadczeniem usług społeczeństwa informacyjnego

Rozprawa doktorska przygotowana pod kierunkiem
dr hab. Pawła Fajgielskiego prof. KUL

Lublin 2023

SPIS TREŚCI

WYKAZ SKRÓTÓW

COPPA – *Children's Online Privacy Protection Act of 1998*, 15 U.S.C. 6501-6505

decyzja KE 2021/914 – decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (Dz. Urz. UE L 199 z dnia 07.06.2021, s. 31)

dyrektywa 2000/31 – dyrektywa 2000/31/WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego na rynku wewnętrznym (dyrektywa o handlu elektronicznym) (Dz. Urz. UE L 178 z dnia 17.07.2000 r., s. 1)

dyrektywa 2002/58 – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. UE L 201 z dnia z 31.07.2002 r., s. 37)

dyrektywa 2015/1535 – dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającą procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. Urz. UE L 241 z dnia 17.09.2015 r., s. 1)

dyrektywa 2016/680 – dyrektywa 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 uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, s. 89)

dyrektywa 95/46 – 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 dnia 23.11.1995 r., s. 31)

Dz. U. – Dziennik Ustaw

Dz. Urz. UE – Dziennik Urzędowy Unii Europejskiej

EIOD – Europejski Inspektor Ochrony Danych

ENISA – *European Union Agency for Cybersecurity*, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa

EROD – Europejska Rada Ochrony Danych

ETPCZ – Europejski Trybunał Praw Człowieka

GIODO – Generalny Inspektor Ochrony Danych Osobowych

ICO – *Information Commissioner's Office*, brytyjski organ nadzorczy ds. ochrony danych osobowych

IOD – Inspektor Ochrony Danych

IoT – *Internet of Things*, tzw. internet rzeczy

kc – ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz.U. z 2023 r. poz. 1610)

KE – Komisja Europejska

kk – ustawa z dnia 6 czerwca 1997 r. Kodeks karny (T.j. Dz.U. z 2022 r. poz. 1138 z późn. zm.)

komunikat KE z 2010 r. – Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów z dnia 04.11.2010 r. *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej*, KOM(2010) 609

komunikat Prezesa UODO – komunikat Prezesa UODO z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. z 2019 r. poz. 666)

Konstytucja – Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r., nr 78, poz. 483 ze zm.)

Konwencja 108 – Konwencja Rady Europy 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r., Dz. U. z 2003 r. nr 3, poz. 25

Konwencja 108+ – protokół zmieniający Konwencję 108 sporządzony 10.10.2018 r.

kpa – ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2023 r. poz. 775 ze zm.)

KPD – Konwencja o Prawach Dziecka przyjęta przez Zgromadzenie Ogólne ONZ dnia 20 listopada 1989 r. (Dz.U. z 1991 r., Nr 120, poz. 526)

Kpk – ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (T.j. Dz. U. z 2022 r. poz. 1375 z późn. zm.)

KPP – Karta Praw Podstawowych Unii Europejskiej, załącznik do Traktatu z Lizbony zmieniającego Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską z 13.12.2007 r. (Dz.U. z 2009 r., Nr 203, poz. 1569)

krio – ustawa z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy (T.j. Dz. U. z 2020 r. poz. 1359 z późn. zm.)

Legalis – System Informacji Prawnej Legalis

LEX – System Informacji Prawnej LEX

M. P. – Monitor Polski

NSA – Naczelny Sąd Administracyjny

ONZ – Organizacja Narodów Zjednoczonych

organizacja działająca na rzecz ochrony danych osobowych – podmiot, o którym mowa w art. 80 ust. 1 rozporządzenia 2016/679

ppsa – stawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (T.j. Dz. U. z 2023 r. poz. 259 z późn. zm.)

Prezes UODO – Prezes Urzędu Ochrony Danych Osobowych

rozporządzenie 2016/679 - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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 04.05.2016, s. 1)

rozporządzenie 2022/2065 - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz. Urz. UE L 277 z 27.10.2022, s. 1)

SN – Sąd Najwyższy

t.j. – tekst jednolity

TFUE - Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana Dz. Urz. UE C 326 z 26.10.2012, s. 47)

TK – Trybunał Konstytucyjny

TSUE – Trybunał Sprawiedliwości Unii Europejskiej

TUE – Traktat o Unii Europejskiej (wersja skonsolidowana Dz. Urz. UE C 326, 26.10.2012, s. 13)

UE – Unia Europejska

uodo z 1997 r. – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922)

uodo z 2018 r. - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (T.j. Dz. U. z 2019 r. poz. 1781)

upk – ustawa z dnia 30 maja 2014 r. o prawach konsumenta (T.j. Dz.U. z 2020 r. poz. 287 z późn. zm)

uRPD - ustawa z dnia 6 stycznia 2000 r. o Rzeczniku Praw Dziecka (T.j. Dz. U. z 2023 r., poz. 292)

upt - ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t. j. Dz.U. z 2022 r. poz. 1648 z późn. zm.)

ustawa o IPN – ustawa z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni Przeciwko Narodowi Polskiemu (T.j. Dz.U. z 2023 r. poz. 102)

uśude - ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t. j. Dz. U. z 2020 r. poz. 344)

wniosek KE z 2012 r. – wniosek Komisji Europejskiej z dnia 25 stycznia 2012 r. „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)", COM/2012/011 final

WSA – Wojewódzki Sąd Administracyjny

WSTĘP

Dzieci są aktywnymi uczestnikami społeczeństwa informacyjnego, którego funkcjonowanie ściśle wiąże się z przetwarzaniem danych osobowych. Rozwój usług społeczeństwa informacyjnego – przejawiający się przede wszystkim w dużej popularności portali społecznościowych, usług świadczonych drogą elektroniczną i stosowaniem nowych technik przetwarzania danych – może rodzić negatywne konsekwencje dla dzieci z powodu naruszeń w obszarze ochrony danych osobowych. Obowiązujące w Polsce oraz Unii Europejskiej do 25 maja 2018 r. przepisy o ochronie danych osobowych nie przewidywały żadnych szczególnych rozwiązań w zakresie ochrony danych osobowych dzieci. Ten stan uległ zmianie w wyniku reformy ochrony danych osobowych i wejścia w życie Rozporządzenia 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), dalej jako „rozporządzenie 2016/679".

Konieczność objęcia dzieci szczególną ochroną, mniej świadomych potencjalnych zagrożeń, była akcentowana na etapie prac nad reformą ochrony danych osobowych. Ogólne rozporządzenie o ochronie danych wprowadziło nieznane wcześniej rozwiązania w zakresie przetwarzania danych osobowych dzieci. Budzą one jednak liczne wątpliwości interpretacyjne, zakreślając szerokie pole do prac badawczych. Istotnym *novum* wprowadzonym przez reformę jest regulacja dotycząca zgody dziecka na przetwarzanie jego danych osobowych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dzieciom, choć należy podkreślić, że analiza art. 8 ust. 1 rozporządzenia 2016/679 nie wyczerpywałaby problematyki ochrony danych osobowych w odniesieniu wyżej wskazanych usług.

Motywacją do podjęcia tematu rozprawy doktorskiej jest chęć wnikliwej analizy przepisów o ochronie danych osobowych pod kątem problematyki przetwarzania danych dziecka w szczególnym kontekście – świadczenia usług społeczeństwa informacyjnego. Ujmując zwięźle, zakres danych przetwarzanych przez usługodawców przeważnie wykracza poza to, co podał sam użytkownik. Dla zilustrowania problemu wskazać można problem przetwarzania danych geolokalizacyjnych i profilowania, a w konsekwencji wyciągania wniosków na temat cech lub preferencji użytkownika, czego może on nie być świadomy. Problematyka ochrony danych osobowych dziecka jest tematem rzadko poruszanym w literaturze, choć od niedawna można zaobserwować wzrost zainteresowania nią. Niemniej dotychczas opublikowane prace traktują o stosunkowo wąskich, wybranych zagadnieniach – przykładowo dotyczą pozyskania zgody na

przetwarzanie danych osobowych. Dostępne są obszerniejsze opracowania poruszające problematykę zbierania danych osobowych dziecka przez placówki oświatowe. Brakuje jednak kompleksowego opracowania poświęconego zagadnieniu przetwarzania danych osobowych dziecka w związku ze świadczeniem usług społeczeństwa informacyjnego o charakterze komercyjnym, zaś niniejsza rozprawa ma szansę tę lukę uzupełnić. Elementy nowatorskie przejawiają się w poddaniu analizie i interpretacji pojęcia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, przesłanek legalności przetwarzania danych osobowych w tym kontekście, uprawnień przysługujących dziecku oraz obowiązków podmiotów uczestniczących w przetwarzaniu – ze szczególnym naciskiem na obowiązek proaktywnego i odpowiedzialnego podejścia do ochrony danych osobowych dzieci, oceny nowych przepisów pod kątem realizacji ich celu, tj. wzmocnienia praw dziecka i skuteczności mechanizmów ich ochrony.

Tezą dysertacji jest założenie, że regulacja przetwarzania danych osobowych dziecka w rozporządzeniu 2016/679 jest fragmentaryczna, zbyt ogólna i rodzi liczne wątpliwości interpretacyjne, a w konsekwencji reforma ochrony danych osobowych nie realizuje w pełni jednego z jej założeń, jakim jest wzmocnienie ochrony danych osobowych dziecka w związku ze świadczeniem usług społeczeństwa informacyjnego. Natomiast jako cele badawcze wskazać należy: 1) dążenie do wykazania, że wzmocnienie ochrony danych dziecka było jednym z założeń reformy; 2) przedstawienie rozwiązań, dzięki którym to założenie miało zostać zrealizowane; 3) przeprowadzenie analizy rozwiązań prawnych mających służyć ochronie danych osobowych dziecka; 4) przedstawienie wniosków z analizy wprowadzonych rozwiązań oraz propozycji zmian, które mogą przyczynić się do wzmocnienia ochrony danych osobowych dziecka.

Podstawową metodę badawczą będzie stanowić metoda formalno-dogmatyczna. Do kluczowych źródeł o charakterze normatywnym, które zostaną poddane analizie, zaliczyć należy przede wszystkim rozporządzenie 2016/679, a także Konstytucję Rzeczypospolitej Polskiej, Kartę Praw Dziecka, Kartę Praw Podstawowych Unii Europejskiej oraz przepisy sektorowe, np. unijny Akt o usługach cyfrowych. Szczególne znaczenie ma także ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, gdyż przedmiotowym zakresem obejmuje m.in. postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych.

Pomocniczo wykorzystana będzie metoda historyczna, co jest uzasadnione okolicznością, że wprowadzenie rozporządzenia 2016/679 stanowi rezultat reformy ochrony danych osobowych, która choć nie jest rewolucyjna – podstawowe instytucje nie uległy bowiem radykalnym zmianom – niesie ze sobą nowe, nieznane rozwiązania. Powoduje to konieczność korzystania z dorobku orzecznictwa i doktryny z okresu poprzedzającego reformę, a jednocześnie jest nieodzowne do podjęcia próby oceny, czy przyświecające reformie cele wzmocnienia praw dzieci – osób, których dane dotyczą (podmiotów danych), zostały zrealizowane. W tym celu jako źródła posłużą przede

wszystkim nieobowiązujące już 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 oraz ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Również na zasadzie subsydiarności zastosowana zostanie metoda komparatystyczna, co będzie polegało na porównaniu rozwiązań przyjętych w rozporządzeniu 2016/679 w zakresie objętym przedmiotem dysertacji z regulacjami zawartymi w obowiązującym w Stanach Zjednoczonych akcie prawnym *Children's Online Privacy Act of 1998* (COPPA). Wybór ten podyktowany jest okolicznością, że COPPA został przyjęty kilkanaście lat przed unijną reformą ochrony danych osobowych i analiza rozwiązań przewidzianych w rozporządzeniu 2016/679 pozwala przypuszczać, że stanowił istotną inspirację. Ponadto nie można pominąć, że technologie informacyjno-komunikacyjne i społeczeństwo informacyjne – czy szerzej gospodarka cyfrowa – rozwijały się w latach 90. XX w. w Stanach Zjednoczonych bardzo dynamicznie. Są one także kolebką popularnych usług społeczeństwa informacyjnego – największych portali społecznościowych, co pozwala przypuszczać, że z wyrastającymi na tym polu problemami amerykański prawodawca musiał zmierzyć się wcześniej, przez co warto przyjrzeć się tym doświadczeniom i rozwiązaniom legislacyjnym. Wreszcie zauważyć trzeba, że zakres przedmiotowy COPPA, jak i niektórych przepisów rozporządzenia 2016/679 jest bardzo zbliżony, co tym bardziej uzasadnia porównanie obydwu regulacji.

Metoda historyczna i komparatystyczna będą uzupełniać zastosowanie metody formalno-dogmatycznej. Nieodzowne będzie wykorzystanie dorobu doktryny, orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej, który dokonywał wykładni unijnych przepisów w dziedzinie ochrony danych osobowych, orzecznictwa sądów administracyjnych, decyzji Prezesa Urzędu Ochrony Danych Osobowych i organów nadzorczych ds. ochrony danych osobowych ustanowionych w innych państwach członkowskich Unii Europejskiej. Nie sposób pominąć także źródeł o charakterze niewiążącym, lecz wyznaczających kierunki interpretacji, takich jak wytyczne unijnych organów nadzorczych ds. ochrony danych osobowych skupionych w Europejskiej Radzie Ochrony Danych (wcześniej Grupie Roboczej Art. 29), materiały informacyjne opublikowane przez Prezesa Urzędu Ochrony Danych Osobowych. Na szczególną uwagę, ze względu na rozwinięcie kwestii ochrony danych osobowych dzieci, zasługują wybrane opracowania organów nadzorczych: irlandzkiego, brytyjskiego (powstałe na kanwie rozporządzenia 2016/679) i francuskiego. Dzięki bezpośredniemu stosowaniu rozporządzenia 2016/679 we wszystkich państwach członkowskich Unii Europejskiej i obowiązkowi dążenia do jednolitego stosowania jego przepisów, zasadne jest posiłkowanie się zawartymi w nich wskazówkami interpretacyjnymi w niniejszej rozprawie.

Dysertacja składa się ze wstępu, pięciu rozdziałów merytorycznych oraz zakończenia. Pierwszy rozdział poświęcony jest zagadnieniom wprowadzającym. Zostanie w nim przedstawiona geneza prawnych regulacji służących ochronie praw osób fizycznych w związku z przetwarzaniem dotyczących ich danych osobowych, powszechnie określana ochroną danych osobowych, a także syntetycznie zostaną scharakteryzowane kluczowe akty prawne obowiązujące przed reformą. Następnie omówione zostaną założenia i cele reformy związane z ochroną praw dzieci i dostrzeżeniem potrzeby ich wzmocnienia z powodu gwałtownego rozwoju nowych technik przetwarzania danych osobowych. Będzie to stanowiło grunt do dalszych rozważań na temat rozwiązań przyjętych w rozporządzenia 2016/679 w wyniku reformy. W rozdziale pierwszym zostaną poddane analizie kluczowe pojęcia, które będą wykorzystywane następnie w całej dysertacji.

W rozdziale drugim, po określeniu kręgu podmiotów, które są adresatami obowiązków przewidzianych w rozporządzeniu 2016/679, przedstawione zostaną naczelne zasady ochrony danych osobowych określone w art. 5 ust. 1 rozporządzenia 2016/679: zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu przetwarzania, minimalizacji danych, prawidłowości danych, ograniczenia przechowywania danych, zachowania integralności oraz poufności danych. W ramach rozwinięcia problematyki przestrzegania zasady zgodności z prawem, zostaną przedstawione i omówione podstawy prawne przetwarzania danych osobowych, w tym nowe, nieznane wcześniej w prawie polskim i prawie Unii Europejskiej rozwiązania dotyczące zgody na przetwarzanie danych osobowych dziecka, związanej ze świadczeniem usług społeczeństwa informacyjnego. Rozważania będą także dotyczyć możliwości zastosowania pozostałych przesłanek legalizujących przetwarzanie, w tym budzącej kontrowersje przesłanki przetwarzania do celów wynikających z prawnie uzasadnionych interesów (por. art. 6 ust. 1 lit. f rozporządzenia 2016/679).

Rozdział trzeci traktuje o uprawnieniach, jakie przysługują dziecku na podstawie art. 15-22 rozporządzenia 2016/679. Koncentrując się na specyfice świadczenia usług społeczeństwa informacyjnego, przedstawione zostaną funkcje poszczególnych uprawnień oraz pozytywne i negatywne przesłanki ich realizacji. W rozdziale trzecim zostanie ponadto poruszony problem sposobu wykonywania tych uprawnień, gdyż niezbędne jest analiza ważkiego problemu czy – i w jakim zakresie – dziecko może samodzielnie korzystać z przysługujących mu środków, mając na uwadze, że nierzadko jest ono nastolatkiem korzystającym samodzielnie z usług społeczeństwa informacyjnego.

Rozdział czwarty poświęcony będzie obowiązkom związanym z przetwarzaniem danych osobowych dziecka. Przedmiotem rozważań będą więc powinności odnoszące się do wdrożenia adekwatnych do zagrożeń technicznych i organizacyjnych środków bezpieczeństwa, co zgodnie z

przewodnim na gruncie rozporządzenia 2016/679 podejściem opartym na ryzyku, powinno być poprzedzone stosowną analizą, a niekiedy dodatkowo oceną skutków dla ochrony danych. Omówione zostaną również obowiązki polegające na konieczności uwzględniania ochrony danych osobowych w fazie projektowania (planowania) i w trakcie prowadzenia operacji przetwarzania oraz przestrzegania zasady domyślnej ochrony danych. Ponadto w tym rozdziale zostaną poruszone ważkie zagadnienia związane z naruszeniem ochrony danych osobowych w rozumieniu art. 4 pkt 12 rozporządzenia 2016/679 oraz wynikających z niego obowiązków. Rozdział czwarty zwieńczy omówienie znaczenia zasady rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679) i przejawów jej przestrzegania.

Ostatni, piąty rozdział, dotyczy odpowiedzialności za naruszenia związane z przetwarzaniem danych osobowych dziecka w związku ze świadczeniem usług społeczeństwa informacyjnego. Ochrona danych osobowych pozostałyby w sferze postulatów, gdyby nie istniały skuteczne środki ochrony prawnej. Celem reformy było wzmocnienie egzekwowania przestrzegania przepisów o ochronie danych osobowych, dlatego w dysertacji omówiona będzie odpowiedzialność administracyjna, łącznie z kwestią nakładania administracyjnych kar pieniężnych. Przedstawione zostaną kompetencje Prezesa Urzędu Ochrony Danych Osobowych, do których zaliczyć należy m.in. upowszechnianie wiedzy o prawach związanych z przetwarzaniem i poświęcanie szczególnej uwagi działaniom skierowanym do dzieci (por. art. 57 ust. 1 lit. b rozporządzenia 2016/679). Analizie poddane zostaną proceduralne aspekty korzystania ze środków ochrony prawnej przez dziecko, w tym wnoszenia skargi do Prezesa Urzędu Ochrony Danych Osobowych. Nadto rozważaniom zostanie poddana problematyka odpowiedzialności cywilnej i karnej za naruszenia w obszarze ochrony danych osobowych – zostanie podjęta próba oceny adekwatności istnienia trzech reżimów odpowiedzialności w kontekście naruszeń związanych z przetwarzaniem danych osobowych dzieci w związku ze świadczeniem usług społeczeństwa informacyjnego.

W rozprawie uwzględniono stan prawny na dzień 1 września 2023 r.

ROZDZIAŁ I
ZAGADNIENIA WPROWADZAJĄCE

1. Geneza i rozwój prawa ochrony danych osobowych

Prawo do ochrony danych osobowych wywodzi się z szerszej koncepcji prawa do prywatności – której pierwszy zarys przedstawili w 1890 r. Samuel D. Warren i Louis D. Brandeis w artykule zatytułowanym *The right to privacy*[1]. Potrzebę objęcia prawną ochroną prywatnej sfery życia człowieka upatrywali w zagrożeniach, jakie niesie ze sobą postęp cywilizacyjny – zwiększenie intensywności życia, nowe wynalazki, reklama, rozwój prasy – co sprawia, że człowiek bardziej docenia odosobnienie. Naruszenie prywatności – jak piszą autorzy – może powodować psychiczne cierpienie, gdy nierzetelne lub wręcz szkalujące informacje o osobie są rozpowszechniane na szeroką skalę, zwłaszcza, gdy wykorzystywane są nowe urządzenia umożliwiające obróbkę czy reprodukcję dźwięków i obrazów. Samuel D. Warren i Louis D. Brandeis trafnie zidentyfikowali ryzyko związane z wykorzystaniem informacji o człowieku i słusznie stwierdzili, że znane wówczas prawu mechanizmy ochrony nie są adekwatne do charakteru naruszeń w sferze prywatności. W XX w. ochrona prawa do prywatności, a następnie także prawa do ochrony danych osobowych, została wprowadzona w prawie międzynarodowym, a także prawie poszczególnych państw[2].

Ochronę prywatności przewiduje szereg instrumentów, choć na płaszczyźnie prawa międzynarodowego wiele z nich ma charakter niewiążący – stanowi tzw. *soft law*, jak np. Powszechna Deklaracja Praw Człowieka przyjęta w 1948 r. przez Zgromadzenie Ogólne ONZ[3]. Przewiduje ona w art. 12 wolność od ingerencji w życie prywatne, rodzinne, domowe, korespondencję; ustanawia zakaz uwłaczania honorowi lub dobremu imieniu innej osoby, a także prawo do ochrony prawnej przeciwko takim działaniom. Podobne rozumienie prawa do prywatności przyjęto w systemie ochrony Rady Europy i pierwszej wiążącej umowie międzynarodowej odnoszącej się do omawianej problematyki – Konwencji o ochronie praw człowieka i podstawowych wolności z dnia 4 listopada 1950 r.[4], której art. 8 stanowi, że każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej

[1] S. D. Warren, L. D. Brandeis, *The right to privacy,* "Harvard Law Review" 1890, vol. IV, s. 193-220.
[2] Pierwsze regulacje w tym zakresie zostały wprowadzone w latach 70. XX w. w Hesji (niemieckim kraju związkowym) i Szwecji – M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010, s. 10.
[3] Powszechna Deklaracja Praw Człowieka przyjęta w Paryżu dnia 10.12.1948 r., http://libr.sejm.gov.pl/tek01/txt/onz/1948.html (dostęp: 23.09.2020).
[4] Dz. U. z 1993 r. Nr 61, poz. 284.

korespondencji. Europejski Trybunał Praw Człowieka uznaje w swoim orzecznictwie, że ochrona przewidziana w art. 8 obejmuje także ochronę danych osobowych[5]. Prawo do prywatności i prawo do ochrony danych osobowych, mimo, że mają podobną podbudowę aksjologiczną, nie są jednak tożsame. Rozwój koncepcji ochrony danych osobowych nastąpił w wyniku pojawienia się i coraz powszechniejszego wykorzystania technologii informacyjno-komunikacyjnych, przede wszystkim internetu, pozwalających na szybki przepływ informacji. Dzięki internetowi przesyłanie nawet dużych wolumenów danych z upływem czasu stawało się coraz łatwiejsze, co więcej, nie napotykało barier w postaci granic państwowych. Dlatego w 1981 r. Rada Europy przyjęła Konwencję 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[6]. Jej cel został określony w art. 1, zgodnie z którym jest nim zapewnienie każdej osobie fizycznej, bez względu na narodowość lub miejsce zamieszkania, poszanowania jej praw i podstawowych wolności na terytorium każdej ze stron konwencji, a w szczególności jej prawa do prywatności w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych („ochrona danych"). Ochrona danych jest więc, na gruncie konwencji 108, ściśle powiązana z automatycznym przetwarzaniem danych osobowych, które zostało zdefiniowane w art. 2 lit. c i oznacza operacje wykonane w całości lub częściowo za pomocą procedur zautomatyzowanych: gromadzenie danych, stosowanie do nich operacji logicznych i/lub arytmetycznych, ich modyfikowanie, usuwanie, wybieranie lub rozpowszechnianie. Natomiast dane osobowe zdefiniowano jako każdą informację dotyczą osoby fizycznej o określonej tożsamości lub dającej się zidentyfikować. Konwencja 108 ustanawia m.in. zasady ochrony danych osobowych (art. 5), dodatkowe warunki przy przetwarzaniu szczególnych kategorii danych (art. 6), obowiązek podjęcia odpowiednich środków bezpieczeństwa w odniesieniu do danych osobowych zgromadzonych w zbiorach zautomatyzowanych (art. 7), uprawnienia osób, których dane dotyczą (art. 8), a także zasady przepływu danych przez granice (art. 12).

Konwencja 108 jest pierwszym międzynarodowym instrumentem ochrony danych osobowych, w dodatku jedyną prawnie wiążącą umową międzynarodową w tej dziedzinie. Ponadto przystępują do niej państwa także spoza Europy, np. Meksyk, Argentyna, Senegal[7]. W związku z nowymi problemami, jakie niesie ze sobą rozwój technologii informacyjno-komunikacyjnych, a także potrzebą zapewnienie efektywnego wdrażania postanowień Konwencji,

[5] Wyrok ETPCZ z dnia 16.02.2000 r., 27798/95, Amann v. Szwajcaria; wyrok ETPCZ z dnia 03.04.2007 r., 62617/00, Copland v. Wielka Brytania; wyrok ETPCZ z dnia 02.09.2010 r., 35623/05, Uzun v. Niemcy; orzeczenia są dostępne w bazie HUDOC (https://hudoc.echr.coe.int, dostęp: 09.09.2020).
[6] Dz. U. z 2003 r. Nr 3, poz. 25, dalej jako: konwencja 108.
[7] Informacja o stronach konwencji 108, a także państwach, które planują do niej przystąpić, dostępna jest na stronie https://www.coe.int/en/web/data-protection/convention108/parties (dostęp: 23.09.2020).

uznano, że wymaga modernizacji[8], dlatego przygotowano protokół zmieniający konwencję – tzw. Konwencję 108+[9]. Obecnie trwa proces jego ratyfikacji[10].

Oprócz przyjęcia konwencji 108, aktywność Rady Europy w obszarze ochrony danych osobowych uzupełniają liczne rekomendacje Komitetu Stałego Ministrów adresowane do państw-stron[11]. Traktują one o ochronie danych osobowych w różnych dziedzinach, co świadczy o tym, że przy projektowaniu i wdrażaniu skutecznych mechanizmów ochrony niezbędne jest uwzględnianie specyfiki przetwarzania w danym sektorze – charakterystycznych dla niego uwarunkowań i problemów.

Dorobek Rady Europy, w tym orzecznictwo ETPCZ, stanowi ogromny wkład w rozwój ochrony danych osobowych. Niektórzy podnoszą, że zmodernizowana konwencja 108 ma szansę stać się uniwersalnym instrumentem ochrony danych osobowych[12]. Jednak pewną przeszkodą w osiągnięciu takiego stanu jest to, że nie konwencja 108 nie jest stosowana bezpośrednio – adresatami zawartych niej w norm są państwa-strony[13] – to na nie został nałożony obowiązek przyjęcia w prawie krajowym rozwiązań, które doprowadzą do osiągnięcia pożądanego standardu ochrony, i to od ich działań będzie zależało, czy i w jakim stopniu uda się to zrealizować.

Konwencja 108 była inspiracją dla stworzenia mechanizmu ochrony danych osobowych w Unii Europejskiej – przyjęcia dyrektywy 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[14], co podkreślono w motywie 11 jej preambuły. Przyjęcie wspólnych zasad ochrony danych osobowych w UE związane było z ustanowieniem rynku wewnętrznego i funkcjonujących w jego ramach swobód przepływu towarów, osób, usług i kapitału, z którym powiązany jest przepływ danych osobowych[15]. Zróżnicowany poziom ochrony danych osobowych w państwach członkowskich został uznany za czynnik zwiększający

[8] U. Góral, S. Kwasny, *Proces modernizacji Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych*, „Monitor Prawniczy" dodatek: *Aktualne problemy prawnej ochrony danych osobowych 2014*, G. Sibiga (red.), 2014, nr 9, s. 58.

[9] *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* Strasbourg, 10.10.2018 r. (https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016808ac918, dostęp: 07.09.2020).

[10] Polska ratyfikowała protokół 10.06.2020 r., ale nie wszedł jeszcze w życie ze względu na brak wymaganej liczby ratyfikacji.

[11] Wykaz rekomendacji, a także ich treść, jest dostępna na stronie https://www.coe.int/en/web/data-protection/legal-instruments (dostęp: 07.09.2020).

[12] M. Ciechomska, *Zmiana Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych szansą na powstanie globalnego instrumentu ochrony danych*, „Monitor Prawniczy" dodatek: *Wdrażanie ogólnego rozporządzenia o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2017*, Sibiga G. (red.), 2017, nr 16, s. 876.

[13] A. Mednis, *Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej*, „Państwo i Prawo" 1997, nr 6, s. 31.

[14] Dz. Urz. UE L 281 z dnia 23.11.1995 r., s. 31-50, dalej jako: dyrektywa 95/46.

[15] Por. motyw 3 preambuły dyrektywy 95/46.

ryzyko wystąpienia utrudnienia realizacji przedsięwzięć ekonomicznych, zakłócenia konkurencji, a także wywiązania się przez państwa członkowskie z ich obowiązków[16].

W dyrektywie 95/46 uregulowano kilka ogólnych zasad przetwarzania danych osobowych (art. 6), wynikających z nich obowiązków, w tym dotyczących zabezpieczenia danych osobowych (art. 17) oraz skorelowanych z nimi uprawnień osób fizycznych (art. 10-12, 14-15). Dyrektywa 95/46 przewidywała obowiązek ustanowienia w państwach członkowskich organów nadzorczych, odpowiedzialnych za kontrolę przestrzegania przepisów przyjętych w celu jej wdrożenia. Na administratorach – czyli podmiotach decydujących o sposobach i celach przetwarzania, zobowiązanych do przetwarzania danych osobowych zgodnie z zasadami ich ochrony – ciążył obowiązek zawiadomienia organu nadzorczego o planowanej całościowej lub częściowej operacji automatycznego przetwarzania danych lub zestawu takich operacji mających służyć jednemu celowi lub wielu powiązanym ze sobą celom (por. art. 18 ust. 1 dyrektywy 95/45). Organ nadzorczy realizował w ten sposób kontrolę uprzednią[17]. Przysługiwały mu także inne uprawnienia o charakterze kontrolnym oraz kompetencje, dzięki którym mógł nakazać działania mające na celu wyeliminowanie nieprawidłowości związanych z przetwarzaniem danych osobowych i przywrócenie zgodności z prawem (por. art. 28 dyrektywy 95/46).

Na mocy dyrektywy 95/46 została ponadto powołana Grupa Robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, w skład której wchodzą przedstawiciele organów nadzorczych powołanych przez państwa członkowskie, przedstawiciel organu właściwego do spraw ochrony danych osobowych przez unijne instytucje oraz przedstawiciel Komisji Europejskiej. Do zadań tej grupy, nazywanej Grupą Roboczą Art. 29, należało przede wszystkim przyczynianie się do jednolitego stosowania przepisów o ochronie danych osobowych w Unii Europejskiej, doradzanie Komisji Europejskiej w przypadku zamiaru wprowadzenia zmian w dyrektywie 95/46, formułowanie zaleceń we wszystkich sprawach dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych (art. 30). Wytyczne Grupy Roboczej Art. 29 stanowią istotny wkład w sposób stosowania i rozumienia przepisów dyrektywy 95/46. W dużej mierze omówione w nich zagadnienia konstrukcyjne, dotyczące podstawowych instytucji ochrony danych osobowych, pozostały aktualne także po uchyleniu dyrektywy 95/46, dlatego zasadne jest posiłkowanie się nimi także przy interpretacji przepisów wprowadzonych w wyniku reformy ochrony danych osobowych. Niektóre wytyczne Grupa Robocza Art. 29 przygotowała już na

[16] Por. motyw 7 preambuły dyrektywy 95/46.
[17] W Polsce, ze względu na przyjęte rozwiązania, kontrola ta miała w określonych przypadkach charakter kontroli uprzedniej i faktycznej – por. P. Fajgielski, *Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno-prawne*, Lublin 2008, s. 245.

podstawie nowych przepisów, w okresie poprzedzającym rozpoczęcie ich stosowania, np. w 2017 r. opublikowała wytyczne dotyczące zasady przejrzystości[18].

Powierzenie Grupie Roboczej Art. 29 zadań mających na celu zapewnienie jednolitego stosowania przepisów o ochronie danych osobowych było istotne ze względu na charakter dyrektywy. Dyrektywa jest bowiem aktem, który wymaga wdrożenia (implementacji) do krajowego porządku prawnego każdego z państw członkowskich, poprzez przyjęcie przez nie aktów prawnych, których zadaniem jest realizacja celów wyznaczonych przez dyrektywę. Innymi słowy dyrektywa zobowiązuje państwa do wdrożenia określonych w niej założeń, w taki sposób, by zapewnić jej pełną skuteczność, jednak nie determinuje konkretnych służących temu środków. Dyrektywa jest więc skierowana do państw członkowskich i co do zasady nie wywołuje skutku bezpośredniego – czyli, poza pewnymi wyjątkami[19], nie może na nią bezpośrednio powołać się obywatel państwa członkowskiego. Dyrektywa ma więc prowadzić do harmonizacji prawa państw członkowskich w określonym zakresie (zbliżenia ustawodawstw), lecz nie ujednolica prawa całkowicie. Konsekwencją przyjęcia dyrektywy 95/46 było wprowadzenie w każdym państwie członkowskim odrębnych regulacji poświęconych problematyce ochrony danych osobowych. Mimo, że wszystkie miały na celu wdrożyć dyrektywę 95/46, nie udało się uniknąć różnic między rozwiązaniami przyjętymi w poszczególnych państwach członkowskich.

Prawo do ochrony danych osobowych gwarantuje ponadto Karta Praw Podstawowych UE[20], która została przyjęta w 2000 r., a w związku z reformą Unii Europejskiej – wraz z wejściem w życie Traktatu z Lizbony[21] z dniem 1 grudnia 2009 r. – uzyskała moc prawną, stając się częścią pierwotnego prawa UE[22]. Przepis art. 8 ust. 1 KPP stanowi, że każdy ma prawo do ochrony danych osobowych, które go dotyczą. Kolejne dwa ustępy ustanawiają kluczowe gwarancje, które mają urzeczywistniać prawo do ochrony danych osobowych: dane osobowe muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą, a każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania; przestrzeganie tych zasad podlega kontroli niezależnego organu. Przepis art. 8 ust. 1 KPP jest wyraźnie wzorowany na podstawowych zasadach ochrony danych osobowych ustanowionych w dyrektywie 95/46, w pewnym zakresie

[18] Grupa Robocza Art. 29, *Guidelines on Transparency under Regulation 2016/679 adopted on 29 November 2017,* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (dostęp: 23.09.2020).
[19] Wyjątki ukształtowało orzecznictwo TSUE – wyrok z dnia 04.12.1974 r. w sprawie 41/74; wyrok z dnia 19.01.1982 r. w sprawie 8/81; por. J. Osiejewicz, *Harmonizacja prawa państw członkowskich Unii Europejskiej*, Warszawa 2016, Legalis.
[20] Karta Praw Podstawowych UE – załącznik do Traktatu z Lizbony zmieniającego Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską z 13.12.2007 r., Dz.U. z 2009 r., Nr 203, poz. 1569, dalej jako: KPP.
[21] Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie dnia 13 grudnia 2007 r., Dz. Urz. UE C 306 z 17.12.2007 r., s. 1—27.
[22] Por. A. Wróbel, *Wprowadzenie do komentarza do KPP*, [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, wyd. 2, Warszawa 2020, s. 2.

jest także zbliżony do regulacji zawartych w konwencji 108[23]. Warto zauważyć, że o prawie do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się traktuje inny przepis KPP – mianowicie art. 7.

2. Ochrona danych osobowych w Konstytucji

W Polsce przed przyjęciem pierwszych regulacji prawnych odnoszących się bezpośrednio do ochrony danych osobowych prywatność – jako dobro osobiste[24] – mogła być chroniona w sposób przewidziany w art. 23 i 24 ustawy z dnia 23 kwietnia 1964 r. kodeks cywilny[25]. Zdaniem A. Kopffa, który opowiadał się za ochroną prywatności jako dobra osobistego, stanowi ona „to wszystko, co ze względu na uzasadnione odosobnienie się jednostki od ogółu społeczeństwa służy jej do rozwoju fizycznej i psychicznej osobowości oraz zachowania osiągniętej pozycji społecznej"[26]. Ochrona prywatności realizowana w ramach ochrony dóbr osobistych okazała się jednak niewystarczająca[27], ponieważ zasadniczo nie ma charakteru prewencyjnego – nie pozwala skutecznie zapobiegać zagrożeniom występującym w tym obszarze[28].

Przełomowe dla ochrony danych osobowych w Polsce było uchwalenie Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.[29] Wprawdzie Konstytucja nie posługuje się pojęciem danych osobowych, nie ulega wątpliwości, że art. 51 odnosi się właśnie do tego zagadnienia i wprowadza „nową kategorię prawa jednostki do ochrony danych osobowych"[30]. Przepis art. 51 ust. 1 Konstytucji stanowi, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby, a władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Przepis art. 51 ust. 2 i 3 Konstytucji określają natomiast uprawnienia, jakie przysługują każdemu w związku z pozyskaniem informacji na jego temat[31].

---

[23] G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Bruksela 2014, s. 204.

[24] Por. Wyrok SN z dnia 18.01.1984 r., sygn. akt I CR 400/83, LEX. Warto zauważyć, że w tym orzeczeniu SN posłużył się także pojęciem danych osobowych: „>>Anonimowość<< reportażu jest kwestią względną. Dane osobowe, profesjonalne i środowiskowe przestają być anonimowe wówczas, gdy dla osób, wśród których żyje konkretna jednostka, nie ulega wątpliwości, o kogo chodzi".

[25] T.j. Dz. U. z 2023 r. poz. 1610, dalej jako: kc.

[26] A. Kopff, *Koncepcja praw do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne)*, „Studia Cywilistyczne" 1972, t. 20, s. 32 n., 37, cytat za J. Barta, R. Markiewicz, *Prawo do prywatności w społeczeństwie informatycznym*, „Ethos" 1999, nr 1/2 (45/46), s. 368.

[27] Por. M. Safjan, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym,* „Państwo i Prawo" 2002, nr 6, s. 7.

[28] Por. P. Fajgielski, *Kontrola przetwarzania i ochrony…*, s. 30.

[29] Dz. U. z 1997 r., Nr 78, poz. 483 ze zm., dalej jako Konstytucja.

[30] Wyrok TK z dnia 19.05.1998 r., sygn. akt U 5/97, Dz.U. z 1998 r. Nr 67 poz. 444.

[31] Początkowo projektowany art. 51 nie zawierał tych gwarancji – o ich dodanie skutecznie zabiegała I. Lipowicz – M. Wild, *Komentarz do art. 51 Konstytucji*, [w:] M. Safjan, L. Bosek, *Konstytucja RP. Tom I. Komentarz do art. 1–86*, Warszawa 2016, Legalis.

Uprawnienia te obejmują prawo dostępu do urzędowych dokumentów i zbiorów danych (z zastrzeżeniem ograniczeń określonych w ustawie), prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. Zgodnie z ust. 5, zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa. Przepis art. 51 Konstytucji, kreując treść prawa do ochrony danych osobowych, wskazuje podmioty uprawnione i podmioty zobowiązane, ustanawia gwarancje o kardynalnym znaczeniu dla ochrony osoby fizycznej – podmiotowe prawo do ochrony danych osobowych[32]. Warto podkreślić, że w świetle art. 51 Konstytucji obowiązek ujawnienia informacji o sobie może być wprowadzony jedynie ustawą, a nie aktem niższego rzędu. Ponadto wprowadza on ograniczenie dla władz publicznych w zakresie pozyskiwania danych o obywatelach, wyznaczając w ten sposób kluczową zasadę – zakaz zbierania informacji innych niż niezbędne w demokratycznym państwie prawnym – co miało fundamentalne znaczenie w procesie demokratyzacji Polski, ograniczenia swobody gromadzenia „wielkich zbiorów danych o obywatelach"[33]. Zdaniem I. Lipowicz, przez dane niezbędne w demokratycznym państwie prawnym powinno się rozumieć „dane, bez których funkcjonowanie państwa byłoby niemożliwe lub znacznie utrudnione"[34]. Wreszcie Konstytucja gwarantuje każdemu, w razie zaistnienia nieprawidłowości dotyczących informacji o nim – co może mieć wpływ na różne sfery życia i nieść niekiedy bardzo poważne konsekwencje – podstawowe prawa, dzięki którym może żądać zaprzestania tych naruszeń.

Konstytucja w odrębnej jednostce redakcyjnej, art. 47, traktuje o prawie do prywatności, stanowiąc, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. W literaturze podkreśla się, że art. 47 powinien być traktowany jako kontekst interpretacyjny w stosunku do art. 51, ze względu na to, że obydwa przepisy chronią tę samą wartość[35]. Podobne stanowisko prezentuje I. Lipowicz twierdząc, że prawo do ochrony danych osobowych może być postrzegane jako „wyspecjalizowana konstrukcja" w stosunku do art. 47 i odnosząc się do orzecznictwa TK oraz koncepcji autonomii informacyjnej jednostki[36]. Jest to zasada wywodząca się z orzecznictwa niemieckiego Federalnego Trybunału Konstytucyjnego, zgodnie z którą jednostka ma prawo do samodzielnego decydowania o zakresie ujawnianych informacji o niej i sposobie ich

[32] K. Buczma, *Konstytucyjne podstawy prawa do ochrony danych osobowych*, [w:] J. Misztal-Konecka, G. Tylec (red.), *Wizja europejskiego społeczeństwa informacyjnego i jej realizacji w prawie polskim*, Lublin 2012, s. 45.
[33] G. Szpor, *Kierunki zmian w ustawodawstwie dotyczącym ochrony danych osobowych*, [w:] A. Mednis (red.), *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, Warszawa 2013, s. 54.
[34] I. Lipowicz, *Konstytucyjne podstawy ochrony danych osobowych*, [w:] P. Fajgielski (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008, s. 49.
[35] M. Wild, *Komentarz do art. 51 Konstytucji*, [w:] M. Safjan, L. Bosek, *Konstytucja RP…*, Legalis; R. Piotrowski, Prawo do prywatności i ochrony danych osobowych jako wartości konstytucyjne, [w:] A. Mednis (red.), *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, Warszawa 2016, s. 25.
[36] I. Lipowicz, *Konstytucyjne podstawy ochrony…,* s. 47.

wykorzystania, choć nie jest to prawo nieograniczone – mogą bowiem istnieć sytuacje, w których prymat wiedzie tzw. interes ogółu[37]. Koncepcja autonomii informacyjnej jednostki występuje także w orzecznictwie TK[38], który podobnie jak trybunał niemiecki uważa, że oznacza ona „prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, znajdującymi się w posiadaniu innych podmiotów"[39]. Na temat relacji art. 47 i art. 51 Konstytucji wypowiedzieli się także J. Barta i R. Markiewicz, którzy stwierdzili, że stanowią one reżimy wzajemnie niezależne, ponieważ o ile niekiedy może dojść do jednoczesnego naruszenia prawa do prywatności i ochrony danych osobowych, to „wystąpić mogą również sytuacje, w których przetwarzanie danych zapewne nie zostałoby zakwalifikowane jako naruszenie prawa do prywatności; podobnie można wyobrazić sobie przypadki wkroczenia w objętą ochroną sferę prywatności poprzez działania inne niż przetwarzanie danych osobowych"[40].

Konstytucyjne wolności i prawa nie mają jednak charakteru absolutnego. Zgodnie z art. 31 ust. 3 Konstytucji, ograniczenia w zakresie korzystania z nich mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw. Warto podkreślić, że art. 47 Konstytucji znalazł się w katalogu przepisów ustanawiających prawa i wolności, których ograniczenie nie jest dopuszczalne w czasie stanu wojennego i wyjątkowego, co wynika z art. 233 ust. 1 Konstytucji i świadczy o szczególnym znaczeniu prawa do prywatności[41].

3. Ustawowa regulacja ochrony danych osobowych przed unijną reformą

Pierwszym polskim aktem prawnym kompleksowo regulującym ochronę danych osobowych była ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[42]. Mimo, że powstała przed przystąpieniem Polski do Unii Europejskiej, była wzorowana na dyrektywie 95/46[43]. Uodo z 1997 r. określała zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób

[37] P. Litwiński, *Zasada autonomii informacyjnej w orzecznictwie Trybunału Konstytucyjnego a stosowanie przepisów o ochronie danych osobowych*, [w:] P. Fajgielski (red.), *Ochrona danych osobowych w Polsce…*, s. 170.
[38] Wyrok TK z dnia 12.11.2002 r., sygn. akt SK 40/01, OTK ZU 6A/2002, poz. 81.
[39] Wyrok TK z dnia 19.02.2002 r., sygn. akt U 3/01, OTK ZU 1A/2002, poz. 3.
[40] J. Barta, R. Markiewicz, *Prawo do prywatności w społeczeństwie informatycznym*, „Ethos" 1999, nr 1/2 (45/46), s. 380.
[41] D. Kuźnicka-Błaszkowska, *Prawna ochrona życia prywatnego a ochrona informacji o sobie samym w Konstytucji RP w orzecznictwie Trybunału Konstytucyjnego – wybrane aspekty*, „Acta Universitatis Wratislaviensis" 2020, nr 121, s. 210.
[42] T.j. Dz. U. z 2016 r. poz. 922, dalej uodo z 1997 r.
[43] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, wyd. VI, Warszawa 2015, Lex.

fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych. Zawierała także przepisy konstytuujące organ właściwy do spraw związanych z ochroną danych osobowych – Generalnego Inspektora Ochrony Danych Osobowych[44], jego zadania i kompetencje, regulowała niektóre aspekty postępowań prowadzonych na podstawie tej ustawy, w tym postępowanie kontrolne, oraz przewidywała, w art. 48-54a, penalizację niektórych działań lub zaniechań związanych z przetwarzaniem danych osobowych i niewypełnianiem ustawowych obowiązków.

Obowiązki administratora danych osobowych, czyli zgodnie z art. 7 pkt 4 uodo z 1997 r. podmiotu decydującego o celach i środkach przetwarzania danych osobowych, wynikały z zasad określonych w rozdziale 3 tej ustawy, przede wszystkim w art. 26. Administrator danych osobowych miał obowiązek zapewnić, by dane osobowe były przetwarzane zgodnie z prawem[45], były zbierane dla oznaczonych, zgodnych z prawem celów i co do zasady niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane oraz przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Administrator danych osobowych miał obowiązek[46] poinformować osobę, której dane przetwarzał – niezależnie od tego, czy dane zostały pozyskane bezpośrednio od niej, czy też z innego źródła – m.in. o swojej tożsamości i danych kontaktowych, celach przetwarzania i odbiorcach danych[47] lub ich kategoriach, prawie dostępu do treści swoich danych oraz ich poprawiania, o dobrowolności albo obowiązku podania danych.

Obowiązki administratora danych osobowych w zakresie zabezpieczenia danych polegały na wdrożeniu środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, przede wszystkim przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Środki służące tym celom powinny być odpowiednie do zagrożeń oraz kategorii danych[48], co wskazywało na konieczność dokonania przez administratora oceny ryzyka i zastosowania adekwatnych do niego zabezpieczeń. Z drugiej strony ustawodawca przewidział delegację dla ministra do spraw informatyzacji do określenia w drodze rozporządzenia

[44] Zwanego dalej GIODO.
[45] Szerzej na ten temat por. M. Sakowska-Baryła, *Przesłanki dopuszczalności przetwarzania danych osobowych w art. 23 ustawy o ochronie danyc*h, „Przegląd Prawa Handlowego" 2007, nr 10, s. 10-14.
[46] Było to zasadą, od której istniały wyjątki, np. okoliczność, że osoba dysponowała wcześniej informacjami o przetwarzaniu danych osobowych – patrz art. 24 ust. 2 i art. 25 ust. 2 uodo z 1997 r.
[47] Stosownie do art. 7 pkt 6 ustawy o ochronie danych osobowych z 1997 r., przez odbiorcę należy rozumieć każdego, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela administratora danych osobowych mającego siedzibę albo miejsce zamieszkania w państwie nienależącym do Europejskiego Obszaru Gospodarczego, podmiotu przetwarzającego dane osobowe w imieniu administratora danych osobowych, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
[48] Dobór środków zabezpieczenia danych powinien uwzględniać okoliczność przetwarzania danych osobowych podlegających szczególnej ochronie, tzw. danych wrażliwych – określonych w art. 27 ust. 1 uodo z 1997 r.

sposobu prowadzenia i zakresu dokumentacji opisującej przetwarzanie danych i zabezpieczenia, podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych. W rezultacie w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[49], wprowadzono trzy poziomy bezpieczeństwa dotyczące przetwarzania danych w systemie informatycznym: podstawowy, średni, wysoki i przyporządkowane im środki ochrony. Kryteriami decydującymi o obowiązku zastosowania środków na określonym poziomie była okoliczność przetwarzania tzw. danych wrażliwych oraz połączenia urządzeń służących do przetwarzania danych do sieci publicznej. Przepisy ww. rozporządzenia określały również sposób prowadzenia i zakres dokumentacji opisującej przetwarzanie danych osobowych – na którą składały się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Opracowanie i wdrożenie polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych nie wyczerpywało jednak obowiązków administratora danych osobowych związanych z dokumentacją przetwarzania i ochrony danych osobowych. Uodo z 1997 r. przewidywała również konieczność prowadzenia ewidencji osób upoważnionych do przetwarzania, która powinna zawierać imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, identyfikator, jeżeli dane były przetwarzane w systemie informatycznym[50].

Osobie, której dane były przetwarzane, przysługiwały różne uprawnienia – które ze względu na ich charakter, dzielono na uprawnienia informacyjne (informowanie o przetwarzaniu i jego uwarunkowaniach), korekcyjne (m.in. uaktualnienie, sprostowanie) oraz szczególne (zaprzestanie przetwarzania danych osobowych, sprzeciw, żądanie ponownego rozpatrzenia sprawy, w której treść rozstrzygnięcia jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym)[51]. Osoba, której dane dotyczą, mogła złożyć skargę do GIODO, jeśli uznała, że jej prawa zostały naruszone w związku z przetwarzaniem danych osobowych.

[49] Dz. U. z 2004 r. Nr 100 poz. 1024.
[50] Szerzej na temat obowiązków dokumentacyjnych na gruncie uodo z 1997 r. D. Fleszer, *Dokumentacja przetwarzania danych osobowych,* „Roczniki Administracji i Prawa" 2017, nr XVII, s. 71-87.
[51] Por. P. Fajgielski, *Kontrola przetwarzania i ochrony…*, s. 46-47.

4. Reforma ochrony danych osobowych

4.1 Geneza reformy i objęcie dziecka szczególną ochroną jako jeden z jej celów

W dniu 4.11.2010 r. Komisja Europejska przedłożyła Parlamentowi Europejskiemu, Radzie, Europejskiemu Komitetowi Ekonomiczno-Społecznemu oraz Komitetowi Regionów komunikat *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej*[52]. Stwierdziła w nim, że dyrektywa 95/46 stanowi „kamień milowy w historii ochrony danych osobowych w Unii Europejskiej" i choć jej cele – ochrona praw podstawowych i swobodny przepływ danych osobowych w ramach rynku wewnętrznego, czyli obszaru bez granic wewnętrznych, w którym jest zapewniony swobodny przepływ towarów, osób, usług i kapitału[53] – pozostają aktualne, rozwój technologiczny i globalizacja spowodowały tak daleko idące zmiany, że konieczne staje się zmierzenie z nowymi wyzwaniami w dziedzinie ochrony danych osobowych. Komisja Europejska jako najbardziej ewidentny przykład zagrożeń związanych z upublicznianiem na masową skalę informacji wskazała „sieci społecznościowe z setkami milionów członków rozsianych po całym świecie"[54]. Przeprowadzone przez komisję publiczne konsultacje dowiodły, że interesariusze są zgodni co do tego, że potrzebna jest jedna regulacja z zakresu ochrony danych osobowych, dotycząca wszystkich sektorów, w celu zagwarantowania jednolitego podejścia w tym obszarze. Komisja Europejska wyjaśniła, że po wejściu w życie Traktatu z Lizbony możliwe jest przyjęcia takiego aktu prawnego na podstawie art. 8 KPP.

Rada Unii Europejskiej wyraziła aprobatę dla propozycji KE w konkluzjach przyjętych w ramach posiedzenia Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w dniach 24-25.02.2011 r.[55]. W związku z szerokim poparciem planowanych zmian w zakresie prawa ochrony danych osobowych Komisja Europejska w 2012 r. skierowała do Parlamentu Europejskiego i Rady wniosek prawodawczy[56]. Zawierał on projekt Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), mającego –

---

[52] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej*, KOM(2010) 609, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A52010DC0609 (dostęp: 23.09.2020), dalej jako: komunikat KE z 2010 r.

[53] Art. 26 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej (Dz. Urz. C 326 z 26.10.2012, s. 47), dalej jako: TFUE.

[54] Komunikat KE z 2010 r., s. 2.

[55] Council conclusions on the Communication from the Commission to the European Parliament and the Council -A comprehensive approach on personal data protection in the European Union, 3071st Justice and Home Affairs Council meeting Brussels, 24-25.02.2011 r., https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf (dostęp: 23.09.2020).

[56] Wniosek Komisji Europejskiej z dnia 25 stycznia 2012 r. **„**Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)", COM/2012/011 final, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A52012PC0011#document1 (dostęp: 23.09.2020), dalej jako: wniosek KE z 2012 r.

obok nowej dyrektywy 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 – tworzyć nowe ramy prawne ochrony danych osobowych w Unii Europejskiej. W uzasadnieniu do wniosku KE z 2012 r. powtórzyła ona argumentację przemawiającą za reformą ochrony danych osobowych, przedstawioną wcześniej w swoim komunikacie z 2010 r. Wyjaśniła także, że „Rozporządzenie uważa się za najbardziej odpowiedni instrument prawny służący do zdefiniowania ram ochrony danych osobowych w Unii" i wskazała, że osiągnięcie tego celu innymi instrumentami nie jest możliwe, m.in. ze względu na niemożność ich zrealizowania samodzielnie przez poszczególne państwa członkowskie, dlatego wybór tego rodzaju aktu prawnego jest zgodny z tzw. zasadą pomocniczości[57]. Treść projektu zmieniała się w trakcie trwającego kilka lat procesu legislacyjnego[58]. Wpływ na to miały m.in. uwagi zgłoszone przez przedsiębiorstwa świadczące usługi za pośrednictwem internetu – np. operatorzy wyszukiwarek, podmioty prowadzące portale społecznościowe – dla których dane są podstawowym czynnikiem pozwalającym na tworzenie i rozwój usług[59].

Ważnym czynnikiem w procesie kształtowania nowego aktu prawnego regulującego ochronę danych osobowych, w tym jednym z powodów przedłużania się prac nad nim[60], było przygotowywanie strategii dotyczącej utworzenia jednolitego rynku cyfrowego (*Digital Single Market*) – zaprezentowanej w 2015 r. przez KE w komunikacie[61]. Jednolity rynek cyfrowy zdefiniowano w nim jako „przestrzeń, w której zapewniony jest swobodny przepływ towarów, osób, usług i kapitału, a obywatele i przedsiębiorstwa mogą bez przeszkód i na zasadach uczciwej konkurencji uzyskać dostęp do usług online lub je świadczyć. W takiej przestrzeni zagwarantowany jest także wysoki poziom ochrony konsumentów i danych osobowych, niezależnie od obywatelstwa lub miejsca zamieszkania"[62]. Zdaniem B. Pachulskiej-Smulskiej, „Istotą jednolitego rynku cyfrowego jest usunięcie krajowych ograniczeń dla transakcji dokonywanych za pośrednictwem Internetu"[63]. Utworzenie jednolitego rynku cyfrowego ma

[57] Wniosek KE z 2012 r., s. 6-7.
[58] Odrzucono m.in. poprawki KE mające na celu złagodzenie niektórych obowiązków w przypadku mikro- i małych przedsiębiorstw – por. M. Siwicki, *Ochrona osób fizycznych w związku z przetwarzaniem i swobodnym przepływem danych osobowych (uwagi w związku z projektem rozporządzenia Parlamentu Europejskiego i Rady*), „Państwo i Prawo" 2016, nr 3.
[59] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej*, Warszawa 2014, s.73.
[60] Tamże.
[61] Komunikat z dnia 5 maja 2015 r. Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów *Strategia jednolitego rynku cyfrowego dla Europy*, COM(2015) 192 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52015DC0192&from=EN, (dostęp: 23.09.2020).
[62] Tamże.
[63] B. Pachulska-Smulska, *Konsument na jednolitym rynku cyfrowym*, [w:] M. Królikowska-Olczak, B. Pachulska-Smulska (red.), *Ochrona prawna konsumenta na rynku mediów elektronicznych*, Warszawa 2015, Legalis.

nastąpić w wyniku wprowadzenia zmian na gruncie prawa telekomunikacyjnego, prawa autorskiego, zasad ochrony konsumentów oraz ochrony danych osobowych – co jest kluczowe, gdyż zdaniem KE małe zaufanie konsumentów do dostawców wyszukiwarek internetowych, portali społecznościowych, platform handlu elektronicznego czy poczty elektronicznej jest główną przeszkodą dla powodzenia całej koncepcji, która ma przynieść wymierne korzyści ekonomiczne[64] i uczynić z Unii Europejskiej lidera gospodarki cyfrowej.

Kreśląc w komunikacie KE z 2010 r. główne kierunki zmian wskazano na potrzebę wzmocnienia praw osób fizycznych – zwłaszcza dzieci, ułatwienia swobodnego przepływu danych osobowych na rynku wewnętrznym, uproszczenia międzynarodowych transferów danych osobowych. Postulat podniesienia poziomu ochrony danych osobowych dzieci podyktowany był wynikami badań, które wykazały, że dzieci są mniej świadome zagrożeń związanych z korzystaniem z internetu i konsekwencji wynikających z wykorzystania ich danych osobowych. Stanowisko w sprawie zawartych w komunikacie KE z 2010 r. propozycji, w tym dotyczących wzmocnienia ochrony praw dzieci, przedstawiło wiele podmiotów. Europejski Inspektor Ochrony Danych stwierdził, że trafnie nakreślono w nim główne problemy i wyzwania, choć pożądane byłoby bardziej ambitne podejście do reformy ochrony danych osobowych[65]. EIOD zauważył, że korzystająca z portali społecznościowych młodzież ma ograniczoną wiedzę na temat zakresu ujawnianych w ten sposób informacji o sobie i związanych z tym potencjalnych, długofalowych skutków. W celu wzmocnienia ochrony danych osobowych dzieci zaproponował wprowadzenie do nowej regulacji kilku rozwiązań, np. dodatkowych wymogów związanych z informowaniem dzieci o przetwarzaniu ich danych osobowych, postanowień chroniących dzieci przed reklamą behawioralną, zakaz zbierania niektórych kategorii danych osobowych od dzieci, zasad udzielania zgody na przetwarzanie przez dziecko i przez rodziców, w tym określenia sposobów weryfikacji wieku dziecka[66].

Spostrzeżenia na temat sytuacji dzieci przedstawił także Parlament Europejski w rezolucji z dnia 06.07.2011 r.[67], w której podkreślił „potrzebę opracowania takiego prawodawstwa z zakresu ochrony danych, które uwzględniałoby szczególną potrzebę ochrony dzieci i małoletnich", a także, że „umiejętność korzystania z mediów musi stać się elementem edukacji formalnej, tak aby

[64] KE oszacowała, że wdrożenie zaproponowanej strategii może zwiększyć europejski PKB o 415 miliardów euro.
[65] Opinia EIOD dotycząca komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", Dz. Urz. UE C 181/1 z dnia 22.06.2011 r., s. 1.
[66] Opinia EIOD dotycząca komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", Dz. Urz. UE C 181/1 z dnia 22.06.2011 r., s. 1.
[67] Rezolucja Parlamentu Europejskiego z dnia 06.07. 2011 r. w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej, https://www.europarl.europa.eu/doceo/document/TA-7-2011-0323_PL.html?redirect#def_1_5 (dostęp: 23.09.2020).

nauczyć dzieci i małoletnich odpowiedzialnego funkcjonowania w środowisku internetowym; w tym celu należy zwrócić szczególną uwagę na przepisy odnoszące się do gromadzenia i dalszego przetwarzania danych dzieci, wzmocnienie zasady celowości w odniesieniu do danych dzieci oraz sposobów pozyskiwania zgody dzieci, a także na behawioralną ochronę przed reklamą"[68].

Jak dowodzą powyższe argumenty, od samego początku procesu legislacyjnego wyraźnie podkreślano, że jednym z głównych celów reformy jest podniesienie poziomu ochrony praw dzieci w kontekście przetwarzania danych osobowych. Uczestnicy prac zdawali sobie sprawę z konieczności przyjęcia rozwiązań dostosowanych do wyzwań, jakie niesie ze sobą korzystanie przez dzieci z internetu i usług społeczeństwa informacyjnego.

4.2 Ogólna charakterystyka rozporządzenia 2016/679 przyjętego w wyniku reformy

Nowy akt prawny – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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)[69] – przyjęto dnia 27.04.2016 r. Na rozporządzenie 2016/679 składa się preambuła – licząca 173 motywy, oraz część normatywna – zawierająca 99 artykułów. Preambuła w unijnych aktach prawnych pełni dwie główne funkcje. Po pierwsze, wyjaśnione są w niej powody, dla których dany akt został przyjęty, do czego zobowiązuje art. 296 TFUE. Po drugie, w preambule przedstawione są informacje, pomocne w interpretacji przepisów, dotyczące przede wszystkim celów, jakie mają być osiągnięte dzięki przyjętym regulacjom – motywy „stanowią zatem kontekst normatywny dla przepisów zawartych w akcie prawnym"[70]. Są istotne w procesie wykładni prawa dokonywanej m.in. przez TSUE i organy nadzorcze ds. ochrony danych osobowych. Choć prawo UE podlega co do zasady takim samym dyrektywom interpretacyjnym jak prawo państw członkowskich, wykładnia językowa nie zawsze sprawdza się w świetle występowania różnic znaczeniowych, wynikających z uwarunkowań językowych – dlatego nadrzędne znaczenie ma wykładnia celowościowo-funkcjonalna, pozwalająca na zapewnienie jak największej skuteczności norm prawa UE (zgodnie z zasadą *effect utile*)[71]. Ponadto służyć ma temu tzw. prounijna wykładnia przepisów prawa państw członkowskich UE – w szczególności przyjmowanych w celu wdrożenia dyrektyw[72]. Wszystkie wersje językowe

[68] Tamże.
[69] Dz.U. UE L 119 z 04.05.2016, s. 1, dalej jako: rozporządzenie 2016/679.
[70] K. Morawska, *Rola oraz status prawny motywów preambuły ogólnego rozporządzenia o ochronie danych – klucz do wykładni przepisów nowego prawa unijnego*, [w:] M. Kawecki, T. Osiej, *Ogólne rozporządzenie o ochronie danych. Wybrane zagadnienia*, Warszawa 2017, s. 29.
[71] J. Helios, W. Jedlecka, *Wykładnia prawa Unii Europejskiej ze stanowiska teorii prawa*, Wrocław 2018, s. 12.
[72] Por. W. Rowiński, *Nakaz dokonywania wykładni prounijnej jako dyrektywa wykładni systemowej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2016, nr 1, s. 100-101 i tam powołane orzecznictwo TSUE.

unijnych aktów prawnych są bowiem uznawane za autentyczne i tak samo wiążące – uznaje się je za oryginały, przyjmując fikcję, że tłumaczenie nie miało miejsca[73]. Motywy zawarte w preambule rozporządzenia 2016/679 są brane pod uwagę także przez polski organ nadzorczy ds. ochrony danych osobowych i powoływane w uzasadnieniach jego decyzji[74], a ponadto w wytycznych oraz rekomendacjach Europejskiej Rady Ochrony Danych[75] – organu powołanego na podstawie art. 68 rozporządzenia 2016/679, następcy Grupy Roboczej Art. 29[76], któremu przyznano, w porównaniu do poprzedniego stanu prawnego, dodatkowe kompetencje służące spójnemu stosowaniu nowego rozporządzenia[77]. Motywy są zatem bardzo istotnym narzędziem interpretacyjnym, lecz zgodnie z orzecznictwem TSUE, nie mają charakteru normatywnego[78].

Stosownie do art. 1 ust. 1 i 2 rozporządzenia 2016/679, ustanawia ono przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych[79]; chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych. Rozporządzenie 2016/679 ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych (art. 2 ust. 1). Wyłączenia spod zakresu stosowania rozporządzenia 2016/679 określa art. 2 ust. 2 i 3 – obejmują przetwarzanie danych osobowych: w ramach działalności nieobjętej zakresem prawa Unii; przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE; przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze; przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar[80], w tym

[73] J. Szponar-Seroka, *Wielojęzyczność jako wyzwanie w procesie stanowienia i wykładni prawa Unii Europejskiej*, „Studenckie Zeszyty Naukowe" 2017, nr 33, s. 97.

[74] Np. w uzasadnieniu decyzji Prezesa UODO z dnia 12.11.2020 r., sygn. DKN.5101.25.2020, odwołano się do motywów ośmiokrotnie, https://uodo.gov.pl/decyzje/DKN.5101.25.2020 (dostęp: 23.11.2020).

[75] Dalej jako: EROD. Wykaz dokumentów przyjętych przez EROD jest dostępny na stronie: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en (dostęp: 23.09.2020).

[76] U. Góral, *Europejska Rada Ochrony Danych – proces transformacji Grupy Roboczej Art. 29*, „Monitor Prawniczy" dodatek: *Wdrażanie ogólnego rozporządzenia…*, s. 13.

[77] Patrz art. 70 rozporządzenia 2016/679.

[78] K. Morawska, *Rola oraz status prawny motywów preambuły ogólnego rozporządzenia o ochronie danych – klucz do wykładni przepisów nowego prawa unijnego*, [w:] M. Kawecki, T. Osiej, *Ogólne rozporządzenie o ochronie danych...*, s. 32-24 i tam powołane orzecznictwo.

[79] W art. 1 ust. 3 rozporządzenia 2016/679 doprecyzowano, że nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Zgodnie z motywem 13, swobodny przepływ danych osobowych jest niezbędny do prawidłowego funkcjonowania rynku wewnętrznego. Szerzej na temat swobodnego przepływu danych osobowych traktuje mój artykuł *Ułatwienie swobodnego przepływu danych osobowych i wsparcie rozwoju gospodarki cyfrowej na rynku wewnętrznym w świetle ogólnego rozporządzenia o ochronie danych*, „Studia i Materiały Miscellanea Oeconomicae" 2018, nr 3, s. 257-265.

[80] Przetwarzanie danych osobowych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania reguluje uchwalona w wyniku

ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom; a także przez instytucje, organy i jednostki organizacyjne UE[81].

Stosownie do art. 3 ust. 2 rozporządzenia 2016/679 ma ono zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w UE, niezależnie od tego, czy przetwarzanie odbywa się w UE. Nieistotna jest zatem okoliczność, gdzie faktycznie dochodzi do przetwarzania danych osobowych – np. gdzie zlokalizowany jest serwer, na którym są one przechowywane[82]. Ponadto do stosowania rozporządzenia 2016/679, zgodnie z jego art. 3 ust. 2, zobowiązane są podmioty niemające jednostek organizacyjnych w UE, które przetwarzają dane osobowe dotyczące osób przebywających w UE, jeśli czynności przetwarzania wiążą się z oferowaniem towarów lub usług takim osobom, których dane dotyczą, w UE – niezależnie od tego, czy wymaga się od tych osób zapłaty, lub monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w UE. W ten sposób podjęto próbę rozszerzenia kręgu podmiotów, na których spoczywają obowiązki związane z ochroną danych osobowych przewidzianą w rozporządzeniu 2016/679, na podmioty spoza UE, których działalność jest „nakierowana" na rynek UE i adresowana do osób przebywających w państwach członkowskich – bez względu na charakter ich pobytu (stały lub tymczasowy) ani jego legalność[83]. Zgodnie z motywem 23 preambuły rozporządzenia 2016/679, aby ustalić, czy ma ono zastosowanie do przetwarzania danych osobowych przez podmiot spoza UE, należy sprawdzić, czy oferowanie usługi osobom w co najmniej jednym państwie członkowskim UE jest „oczywiste" – przy czym „O ile do ustalenia takiego zamiaru nie wystarczy sama dostępność w Unii strony internetowej administratora, podmiotu przetwarzającego, pośrednika, adresu poczty elektronicznej lub innych danych kontaktowych ani posługiwanie się

---

reformy dyrektywa 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 uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, s. 89), którą do polskiego porządku prawnego ma za zadanie implementować ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) – por. A. Gryszczyńska, *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości – zakres przedmiotowy i podmiotowy*, [w:] K. Czaplicki, G. Szpor (red.), *Internet. Przetwarzanie danych osobowych. Processing of personal data*, Warszawa 2019, Legalis; A. Grzelak (red.), *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, Warszawa 2019; M. Kusak, P. Wiliński, *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Warszawa 2020.

[81] Przetwarzanie danych osobowych przez instytucje, organy i jednostki organizacyjne UE reguluje Rozporządzenie 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 dnia 21.11.2018, s. 39-98.

[82] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 3 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, Legalis.

[83] M. Górski, *Komentarz do art. 3 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, Legalis.

językiem powszechnie stosowanym w państwie trzecim, w którym jednostkę organizacyjną ma administrator, o tyle potwierdzeniem oczywistości faktu, że administrator planuje oferować w Unii towary lub usługi osobom, których dane dotyczą, mogą być czynniki takie, jak posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w Unii". Zdaniem EROD okoliczność, czy dana osoba przebywa w UE, powinna być oceniana „w momencie, w którym ma miejsce odpowiednie działanie inicjujące, tj. w momencie oferowania towarów lub usług, lub w momencie, w którym monitorowane jest zachowanie, niezależnie od czasu trwania oferty lub monitorowania"[84]. Jednocześnie EROD wyjaśnia, że jeśli usługa jest kierowana wyłącznie do osób spoza UE, a korzystająca z niej osoba wjedzie na terytorium jednego z państw członkowskich UE i nie przerwie korzystania, rozporządzenia 2016/679 nie stosuje się do takiego przetwarzania[85].

Celem posłużenia się kryterium „nakierowania" jest zwiększenie efektywności ochrony danych osobowych, ponieważ w związku z globalizacją i świadczeniem usług na pośrednictwem internetu przez podmioty spoza UE, zwłaszcza przedsiębiorstwa ze Stanów Zjednoczonych Ameryki – np. prowadzące portale społecznościowe, będące operatorami wyszukiwarek internetowych – dochodzi do zbierania przez nie ogromnej ilości danych[86]. Należy jednak podkreślić, że pojęcie „działalność" powinno być rozumiane szeroko – zawężenie go wyłącznie do działalności gospodarczej byłoby nieuprawnione[87]. Skuteczność rozszerzenia obowiązku stosowania rozporządzenia 2016/679 przez podmioty spoza UE – tzw. eksterytorialny skutek – może budzić wątpliwości, szczególnie w świetle wyroku TSUE z dnia 24.09.2019 r. w sprawie C-507/17[88]. Trybunał orzekł w nim, że operator wyszukiwarki, który na podstawie rozporządzenia 2016/679 uwzględnił wniosek osoby fizycznej o usunięcie linków do stron internetowych, do których prowadziła lista wyników wyświetlana po wpisaniu w wyszukiwarkę jej imienia i nazwiska, nie jest zobowiązany do ich usunięcia ze wszystkich wersji tej wyszukiwarki, a jedynie z wersji, które odpowiadają wszystkim państwom członkowskim UE. Jednocześnie TSUE wskazał, że „operator wyszukiwarki jest odpowiedzialny za podjęcie, w razie konieczności, wystarczająco skutecznych środków w celu zapewnienia rzeczywistej ochrony praw

[84] EROD, *Wytyczne 3/2018 w sprawie terytorialnego zakresu stosowania RODO (art. 3),* wersja 2.0 przyjęta 12.11.2019 r., https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_pl.pdf (dostęp: 23.09.2020), s. 16.
[85] EROD, *Wytyczne 3/2018*… , s. 16.
[86] M. Czerniawski, *Zakres terytorialny a pojęcie „jednostki organizacyjnej" w przepisach ogólnego rozporządzenia o ochronie danych – zarys problemu*, [w:] G. Sibiga (red.), *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, Warszawa 2016, s. 22.
[87] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 3 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis.
[88] Wyrok TSUE z dnia 24.09.2019 r. w sprawie C-507/17, Google LLC, następca prawny Google Inc., przeciwko Commission nationale de l'informatique et des libertés (CNIL).

podstawowych osoby, której dane dotyczą. Środki te same w sobie muszą być zgodne ze wszystkimi wymogami prawnymi i w efekcie uniemożliwiać internautom w państwach członkowskich uzyskiwanie dostępu do spornych linków w wyniku wyszukiwania przeprowadzonego w oparciu o imię i nazwisko tej osoby, lub przynajmniej poważnie zniechęcać ich do uzyskiwania takiego dostępu". TSUE nie wypowiedział się, na czym mogą polegać „poważnie zniechęcające" środki, pozostawiając tę ocenę sądowi odsyłającemu. Wydaje się, że skuteczniejszą zachętą do stosowania unijnych przepisów o ochronie danych osobowych od próby wprowadzenia obowiązku ich stosowania będą korzyści związane z budową przewagi konkurencyjnej ze względu na poszanowanie praw użytkowników usług i rozwojem koncepcji społecznej odpowiedzialności biznesu.

Rozporządzenie 2016/679 określa naczelne zasady przetwarzania danych osobowych; prawa osób, których dane są przetwarzane; obowiązki ciążące na podmiotach, które przetwarzają dane osobowe; zasady przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych; zadania krajowych organów nadzorczych ds. ochrony danych osobowych; zasady współpracy między tymi organami; środki ochrony prawnej, odpowiedzialność i sankcje za naruszenie rozporządzenia 2016/679 – w tym przepisy dotyczące administracyjnych kar pieniężnych; przepisy dotyczące szczególnych sytuacji związanych z przetwarzaniem (m.in. przetwarzanie danych osobowych w kontekście zatrudnienia, przetwarzanie danych osobowych przez kościoły i związki wyznaniowe); zasady przyjmowania przez KE aktów delegowanych i aktów wykonawczych; zawiera także przepisy przejściowe.

Do rozporządzenia 2016/679 przeniesiono wiele rozwiązań z dyrektywy 95/46 – podstawowe instytucje i ogólne zasady przetwarzania danych osobowych są bardzo zbliżone. Jest to spowodowane w dużej mierze koniecznością zachowania zgodności unijnych regulacji z konwencją 108, której stronami są państwa członkowskie UE[89], a także konstatacją, że cele i główne założenia dyrektywy 95/46 pozostają aktualne, choć niezbędne jest dostosowanie ich do aktualnych wyzwań związanych przede wszystkim z rozwojem technologii. W przepisach rozporządzenia 2016/679 zauważalne jest więc podejście ewolucyjne[90]. Z tego względu dorobek orzecznictwa i doktryny, powstały pod rządami dyrektywy 95/46 i uodo z 1997 r., w wielu aspektach pozostaje aktualny i jest przydatny również po rozpoczęciu stosowania rozporządzenia 2016/679. Z drugiej strony nie można umniejszać znaczenia zmian, jakie wprowadzono w wyniku reformy ochrony danych osobowych. Do najważniejszych z nich można zaliczyć uregulowanie

[89] Opinia EIOD dotycząca komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", Dz. Urz. UE C 181/1 z dnia 22.06.2011 r., s. 1.

[90] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2022, wyd. 2, s. 86.

ochrony danych osobowych za pomocą unijnego rozporządzenia, stosowanego bezpośrednio[91]; przyjęcie podejścia opartego na ryzyku – rozumianego jako obowiązek analizowania ryzyka naruszenia praw lub wolności osób, których dane są przetwarzane[92]; wprowadzenie administracyjnych kar pieniężnych za naruszenie rozporządzenia 2016/679; wprowadzenie obowiązku uwzględniania ochrony danych osobowych w fazie projektowania (planowania) i w czasie przetwarzania danych osobowych oraz zasady domyślnej ochrony danych. Moim zdaniem szczególnie istotną zmianą jest również wprowadzenie regulacji dotyczących ochrony danych osobowych dziecka. Rozporządzenie 2016/679 jest pierwszym aktem prawnym, które wprost odnosi się do tej problematyki.

Rozporządzenie 2016/679 weszło w życie dwudziestego dnia po publikacji w Dzienniku Urzędowym Unii Europejskiej, która miała miejsce 04.05.2016 r., natomiast ma zastosowanie od 25.05.2018 r. (art. 99 rozporządzenia 2016/679).

4.3 Wpływ rozporządzenia 2016/679 na polskie prawo

Dwuletni okres między wejściem w życie a rozpoczęciem stosowania rozporządzenia 2016/679 miał pozwolić na zapoznanie się z nowymi przepisami i dostosowanie się do nich przez podmioty, które są obowiązane do ochrony danych osobowych, a także na wprowadzenie ewentualnych zmian legislacyjnych przez poszczególne państwa członkowskie. Wprawdzie unijne rozporządzenie nie wymaga – w przeciwieństwie do dyrektywy – implementacji do krajowych porządków prawnych, ponieważ ma zasięg ogólny, wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich UE[93], zmiany w prawie krajowym okazały się potrzebne z dwóch powodów.

Po pierwsze, konieczny był przegląd ustawodawstwa w celu zmiany przepisów, które okazałyby się niespójne z rozporządzeniem 2016/679 oraz w celu usunięcia odesłań do uodo z 1997 r., której większość przepisów miała zostać uchylona z dniem 25.05.2018 r. Po drugie, rozporządzenie 2016/679 zawiera wiele klauzul kompetencyjnych, które stanowią dla państw członkowskich podstawę do wprowadzenia w swoim porządku prawnym własnych rozwiązań, w zakresie wyznaczonym przez te klauzule[94]. Wśród klauzul kompetencyjnych występujących w rozporządzeniu 2016/679 wyróżnia się klauzule określające obligatoryjny i fakultatywny zakres

[91] Tamże, s. 85.
[92] GIODO, poradnik *Czy jesteś gotowy na RODO?,* https://www.giodo.gov.pl/pl/1520281/10255 (dostęp: 23.09.2020).
[93] Art. 288 TFUE.
[94] D. Lubasz [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2017, s. 113 i tam podane przykłady.

regulacji[95]. Klauzule obligatoryjne dotyczą obowiązku przyjęcia przepisów konstytuujących organ lub organy nadzorcze oraz przepisów o charakterze proceduralnym, gdyż UE nie ma kompetencji do regulowania tych kwestii. Klauzule fakultatywne odnoszą się do różnych zagadnień, w tym jedno z nich dotyczy warunków wyrażenia przez dziecko zgody na przetwarzanie danych osobowych w przypadku wskazanym w art. 8 rozporządzenia 2016/679.

W Polsce prace nad zmianami legislacyjnymi w celu przygotowania do rozpoczęcia stosowania rozporządzenia 2016/679 koordynowało Ministerstwo Cyfryzacji[96]. W ocenie Rządowego Centrum Legislacji przeglądowi należało poddać kilkaset aktów prawnych[97]. Stanowisko i propozycje w sprawie nowych przepisów przedstawiało wiele podmiotów, w tym GIODO[98]. W rezultacie uchwalona została ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych[99] oraz ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 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)[100].

Przepisy uodo z 2018 r. określają podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o jego wyznaczeniu; warunki i tryb akredytacji podmiotu uprawnionego do certyfikacji w zakresie ochrony danych osobowych, akredytowanego przez Polskie Centrum Akredytacji, podmiotu monitorującego kodeks postępowania oraz certyfikacji; tryb zatwierdzenia kodeksu postępowania; organ właściwy w sprawie ochrony danych osobowych – czyli Prezesa Urzędu Ochrony Danych Osobowych[101]; postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych; tryb europejskiej współpracy administracyjnej; kontrolę przestrzegania przepisów o ochronie danych osobowych; odpowiedzialność cywilną za naruszenie przepisów o ochronie danych osobowych i postępowanie przed sądem; odpowiedzialność karną i nakładanie administracyjnych kar pieniężnych za naruszenie przepisów o ochronie danych

[95] G. Sibiga, *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzeni o ochronie danych – wybrane zagadnienia* [w:] G. Sibiga (red.), *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, Warszawa 2016, s. 18-19; P. Kozik, *Zakres swobody regulacyjnej państw członkowskich przy wdrażaniu ogólnego rozporządzenia o ochronie danych osobowych do prawa krajowego*, „Europejski Przegląd Sądowy" 2017, nr 5, s. 20.

[96] Szerzej na ten temat por. A. Kobylańska, M. Lewoszewski, *Poland: A Brief Overview Concerning the Implementation of the GDPR*, "European Data Protection Law Review" 2017, nr 4, s. 507-511.

[97] E. Bielak-Jomaa, D. Lubasz (red.), *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016, s. 15.

[98] *Konieczne zmiany legislacyjne przepisów o ochronie danych osobowych - wstępna analiza ekspertów Biura GIODO,* https://archiwum.giodo.gov.pl/pl/1520281/9747 (dostęp: 23.09.2020).

[99] T.j. Dz. U. z 2019 r. poz. 1781, dalej jako: uodo z 2018 r.

[100] Dz. U. z 2019 r. poz. 730. Warto podkreślić, że przepisy mające na celu zapewnienie stosowania rozporządzenia 2016/679 zostały uchwalone dopiero 9 miesięcy po rozpoczęciu jego stosowania.

[101] Prezes Urzędu Ochrony Danych Osobowych, dalej: Prezes UODO, jest następcą GIODO (por. art. 166 uodo z 2018 r.).

osobowych. Ponadto uodo z 2018 r. zawiera przepisy wyłączające lub ograniczające stosowanie niektórych przepisów rozporządzenia 2016/679[102], przepisy zmieniające inne ustawy, a także przepisy przejściowe. Zakres przedmiotowy uodo z 2018 r. jest zatem odmienny od zakresu uodo z 1997 r., mimo, że tytuły tych ustaw są identyczne.

4.4 Relacje rozporządzenia 2016/679 z innymi przepisami dotyczącymi danych osobowych

Rozporządzenie 2016/679, choć reguluje ochronę danych osobowych w kompleksowy sposób, to podobnie jak w przypadku przepisów implementujących dyrektywę 95/46, nie wyczerpuje jednak tej problematyki. Wyznacza ogólne ramy prawne przetwarzania danych osobowych i nie może być stosowane w oderwaniu od innych regulacji z dwóch powodów.

Po pierwsze, przepisy dotyczące przetwarzania danych osobowych znajdują się także w innych aktach prawnych, które można uznać za przepisy szczególne. Ze względu na przedmiot niniejszej rozprawy znaczenie ma dyrektywa 2000/31/WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego na rynku wewnętrznym (dyrektywa o handlu elektronicznym)[103] i dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[104] oraz wdrażające je do polskiego porządku prawnego przepisy: odpowiednio ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[105] oraz ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[106]. Zgodnie z art. 1 ust. 1 i 2 dyrektywy 2002/58, jej celem jest harmonizacja przepisów krajowych wymaganych do zapewnienia równoważnego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do prywatności i poufności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej, a także w celu zapewnienia swobodnego przepływu w UE tego typu danych oraz urządzeń i usług łączności elektronicznej. Jej przepisy dookreślają i uzupełniają rozporządzenie 2016/679[107]. Stosunek *lex generalis – lex specialis* pomiędzy rozporządzeniem

[102] Np. art. 2 uodo z 2018 r., który wprowadza wyłączenia dotyczące przetwarzania danych osobowych do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej – co jest dopuszczalne na podstawie klauzuli kompetencyjnej zawartej w art. 85 rozporządzenia 2016/679.
[103] Dz. Urz. UE L 178 z dnia 17.07.2000 r., s. 1–16, dalej jako: dyrektywa 2000/31.
[104] Dz. Urz. UE L 201 z dnia z 31.07.2002 r., s. 37 – 47, dalej jako: dyrektywa 2002/58.
[105] T. j. Dz. U. z 2020 r. poz. 344, dalej jako: uśude. Dyrektywa 2000/31 została wdrożona także poprzez przepisy innych ustaw, w tym kc w zakresie dotyczącym umów zawieranych drogą elektroniczną. Szerzej na ten temat por. K. Chałubińska-Jentkiewicz, J. Taczkowska-Olszewska, *Komentarz do art. 1 uśude*, *Świadczenie usług drogą elektroniczną. Komentarz*, Warszawa 2019, Legalis.
[106] T. j. Dz.U. z 2022 r. poz. 1648 z późn. zm., dalej jako: upt.
[107] W art. 1 ust. 2 dyrektywy 2002/58 mowa wprawdzie o dyrektywie 95/46, lecz zgodnie z art. 94 ust. 2 rozporządzenia 2016/679, odesłania do tej uchylonej dyrektywy należy traktować jako odesłania do rozporządzenia 2016/679.

2016/679 a dyrektywą 2002/58 potwierdza art. 95 rozporządzenia 2016/679 i motyw 173 jego preambuły[108]. Należy też zwrócić uwagę na dyrektywę (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającą procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego[109], gdyż zawiera definicję usługi społeczeństwa informacyjnego.

Konieczne jest też zasygnalizowanie toczących się prac nad nowym aktem prawnym dotyczącym świadczenia usług łączności elektronicznej – projektem rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)[110], tzw. rozporządzenia *ePrivacy.* Co istotne, podobnie jak w przypadku rozporządzenia 2016/679, nastąpić ma zmiana rodzaju aktu prawnego regulującego tę materię – z dyrektywy na rozporządzenie. Zakres przedmiotowy i cele dyrektywy 2002/58 i projektowanego rozporządzenia *ePrivacy* są podobne – przyjęcie nowego aktu prawnego podyktowane jest głównie koniecznością dostosowania go do rozporządzenia 2016/679, ujednolicenia obowiązującego prawa w UE w tej dziedzinie oraz wiąże się ze strategią utworzenia jednolitego rynku cyfrowego. Za najważniejsze zmiany, jakie ma wprowadzić rozporządzenie *ePrivacy*, można uznać objęcie jego zakresem tzw. usług łączności interpersonalnej, np. telefonii internetowej (VoIP), komunikatorów internetowych, poczty elektronicznej, z której korzysta się za pośrednictwem przeglądarki internetowej (*webmail*), a także komunikacji w ramach tzw. internetu rzeczy (*Internet of Things*, IoT)[111]. Projekt rozporządzenia *ePrivacy* nie zawiera przepisów dotyczących danych osobowych dzieci. Miało ono wejść w życie równocześnie z rozporządzeniem 2016/679. Mimo, że KE przedłożyła wniosek prawodawczy w 2017 r., wciąż nie zanosi się na szybkie zakończenie procesu legislacyjnego, co zasługuje na krytykę, gdyż oddziałuje negatywnie na skuteczność całej reformy ochrony danych osobowych. W opinii EROD rozporządzenie *ePrivacy* powinno zostać przyjęte jak najszybciej[112].

---

[108] EROD, *Opinia 5/2019 w sprawie wzajemnej zależności między dyrektywą o prywatności i łączności elektronicznej a RODO, w szczególności w zakresie właściwości, zadań i uprawnień organów ochrony danych* przyjęta 12 marca 2019 r., https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_pl.pdf (dostęp: 23.09.2020), s. 12.

[109] Dz. Urz. UE L 241 z dnia 17.09.2015 r., s. 1–15, dalej jako: dyrektywa 2015/1535.

[110] Wniosek Komisji Europejskiej z dnia 10.01.2017 r. „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)", COM/2017/010 final - 2017/03 (COD), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A52017PC0010 (dostęp: 23.09.2020).

[111] X. Konarski, *Rozporządzenie o e-Prywatności jako regulacja sektorowa względem ogólnego rozporządzenie o ochronie danych osobowych (RODO)*, „Monitor Prawniczy" dodatek: *Wdrażanie ogólnego rozporządzenia…*, s. 8.

[112] EROD, *Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB* Adopted on 19 November 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201119_eprivacy_regulation_en.pdf (dostęp: 23.09.2020).

Po drugie, przepisy sektorowe, choć często nie odnoszą się *expressis verbis* do ochrony danych osobowych, także jej dotyczą, np. gdy określają zakres informacji, które mogą być zbierane o osobach fizycznych, sposób i czas przechowywania dokumentów zawierających dane osobowe – choć jest to szczególnie widoczne na przykładzie przepisów regulujących działanie podmiotów publicznych, dotyczy także prywatnych[113].

5. Dane osobowe i ich przetwarzanie na gruncie rozporządzenia 2016/679

5.1 Pojęcie danych osobowych

Pojęcie danych osobowych ma fundamentalne znaczenie na gruncie przepisów o ich ochronie. Mimo, że posiada definicję legalną, a jej brzmienie w wyniku reformy ochrony danych osobowych nie uległo znaczącym zmianom i większość rozważań poczynionych na gruncie uodo z 1997 r. pozostaje aktualna, wciąż powoduje wiele wątpliwości interpretacyjnych.

Zgodnie z art. 4 pkt 1 rozporządzenia 2016/679, dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Możliwą do zidentyfikowania osobą fizyczną jest osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Danymi osobowymi są zatem informacje o konkretnym człowieku. Nie stanowią więc danych osobowych informacje anonimowe lub zanonimizowane[114], a także dotyczące osób prawnych, zwłaszcza przedsiębiorstw, w tym dane o firmie i formie prawnej oraz dane kontaktowe osoby prawnej[115].

Posłużenie się przez prawodawcę unijnego zwrotem „wszelkie informacje"[116] przy definiowaniu danych osobowych – zarówno w dyrektywie 95/46, jak i następnie w rozporządzeniu

[113] Np. art. 74 ust. 2 pkt 4 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2019 r. poz. 351 z późn. zm.) nakłada obowiązek przechowywania dowodów księgowych (zawierających, co do zasady, m.in. określenie stron dokonujących operacji gospodarczej), które dotyczącą środków trwałych w budowie, pożyczek, kredytów oraz umów handlowych, roszczeń dochodzonych w postępowaniu cywilnym lub objętych postępowaniem karnym albo podatkowym przez 5 lat od początku roku następującego po roku obrotowym, w którym operacje, transakcje i postępowanie zostały ostatecznie zakończone, spłacone, rozliczone lub przedawnione. Ten przepis ma zatem wpływ na ustalenie właściwego z perspektywy zasad ochrony danych osobowych wynikających z rozporządzenia 2016/679 czasu przechowywania danych osobowych zawartych w ww. dowodach księgowych.

[114] Motyw 26 preambuły rozporządzenia 2016/679.

[115] Motyw 14 preambuły rozporządzenia 2016/679.

[116] Warto zauważyć, że wyraz „wszelkie" pojawił się w definicji danych osobowych w polskiej wersji językowej rozporządzenia 2016/679 w wyniku sprostowania z dnia 23 maja 2018 r. (Dz. Urz. UE L 127 z 23.05.2018, s. 2), a zatem na dwa dni przed rozpoczęciem stosowania nowych przepisów. Przyczyn zmiany można upatrywać w błędnym tłumaczeniu definicji na język polski (pomięciu jednego wyrazu), ponieważ inne wersje językowe od początku wskazywały na szerokie rozumienie pojęcia danych osobowych, np. w j. angielskim – *'personal data' means any information relating to an identified or identifiable natural person*, w j. niemieckim – *„personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person,* w j. francuskim - *«données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable*.

2016/679 – przesądza o szerokim rozumieniu tego pojęcia, odzwierciedlając taki właśnie zamiar unijnego prawodawcy[117]. Do uznania informacji za dane osobowe bez znaczenia jest więc to, w jakiej formie są utrwalone lub na jakim nośniku się znajdują, co nie budziło wątpliwości także przed reformą ochrony danych osobowych. Grupa Robocza Art. 29 w Opinii nr 4/2007 w sprawie pojęcia danych osobowych wyjaśniła, że są nimi „informacje dostępne w jakiejkolwiek formie, na przykład alfabetycznej, liczbowej, graficznej, fotograficznej lub akustycznej. Obejmuje ono informacje zapisane na papierze oraz informacje zapisane w pamięci komputerowej za pomocą kodu dwójkowego, lub też na przykład na kasecie wideo"[118].

Relacje między pojęciem danych i informacji były przedmiotem zainteresowania przedstawicieli doktryny już na gruncie uodo z 1997 r.[119], w której również zdefiniowano dane osobowe poprzez odniesienie do informacji o osobie fizycznej. W literaturze zwracano uwagę, że pojęcie informacji jest odmiennie rozumiane w różnych dziedzinach, takich jak filozofia czy informatyka, co utrudnia prowadzenie badań, a także stosowanie przepisów o ochronie danych osobowych, dlatego pożądane byłoby podjęcie próby interdyscyplinarnego uzgodnienia definicji[120]. Na płaszczyźnie rozporządzenia 2016/679 zamienne używanie pojęcia danych i informacji jest jednak uprawnione – postępuje tak sam prawodawca unijny. Można uznać to za pewne uproszczenie, które jednak nie jest błędem[121].

Zgodnie z Opinią Grupy Roboczej Art. 29 nr 4/2007 w sprawie pojęcia danych osobowych, informacja nie musi być prawdziwa ani sprawdzona, by mogła być uznana za dane osobowe. Jeśli dane byłyby nieprawdziwe lub niepełne, osobie, której dane dotyczą, przysługuje prawo do ich sprostowania. Do danych osobowych należy więc zakwalifikować także opinie i oceny, np. „Tytus jest dobrym pracownikiem i zasługuje na awans"[122]. To stanowisko potwierdził także TSUE, stwierdzając w wyroku w sprawie C-434/16, że dane osobowe obejmują informacje „zarówno obiektywne, jak i subiektywne, w postaci opinii czy oceny, a jedynym warunkiem, które muszą one spełniać, jest to, aby „dotyczyły" danej osoby. Warunek ten jest zaś spełniony, gdy ze względu na swą treść, cel czy skutek dana informacja jest powiązana z daną osobą"[123]. Taka interpretacja zasługuje na aprobatę. Uznanie informacji za dane osobowe bez względu na to, czy są prawdziwe

[117] Wyrok TSUE z dnia 20 grudnia 2017 r. w sprawie C-434/16, Peter Nowak przeciwko Data Protection Commissioner.
[118] Opinia Grupy Roboczej Art. 29 nr 4/2007 w sprawie pojęcia danych osobowych, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pl.pdf, s. 7 (dostęp: 25.06.2020).
[119] G. Szpor, *Pojęcie informacji a zakres ochrony danych osobowych*, [w:] P. Fajgielski (red.), *Ochrona danych osobowych w Polsce…*, s. 15-19 i tam powołana literatura.
[120] Tamże.
[121] P. Fajgielski, *Ogólne rozporządzenie…*, s. 104.
[122] Opinia Grupy Roboczej Art. 29 nr 4/2007…, s. 6.
[123] Wyrok TSUE z dnia 20 grudnia 2017 r. w sprawie C-434/16, P. Nowak przeciwko Data Protection Commissioner, http://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0 &doclang=PL&mode=lst&dir=&occ=first&part=1&cid=8883772 (dostęp: 25.06.2020).

czy nie, ma szczególne znaczenie w przypadku zautomatyzowanego podejmowania decyzji wpływających na sytuację osoby fizycznej, w tym profilowania, oraz coraz szerszego zastosowania algorytmów i tzw. sztucznej inteligencji[124], ponieważ w określonych sytuacjach pozwala na weryfikację decyzji podjętej z wykorzystaniem tych narzędzi dzięki środkom ochrony przewidzianym przez rozporządzenie 2016/679.

Wymieniony w art. 4 pkt 1 katalog danych osobowych ma charakter otwarty, ponieważ uznanie informacji za dane osobowe jest uwarunkowane rozwojem technicznym, możliwościami przetwarzania, które – choć być może nie są jeszcze znane lub nie są stosowane na szeroką skalę – mogą pojawić się w każdej chwili, a także kontekstem przetwarzania. Oprócz typowych informacji, zazwyczaj pozwalających na identyfikację osoby fizycznej, takich jak imię i nazwisko czy numer identyfikacyjny, np. PESEL, za dane osobowe może być uznana niemal każda informacja posiadająca cechy określone w art. 4 pkt 1 rozporządzenia 2016/679, nawet taka, która wykracza poza ramy potocznego rozumienia personaliów. Taką linię orzeczniczą konsekwentnie utrzymuje TSUE, stwierdzając przykładowo, że pojęcie danych osobowych „odnosi się bez wątpienia do nazwiska osoby w połączeniu z jej numerem telefonu lub informacjami dotyczącymi jej warunków pracy czy sposobów spędzania przez nią wolnego czasu”[125]. Za dane osobowe TSUE uznał także pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu zawodowego i naniesione przez egzaminatora komentarze odnoszące się do tych odpowiedzi[126] oraz – z perspektywy dostawcy usług medialnych – dynamiczny adres IP[127]. Warto również przytoczyć przykłady danych osobowych podane przez Grupę Roboczą Art. 29 w wytycznych dotyczących prawa do przenoszenia danych osobowych, o którym mowa w art. 20 rozporządzenia 2016/679[128]. Omawiając zakres zastosowania tego uprawnienia i okoliczności, w których może wystąpić jego realizacja, Grupa Robocza Art. 29 wskazuje jako przykład danych osobowych listę odtwarzania (lub historię słuchanych utworów) z serwisu strumieniowej transmisji muzyki, listę kontaktów z poczty elektronicznej, informacje na temat zakupów dokonanych przy użyciu różnych kart lojalnościowych, wykaz dokonanych transakcji bankowych, tytuły książek kupionych w księgarni internetowej, rejestry połączeń telefonicznych, a ponadto dane pozyskane w wyniku obserwacji działań użytkowników związanych z korzystaniem z urządzeń, takich jak

[124] Por. L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa 2020.
[125] Wyrok TSUE z dnia 6 listopada 2003 r. w sprawie C-101/01, Bodil Lindqvist.
[126] Wyrok TSUE z dnia 20 grudnia 2017 r. w sprawie C-434/16, Peter Nowak przeciwko Data Protection Commissioner.
[127] Wyrok TSUE z dnia 19 października 2016 r. w sprawie C-582/14, Patrick Breyer przeciwko Bundesrepublik Deutschland.
[128] Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia danych*, przyjęte w dniu 5 kwietnia 2017 r., https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 (dostęp: 25.06.2020), s. 5-12.

„inteligentne" liczniki lub inne rodzaje „połączonych obiektów"[129]. Do takich danych osobowych mogą, zgodnie z wytycznymi, zaliczać się: historia wyszukiwania danej osoby, dane o ruchu i dane dotyczące lokalizacji, tętno monitorowane za pośrednictwem urządzenia do noszenia na ciele[130]. Nie można jednak postawić tezy, że np. lista odtwarzanych utworów muzycznych zawsze pozwala na zidentyfikowanie osoby fizycznej, a zatem że w każdym przypadku stanowi dane osobowe. O ile z perspektywy dostawcy usługi strumieniowej transmisji muzyki taka informacja pozwala pewnie na ustalenie tożsamości jego klienta, o tyle sama lista, udostępniona innemu podmiotowi bez wskazania, przez kogo została utworzona, będzie stanowić zwykłą listę utworów, nie dając prawdopodobnie nawet potencjalnej możliwości ustalenia tożsamości jej „autora". Podobnie w przypadku popularnych imion i nazwisk – bez dodatkowych informacji konkretyzujących, o kogo chodzi, ustalenie tożsamości może być bardzo trudne lub wręcz niemożliwe[131]. Wydaje się więc, że największe trudności w ocenie, czy informacja stanowi dane osobowe, powoduje tzw. przesłanka identyfikowalności[132]. Dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (*identified or identifiable natural person*). Wskazuje to na niezbędność istnienia rzeczowego związku pomiędzy osobą fizyczną a informacjami[133]. Wyraz „zidentyfikować" oznacza ustalić tożsamość kogoś lub czegoś[134]. Przez zidentyfikowanie osoby fizycznej można zatem rozumieć powiązanie informacji z konkretnym człowiekiem, którego ona dotyczy. Zgodnie z motywem 26 rozporządzenia 2016/679, analizując możliwość zidentyfikowania osoby fizycznej „należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny". Analiza, czy dana informacja może prowadzić do identyfikacji osoby fizycznej,

[129] Czyli urządzeń elektronicznych mogących automatycznie komunikować się i wymieniać dane za pomocą internetu, określanych także jako „internet rzeczy", *Internet of things – IoT*.
[130] Tzw. „technologie ubieralne" – *wearable devices* – np. smartwatche.
[131] P. Fajgielski, *Ogólne rozporządzenie…*, s. 110.
[132] Problem ten występował także na gruncie dyrektywy 95/46, ponieważ zawarta w niej definicja danych osobowych również odwoływała się do „zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej". Z tego powodu dorobek naukowy i orzeczniczy, wypracowany przed reformą ochrony danych osobowych, nie utracił aktualności i jest przydatny do interpretacji pojęcia danych osobowych w rozporządzeniu 2016/679.
[133] A. Drozd, *Pojęcie danych osobowych – uwagi wstępne*, [w:] Fajgielski P. (red.), *Ochrona danych osobowych w Polsce…*, s. 24.
[134] *Internetowy słownik języka polskiego PWN*, https://sjp.pwn.pl/sjp/zidentyfikowac;2545998.html (dostęp: 25.06.2020).

powinna zatem w każdym przypadku być poprzedzona ustaleniem kontekstu, w jakim będzie ona występować; kręgu podmiotów, który będzie mógł się z nią zapoznać; sposobów (technik), jakie będą wykorzystywane – z uwzględnieniem, że mogą się one zmieniać w czasie wraz z postępem technologicznym. Zjawisko to – określane mianem relatywizacji pojęcia danych osobowych[135] – polega na tym, że ta sama informacja może być uznana lub nie za dane osobowe, w zależności od tego, jaki podmiot nią dysponuje i czy przykładowo posiada on inne informacje, dzięki którym – dopiero po ich połączeniu – zidentyfikuje osobę fizyczną. Zgodnie z podejściem subiektywnym „Istotne jest to, czy podmiot mający dostęp do danych ma możliwość posłużenia się nimi w ramach własnych środków w celu identyfikacji danej osoby"[136]. Z kolei podejście obiektywne (zwane też absolutnym) zakłada, że informację należy zaliczyć do danych osobowych, jeżeli identyfikacja osoby fizycznej jest możliwa po połączeniu tej informacji z inną, dostarczoną przez odrębny podmiot[137]. Zdaniem P. Litwińskiego, na gruncie rozporządzenia 2016/679 uprawnione jest kierowanie się subiektywnym podejściem w interpretacji pojęcia danych osobowych, ponieważ, zgodnie z powołanym wyżej motywem 26, należy brać pod uwagę nie tylko wszelkie rozsądnie prawdopodobne sposoby, jakimi można się posłużyć w celu identyfikacji – tak jak w poprzednim stanie prawnym – ale również czy istnieje uzasadnione prawdopodobieństwo, iż zostaną one wykorzystane w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej[138]. Wbrew pozorom odmienne stanowisko – przy i tak bardzo szerokiej definicji danych osobowych – mogłoby doprowadzić do obniżenia poziomu ich ochrony. Prawo dotyczące danych osobowych, wymagające zapewnienia przewidzianej w nim ochrony w przypadku niemal każdej informacji, bez względu na okoliczności czy kontekst sytuacji, w jakiej jest ona wykorzystywana, w praktyce może okazać się wręcz niemożliwe do stosowania, a w rezultacie ignorowane czy wręcz dyskredytowane[139]. Nie mniej jednak istniejące trudności w interpretacji pojęcia danych osobowych, których nie niweluje stosowanie subiektywnego podejścia, a tylko w pewnym stopniu je ogranicza, mogą powodować obniżenie poziomu ochrony, ponieważ duży margines oceny może skutkować umyślnym bądź nieumyślnym (wynikającym po prostu z błędnej oceny)

[135] W. Zimny, *Praktyczne skutki nowelizacji ustawy o ochronie danych osobowych z dnia 25 sierpnia 2001 r.*, „Ochrona danych osobowych. Biuletyn ABI" 2001, nr 21, cyt. za: P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis.
[136] Opinia rzecznika generalnego M. Camposa Sáncheza-Bordony z dnia 12.05.2016 r. w sprawie C-582/14, Patrick Breyer przeciwko Bundesrepublik Deutschland.
[137] Tamże.
[138] P. Litwiński, *Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – glosa do wyroku Trybunału Sprawiedliwości z 19.10.2016 r. w sprawie C-582/14 Patrick Breyer*, „Europejski Przegląd Sądowy" 2017, nr 5.
[139] N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, „Law, Innovation and Technology" 2018, vol. 10, nr 1, s. 41. N. Purtova uważa jednak, że głównym źródłem tego ryzyka nie jest szeroka definicja danych osobowych, lecz niewielkie zróżnicowanie obowiązków związanych z ochroną danych osobowych w zależności od uwarunkowań ich przetwarzania.

niezastosowaniem przepisów o ochronie danych osobowych, a tym samym ograniczeniem lub pozbawieniem osób fizycznych przysługujących im praw.

5.2 Szczególne kategorie danych osobowych

Ochrona przewidziana w rozporządzeniu 2016/679 obejmuje co do zasady wszystkie dane osobowe. Jednak niektóre kategorie danych osobowych zasługują na bardziej intensywną ochronę, ponieważ potencjalne naruszenie związane z ich przetwarzaniem może skutkować ingerencją nie tylko w sferę prywatności, lecz także intymności i powodować bardziej doniosłe konsekwencje dla osoby, której dotyczą[140]. Ponadto w przypadku niektórych danych osobowych ich przetwarzanie może rodzić ryzyko dyskryminacji, co jest zasygnalizowane kilkukrotnie w motywach preambuły rozporządzenia 2016/679[141]. Wobec tego prawodawca unijny wyodrębnił w ramach danych osobowych dane należące do szczególnych kategorii i wprowadził zakaz ich przetwarzania, który może być uchylony wyłącznie, jeśli zostanie spełniony dodatkowy warunek (gdy wystąpi przynajmniej jedna z przesłanek z art. 9 ust. 2 rozporządzenia 2016/679) powodujący, że przetwarzanie będzie dopuszczalne. Jednak nawet w takim przypadku konieczne jest zadośćuczynienie dodatkowym obowiązkom związanym z przetwarzaniem danych należących do tej kategorii. Podział na tzw. dane osobowe zwykłe i tzw. dane wrażliwe nie jest jednak doskonały, co podnoszono już pod rządami uodo z 1997 r. Niekiedy przetwarzanie informacji związanych przykładowo z sytuacją ekonomiczną danej osoby może z większym prawdopodobieństwem narazić ją na negatywne konsekwencje, niż w przypadku przetwarzania informacji o tym, że cieszy się dobrym zdrowiem[142].

W myśl art. 9 ust. 1 rozporządzenia 2016/679, do szczególnych kategorii danych osobowych zaliczają się dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej. Warto podkreślić, że zamknięty jest katalog kategorii danych objętych szczególną ochroną, lecz sam katalog informacji – tak jak w przypadku wszystkich danych osobowych – pozostaje otwarty. Stwierdzenie, czy konkretna informacja objęta jest szczególnym reżimem ochrony, musi być zatem poprzedzone zakwalifikowaniem jej do odpowiedniej kategorii. Dokonanie tej oceny może powodować wiele trudności. Po pierwsze, nie wszystkie z rodzajów danych wymienionych w art. 9 ust. 1

[140] P. Fajgielski, *Przetwarzanie szczególnych kategorii danych w świetle ogólnego rozporządzenia o ochronie danych*, [w:] K. Czaplicki, G. Szpor (red.), *Internet. Przetwarzanie danych…*, Legalis.
[141] Patrz motyw 71, 75, 85 preambuły rozporządzenia 2016/679.
[142] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, s. 486.

rozporządzenia 2016/679, zostały zdefiniowanie przez prawodawcę. Po drugie, nawet w przypadku tych, które posiadają definicje legalne – czyli danych dotyczących zdrowia, danych genetycznych, danych biometrycznych – zastosowanie ich w konkretnym stanie faktycznym wciąż wymaga interpretacji przez pryzmat pojęcia danych osobowych i wszystkich elementów składowych jego definicji[143].

5.2.1 Szczególne kategorie danych osobowych posiadające definicje legalne

Dane dotyczące zdrowia, stosownie do definicji zawartej w art. 4 pkt 15 rozporządzenia 2016/679, oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia. To pojęcie należy rozumieć bardzo szeroko. Nie ulega wątpliwości, że do danych dotyczących zdrowia zaliczyć można na przykład wyniki badań laboratoryjnych, informacje o przebytych chorobach, niepełnosprawności. Ciekawych wskazówek interpretacyjnych dostarcza motyw 35 preambuły rozporządzenia 2016/679. Wyjaśniono w nim, że danymi dotyczącymi zdrowia są informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Dla przykładu, do danych dotyczących stanu zdrowia Prezes UODO zalicza informacje o już zrealizowanych świadczeniach medycznych oraz receptach na lekarstwa[144], co ujawnia stan zdrowia danej osoby w przeszłości (a dodatkowo może ujawniać także aktualny, zwłaszcza w przypadku chorób przewlekłych).

Przez informacje o przyszłym stanie zdrowia można z kolei rozumieć, czytając dalszą część motywu 35 preambuły rozporządzenia 2016/679, dane o ryzyku choroby. Te informacje mogą być z kolei wynikiem oceny lekarza przeprowadzonej na podstawie zgromadzonych informacji o pacjencie lub – w przypadku wyłącznie zautomatyzowanego przetwarzania danych osobowych w celu oceny ryzyka – profilowania w rozumieniu art. 4 pkt 4 rozporządzenia 2016/679. W motywie 35 podkreślono także, że do danych dotyczących stanu zdrowia zalicza się informacje zbierane w celu rejestracji i świadczenia usług opieki zdrowotnej zgodnie z dyrektywą Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej[145], na której implementację do polskiego porządku prawnego składa się w sumie kilkanaście aktów prawnych. Wśród nich przede wszystkim warto wymienić ustawę z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[146],

[143] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 9 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…,* Legalis.
[144] Decyzja Prezesa UODO z dnia 12 kwietnia 2019 r., ZSZZS.440.672.2018, https://uodo.gov.pl/decyzje/ZSZZS.440.672.2018 (dostęp: 07.09.2020).
[145] Dz. Urz. UE L 2011 Nr 88, str. 45
[146] T. j. Dz.U. z 2020 r. poz. 849.

która określa m.in. zawartość dokumentacji medycznej i zasady jej udostępniania. Ochrona danych osobowych dotyczących zdrowia, przetwarzanych w szczególności przez podmioty prowadzące działalność leczniczą, jest przedmiotem opracowań poświęconych niekiedy w całości tej tematyce[147].

Przed reformą ochrony danych osobowych nie istniała legalna definicja danych osobowych genetycznych, choć nie oznacza to, że dane genetyczne nie były objęte ochroną[148] lub ta problematyka nie była przedmiotem analiz[149]. Dane genetyczne zostały zdefiniowane w art. 4 pkt 13 rozporządzenia 2016/679 i oznaczają dane osobowe dotyczące 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 pochodzącej od tej osoby fizycznej. Brzmienie tego przepisu świadczy o tym, że katalog źródeł danych genetycznych jest otwarty. Oznacza to, że próbka nie musi pochodzić wyłącznie od tej osoby (a może np. od osób z nią spokrewnionych), a także, że materiał poddawany analizie nie musi stanowić próbki genetycznej, lecz mogą nim być przykładowo wnioski z uprzednio przeprowadzonych badań[150]. W motywie 34 preambuły rozporządzenia 2016/679 wskazano, że dane genetyczne mogą wynikać z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA), kwasu rybonukleinowego (RNA) lub innych elementów umożliwiających pozyskanie równoważnych informacji. Dopuszczenie różnych źródeł danych genetycznych zasługuje na aprobatę, ponieważ w związku z dynamicznym rozwojem nauki trudno przewidzieć i opracować zamknięty katalog informacji czy też nośników, z których możliwe jest pozyskanie danych genetycznych, a pominięcie ich przez prawodawcę mogłoby skutkować powstaniem luki wpływającej ujemnie na prawa osób, których dane dotyczą. Warto zauważyć, że informacje

[147] Por. M. Jackowski (red.), *Ochrona danych medycznych. RODO w ochronie zdrowia*, Warszawa 2018; K. Andres, E. Bielak-Jomaa, M. Jagielski, P. Kawczyński, M. Krasińska, P. Litwiński, A. Sieradzka, K. Wojsyk, *Ochrona danych osobowych medycznych*, wyd. 2, Warszawa 2018; B. Marcinkowski, *Ochrona danych osobowych pacjenta w telemedycynie w świetle RODO*, [w:] I. Lipowicz, G. Szpor, M. Świerczyński (red.), *Telemedycyna i e-Zdrowie. Prawo i informatyka*, Warszawa 2019.

[148] W uodo z 1997 r. w art. 27 ust. 1, będącym odpowiednikiem art. 9 ust. 1 rozporządzenia 2016/679 – czyli przepisie określającym katalog danych objętych szczególną ochroną – wymieniono „dane o kodzie genetycznym". Co ciekawe, polski ustawodawca rozszerzył w ten sposób katalog tego rodzaju danych w stosunku do regulacji zawartej w art. 8 ust. 1 dyrektywy 95/46. W literaturze zaprezentowano pogląd, że dane genetyczne mieszczą się w pojęciu danych o stanie zdrowia – por. T. Wyka, *Granice pozyskiwania danych osobowych dotyczących zdrowia pracownika*, [w:] A. Nerka, T. Wyka (red.), *Granice ochrony danych osobowych w stosunkach pracy*, Warszawa 2009, s. 93. Z kolei argumenty przemawiające za wyodrębnieniem danych o kodzie genetycznym jako oddzielnej kategorii przedstawił A. Mednis w komentarzu do art. 27 uodo z 1997 r. trafnie wskazując, że „informacja genetyczna ujawnia nie tylko stan zdrowia osoby, ale także inne dane, np. skłonności osoby do określonych zachowań, w tym zachowań przestępczych" (A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999, Lex).

[149] Por. Grupa Robocza Art. 29, *Working Document on Genetic Data*, przyjęty 17.03.2004, WP 91, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf (dostęp: 07.09.2020).

[150] B. Fischer, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.

zaliczające się do danych genetycznych mogą jednocześnie stanowić desygnaty pojęcia danych dotyczących zdrowia.

Biometria, rozumiana jako specjalna technika, za pomocą której dokonuje się pomiaru określonych cech osobniczych – fizycznych, fizjologicznych, behawioralnych – wykorzystywana jest co do zasady w celu identyfikacji lub weryfikacji tożsamości osoby. Pomiar cech fizycznych i fizjologicznych może dotyczyć przykładowo kształtu i układu linii papilarnych palca, obrazu tęczówki lub siatkówki oka, kształtu i rysów twarzy, zapachu ciała, zaś w przypadku cech behawioralnych – dynamiki pisania na klawiaturze, sposobu poruszania się[151]. Po pobraniu próbki biometrycznej, którą może być zatem np. odcisk palca czy nagranie głosu, odczytuje się z niej, za pomocą specjalnego systemu, informacje biometryczne. Następnie system, porównując je z wcześniej przypisanymi konkretnym osobom wzorcami biometrycznymi, weryfikuje ich tożsamość. Jest to więc proces polegający na automatycznej analizie i interpretacji danych[152]. Niekiedy w celu zwiększenia pewności wyniku (dokładności i skuteczności), wykorzystuje się jednocześnie różne techniki biometryczne i przynajmniej dwie cechy dotyczące tej samej osoby – mowa wtedy o biometrii multimodalnej, zwanej także wielopoziomową[153].

Dane biometryczne zostały po raz pierwszy zdefiniowane na gruncie przepisów o ochronie danych osobowych w rozporządzeniu 2016/679. Zgodnie z art. 4 pkt 14, oznaczają one dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby. Jako przykłady danych biometrycznych wskazano w tym przepisie wizerunek twarzy i dane daktyloskopijne. Jednak nie w każdym przypadku dysponowanie wizerunkiem twarzy, utrwalonym np. na zdjęciu, będzie oznaczało, że ma się do czynienia z danymi biometrycznymi, objętymi intensywniejszą ochroną z racji zaliczenia ich do szczególnych kategorii danych osobowych. Wyjaśnia to motyw 51 rozporządzenia 2016/679, w którym stwierdzono, że fotografie są objęte powyższą definicją wyłącznie wtedy, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości. Wspominany w motywie 51 wizerunek twarzy i fotografię należy potraktować tylko jako przykład pomagający rozróżnić sytuacje, w których – w zależności od celu przetwarzania i stosowanej techniki – te same dane osobowe mogą stanowić tzw. dane zwykłe lub dane należące do szczególnych kategorii. Wyróżnia się zatem trzy elementy

[151] Informacja Generalnego Inspektora Ochrony Danych Osobowych o zagrożeniach płynących z upowszechnienia danych biometrycznych w kontaktach obywateli z instytucjami publicznymi i prywatnymi, przyjęta w czerwcu 2017 r., https://archiwum.giodo.gov.pl/pl/file/12478 (dostęp: 07.09.2020), s. 4.

[152] M. Bąba, *Próba wyznaczenia zakresu pojęcia danych biometrycznych*, „Prawo Mediów Elektronicznych" 2016, nr 2, s. 30.

[153] Grupa Robocza Art. 29, *Opinia nr 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych*, przyjęta w dniu 27 kwietnia 2012 r., WP193, https://archiwum.giodo.gov.pl/pl/file/5337 (dostęp: 07.09.2020), s. 6.

definicji danych biometrycznych, które powinny zaistnieć łącznie, by można było zakwalifikować informację do tej grupy: 1) charakter danych – czy dotyczą one cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej; 2) stosowane środki i sposoby przetwarzania – czy są wykorzystywane specjalne techniki; 3) cel przetwarzania – czy jest nim jednoznaczna identyfikacja osoby fizycznej[154]. Kryterium przetwarzania w celu jednoznacznego zidentyfikowania osoby fizycznej zostało wskazane także w art. 9 ust. 1 rozporządzenia 2016/679[155]. Dlatego nawet w przypadku stosowania specjalnych technik w przetwarzaniu danych dotyczących cech fizycznych, fizjologicznych lub behawioralnych, lecz bez wykorzystywania pozyskanych w ten sposób informacji do zidentyfikowania konkretnych osób fizycznych, nie dochodzi do przetwarzania szczególnych kategorii danych osobowych. Taka sytuacja może mieć miejsce, gdy celem przetwarzania jest „odróżnienie jednej kategorii osób od innej, ale nie jednoznaczne zidentyfikowanie danej osoby"[156] według określonego kryterium, np. płci.

W ostatnich latach można zaobserwować wzrost zainteresowania technikami biometrycznymi, a obszary, w których znajdują zastosowanie, stale się powiększają – przede wszystkim o usługi, z których korzysta się w codziennych sytuacjach (np. uwierzytelnienie właściciela telefonu poprzez odcisk linii papilarnych, zamiast podania przez niego hasła składającego się z kilku cyfr; automatyczne rozpoznawanie twarzy na zdjęciach opublikowanych w portalach społecznościowych). Mimo zalet związanych z identyfikacją biometryczną, takich jak np. brak konieczności zapamiętywania wielu haseł, stwarza ona poważne ryzyko dla praw i wolności osób, których dane są wykorzystywane w tym celu, zwłaszcza, jeśli podmiot zobowiązany do właściwego zabezpieczenia danych osobowych nie zdaje sobie sprawy z faktu przetwarzania danych biometrycznych, nie zagłębiając się w techniczne aspekty takich operacji[157].

Do najbardziej poważnych zagrożeń związanych z przetwarzaniem danych biometrycznych może należeć ryzyko pozyskania danych w szerszym zakresie, niż jest to niezbędne do identyfikacji osoby fizycznej i dalsze wykorzystanie tych informacji bez jej wiedzy w zupełnie innych celach (np. marketingowych) i poprzez inne operacje przetwarzania (np. profilowanie). W literaturze opisano przypadki badania poziomu satysfakcji klienta poprzez

[154] EROD, *Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo*, wersja 2.0 przyjęte w dniu 29 stycznia 2020 r., https://edpb.europa.eu/our-work-tools/our-documents/pokyny/guidelines-32019-processing-personal-data-through-video-devices_en (dostęp 07.09.2020), s. 19-20.

[155] Fragment tego przepisu, odnoszący się do danych biometrycznych, brzmi: „zabrania się przetwarzania (…) danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej (…)".

[156] EROD, *Wytyczne 3/2019…*, s. 19-20.

[157] Prezes UODO nałożył administracyjną karę pieniężną w wysokości 20 tys. zł na szkołę podstawową, w której pobierano odciski palców dzieci i wykorzystywano identyfikację biometryczną w celu weryfikacji uiszczenia opłaty za posiłek wydawany w szkolnej stołówce. Szkoła w swoich wyjaśnieniach podniosła, że „nie posiada żadnego zbioru, który zawierałby obrazy linii papilarnych dzieci. Dane związane z czytnikiem na odcisk palca gromadzone są tylko w samym czytniku w postaci zapisu ciągu bajtów" (decyzja Prezesa UODO z dnia 18 lutego 2020 r., ZSZZS.440.768.2018, https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018, dostęp 07.09.2020).

techniki automatycznego rozpoznawania mimiki twarzy[158]. Wykorzystywanie metod biometrycznych w celu poszukiwania innych cech niż unikalne dla danej osoby określa się jako tzw. *soft biometrics*[159]. Ponadto bezpieczeństwo systemów uwierzytelniania opartych na metodach biometrycznych jest iluzoryczne. Po pierwsze, informacje biometryczne z natury rzeczy nie są chronione przed dostępem innych osób – ich pozyskanie okazuje się stosunkowo łatwe[160]. Po drugie, nie można uznać metod uwierzytelnienia opartych wyłącznie na technikach biometrycznych za „silne" i odpowiednie w przypadku dostępu do systemów, w których przetwarzane są dane osobowe, ponieważ zgodnie z aktualną wiedzą techniczną za takie uważa się metody bazujące przynajmniej na dwóch czynnikach (tzw. uwierzytelnianie dwuskładnikowe – tymi składnikami mogą być przykładowo: hasła, tokeny bezpieczeństwa, USB z tajnym tokenem)[161]. Okazuje się także, że możliwe jest częściowe odtworzenie z wzorca biometrycznego źródłowych danych biometrycznych, a to z kolei może być wystarczające do identyfikacji danej osoby przez inny system biometryczny niż ten, w którym dane były pierwotnie przetwarzane[162], poza kontrolą osoby, której dane dotyczą.

Mając na względzie powyższe zagrożenia, a także fakt, że niektóre mogą być obecnie trudne do przewidzenia, zdefiniowanie w przepisach o ochronie danych osobowych pojęcia danych biometrycznych i zamiar objęcia ich szczególną ochroną zasługuje na aprobatę. Identyfikacja biometryczna, co należy zdecydowanie podkreślić, opiera się m.in. na cechach trwałych, tzn. takich, które co do zasady towarzyszą człowiekowi przez całe życie[163] i których nie może zmienić, dlatego nie należy traktować danych biometrycznych jak każdych innych informacji, za pomocą których można np. uzyskać dostęp do określonej usługi lub miejsca, np. hasła. Definicja danych biometrycznych powstała na gruncie wcześniej wypracowanych koncepcji i przeanalizowanych problemów[164] i w swojej konstrukcji zawiera niezbędne elementy (określa

---

[158] M. R. González-Rodríguez, M. C. Díaz-Fernández, C. Pacheco Gómez, *Facial-expression recognition: An emergent approach to the measurement of tourist satisfaction through emotions*, „Telematics and Informatics" 2020, nr 51.

[159] EIOD, Agencia Española de Protección de Datos, *14 misunderstandings with regard to biometric identification and authentication*, https://edps.europa.eu/data-protection/our-work/publications/papers/14-misunderstandings-regard-biometric-identification_en (dostęp: 07.09.2020).

[160] Okazuje się, że zabezpieczenia dostępu do urządzeń takich jak telefony za pomocą metod biometrycznych mogą być dość łatwo przełamane, o czym informowano w mediach, opisując np. możliwość wykorzystania dobrej jakości zdjęcia twarzy w celu odblokowania telefonu. Niderlandzka organizacja *Consumenten bond* przeprowadziła w 2019 r. test, w którym okazało się to możliwe w przypadku 26 z 60 testowanych urządzeń (https://www.consumentenbond.nl/veilig-internetten/gezichtsherkenning-te-hacken, dostęp: 07.09.2020).

[161] ENISA, *Guidelines for SMEs on the security of personal data processing*, https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing (dostęp 07.09.2020), s. 40.

[162] EIOD, Agencia Española de Protección de Datos, *14 misunderstandings…* .

[163] D. Lubasz, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, P. Makowski, K. Witkowska-Nowakowska, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, Lex.

[164] Grupa Robocza Art. 29, *Working document on biometrics*, przyjęty w dniu 01.08.2003, WP 80, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf (dostęp 07.09.2020), Grupa Robocza Art. 29, *Opinia nr 3/2012 w sprawie zmian sytuacji w dziedzinie technologii*

jakiego rodzaju danych dotyczy, w jaki sposób przetwarzanych, w jakim celu). Wątpliwości może natomiast budzić to, czy i w jakim stopniu udało się prawodawcy unijnemu zrealizować cel, jakim było objęcie danych biometrycznych szczególną ochroną – a także w jakim zakresie udało się to w odniesieniu do danych osobowych dzieci. Uzasadnione obawy może budzić ryzyko, że przetwarzanie danych osobowych w ramach tzw. *soft biometrics* pozostanie poza reżimem ochrony przewidzianym dla danych należących do szczególnych kategorii, ponieważ są nim objęte wyłącznie dane przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej.

5.2.2 Szczególne kategorie danych osobowych nieposiadające definicji legalnych

Unijny prawodawca nie zdefiniował większości spośród kategorii danych wymienionych w art. 9 ust. 1 rozporządzenia 2016/679, choć niektóre z nich mogą powodować duże trudności interpretacyjne.

Objęcie szczególną ochroną danych ujawniających pochodzenie rasowe lub etniczne – z poczynionym w motywie 51 zastrzeżeniem, że Unia Europejska nie akceptuje teorii sugerujących istnienie osobnych ras ludzkich – stanowi wyraz jej dążenia do zapobiegania dyskryminacji na tym tle, choć w istocie jest to wspólny argument przemawiający za zwiększoną ochroną wszystkich danych wymienionych w art. 9 ust. 1 rozporządzenia 2016/679. Przez grupę etniczną można rozumieć społeczność, którą charakteryzują cechy, takie jak „nazwa (etnonim), język lub zdecydowanie odmienna gwara, wspólne pochodzenie z określonego terytorium lub od wspólnego przodka, świadomość historii i kultury, system wartości i symbolika grupowa, religia, poczucie więzi łączącej jej członków przy jednoczesnym dystansie do innych grup”[165].

Przez dane osobowe ujawniające poglądy polityczne można rozumieć informacje o preferencjach politycznych, które niekoniecznie muszą przejawiać się poprzez formalne członkostwo w konkretnym ugrupowaniu. Pod rządami uodo z 1997 r. do szczególnych kategorii danych, obok danych o poglądach politycznych, zaliczano także informacje o przynależności partyjnej[166]. Trudno zgodzić się z wyrażonym w literaturze poglądem, że brak wskazania wprost tego rodzaju informacji w art. 9 ust. 1 rozporządzenia 2016/679 oznacza, że nie stanowią one już danych objętych szczególną ochroną[167]. Informacja o przynależności do partii będzie objęta

biometrycznych, przyjęta w dniu 27.04.2012 r., WP193, https://archiwum.giodo.gov.pl/pl/ file/5337 (dostęp: 07.09.2020), Grupa Robocza Art. 29, *Opinia w sprawie systemów rozpoznawania twarzy w usługach online i usługach komórkowych*, przyjęta w dniu 22.03.2012 r., WP 192, https://archiwum.giodo.gov.pl/pl/1520111/4620 (dostęp 07.09.2020).

[165] *Encyklopedia PWN*, https://encyklopedia.pwn.pl/haslo/grupa-etniczna;3908271.html (dostęp: 23.09.2020).

[166] Art. 27 ust. 1 uodo z 1997 r.

[167] P. Litwiński, *Komentarz do art. 9 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis.

ochroną przewidzianą w tym przepisie właśnie ze względu na to, że ujawnia poglądy polityczne osoby, której dotyczy[168], a przynajmniej jest to bardzo wysoce prawdopodobne.

Do szczególnych kategorii danych osobowych zaliczono także przekonania religijne lub światopoglądowe. Informacje o przekonaniach religijnych należą do najbardziej intymnych sfer życia człowieka, co uzasadnia objęcie takich danych osobowych szczególną ochroną. Są też objęte ochroną konstytucyjną – zakaz zobowiązywania kogokolwiek przez organy władzy publicznej do ujawnienia swojego światopoglądu, przekonań religijnych lub wyznania przewiduje art. 53 ust. 7 Konstytucji RP, jako jeden z przejawów wolności sumienia i religii. Cel wymienienia w tym przepisie wszystkich trzech rodzajów informacji budzi wątpliwości komentatorów, gdyż ich zdaniem przekonania religijne i wyznanie bezsprzecznie mieszczą się w pojęciu światopoglądu – upatrują go w dążeniu do uniknięcia interpretacji zawężających[169].

O ile pojęcie przekonań religijnych wydaje się zrozumiałe, o tyle uzasadnione wątpliwości budzi to, jak na gruncie przepisów rozporządzenia 2016/679 należy rozumieć przekonania światopoglądowe. Według słownika języka polskiego, światopogląd to „zespół czyichś poglądów na świat i na życie, wpływający na jego zachowanie"[170]. Ta definicja jest jednak mało pomocna, ponieważ zakres informacji, jakie mogą mieścić się w tym pojęciu, wydaje się praktycznie nieograniczony. Zdaniem przedstawicieli doktryny wprowadzenie kategorii danych ujawniających przekonania światopoglądowe, w miejsce przekonań filozoficznych – które stanowiły dane szczególnie chronione w świetle art. 27 ust. 1 uodo z 1997 r. – oznacza „istotne ograniczenie zakresu danych objętych specjalnymi zasadami ochrony jedynie do przekonań osoby o fundamentalnym dla niej znaczeniu"[171]. Jednocześnie w literaturze przedmiotu prezentowana jest przeciwstawna teza, mówiąca o tym, że wprowadzone w rozporządzeniu 2016/679 pojęcie przekonań światopoglądowych jest bardziej pojemne w stosunku do pojęcia przekonań filozoficznych czy danych o przynależności wyznaniowej – ponieważ na światopogląd mogą składać się także inne czynniki, niezwiązane z tymi sferami życia[172]. Warto jednak zadać pytanie, czy wprowadzenie jakiejkolwiek zmiany – w stosunku do poprzedniego stanu prawnego – rzeczywiście było zamiarem unijnego prawodawcy. W wersji anglojęzycznej art. 9 ust. 1 oraz motywu 75 rozporządzenia 2016/679 występuje bowiem zwrot *philosophical beliefs*, identycznie jak w przepisach dyrektywy 95/46 – co wyjaśnia, dlaczego we wzorowanej na jej przepisach uodo

[168] M. Kuba, *Komentarz do art. 9 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, Lex.
[169] M. Olszówka, *Komentarz do art. 53 Konstytucji RP*, [w:] M. Safjan, L. Bosek (red.), M. Safjan, L. Bosek (red.), *Konstytucja RP…*, Legalis.
[170] *Internetowy Słownik Języka Polskiego PWN*, https://sjp.pwn.pl/szukaj/światopogląd.html (dostęp: 07.09.2020).
[171] P. Litwiński, K. Kaźmierczak, *Elementarz ochrony danych osobowych*, [w:] D. Dörre-Kolasa (red.), *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2017, s. 8.
[172] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 9 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis.

z 1997 r. mowa była właśnie o przekonaniach filozoficznych. Polskojęzyczna wersja rozporządzenia 2016/679 istotnie różni się więc od anglojęzycznej. Wobec powyższego wydaje się uprawnione sięgnięcie do dorobku doktryny powstałego na gruncie uodo z 1997 r. Zdaniem jej komentatorów dane dotyczące przekonań religijnych lub filozoficznych odnoszą się „także do postawy ateistycznej lub agnostycznej, kategoria ta nie obejmuje natomiast zasad moralnych”[173].

Problem z różnicą w brzmieniu art. 9 ust. 1 rozporządzenia 2016/679 w różnych wersjach językowych, a także nieostrość pojęcia danych ujawniających przekonania światopoglądowe, wydaje się niezauważony i można raczej spodziewać się jego szerokiej interpretacji ze strony organu nadzorczego. Może mieć to pozytywne albo negatywne skutki. Zakwalifikowanie większego zakresu danych osobowych do szczególnych kategorii podnosi poziom ochrony praw osób, których dane dotyczą. Jednak rozszerzającą wykładnię wyjątków – jakim jest zaliczenie niektórych kategorii danych osobowych do tzw. danych wrażliwych – trudno uznać za prawidłowy zabieg w świetle reguł interpretacji prawa (*exceptiones non sunt extendendae*), a ponadto może to bardzo negatywnie oddziaływać na sytuację przedsiębiorców i innych podmiotów zobowiązanych do stosowania rozporządzenia 2016/679 – doprowadzając wręcz do sytuacji, w której nie będą świadomi, które spośród nałożonych przez nie obowiązków będą ich dotyczyć w danym stanie faktycznym. Wiele z nich jest uzależnionych właśnie od faktu przetwarzania danych wymienionych w art. 9 ust. 1 rozporządzenia 2016/679. Nieostrość pojęcia przekonań światopoglądowych stanowi istotne ograniczenie pewności prawa. Decyzja o zakwalifikowaniu lub nie danych osobowych do tej kategorii może być więc jednym z trudniejszych zadań na gruncie rozporządzenia 2016/679. Obawy przed prawnymi, finansowymi, a także wizerunkowymi konsekwencjami niezastosowania się do tych norm najprawdopodobniej mogą skutkować albo stosowaniem interpretacji rozszerzającej i uznawaniem wątpliwych, granicznych przypadków za dane zaliczające się do przekonań światopoglądowych, albo wręcz odwrotnie – próbą marginalizowania tego problemu.

W katalogu kategorii danych osobowych objętych szczególną ochroną znalazły się także informacje o przynależności do związków zawodowych. Może za tym przemawiać potencjalne ryzyko nierównego traktowania pracownika, czy wręcz dyskryminowania go przez pracodawcę z powodu uczestnictwa w związku zawodowym[174], choć ustawodawca przewiduje ochronę pracownika przed nierównym traktowaniem także z powodu nieprzynależenia do związku. Zgodnie z art. 3 ust. 1 ustawy z dnia 23 maja 1991 r. o związkach zawodowych[175], zakazane jest nierówne traktowanie w zatrudnieniu z powodu przynależności do związku zawodowego lub

[173] *Komentarz do art. 27 uodo z 1997 r.* J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, LEX.
[174] P. Fajgielski, *Ogólne rozporządzenie…*, s. 202.
[175] T.j. Dz.U. z 2019 r. poz. 263.

pozostawania poza nim albo wykonywania funkcji związkowej, którego skutkiem jest w szczególności odmowa nawiązania lub rozwiązanie stosunku prawnego, niekorzystne ukształtowanie wynagrodzenia za pracę zarobkową lub innych warunków zatrudnienia albo pominięcie przy awansowaniu lub przyznawaniu innych świadczeń związanych z pracą zarobkową, pominięcie przy typowaniu do udziału w szkoleniach podnoszących kwalifikacje zawodowe. Zwrócenie uwagi przez ustawodawcę właśnie na te skutki może oznaczać, że jego zdaniem są one najbardziej dotkliwe dla pracownika, a ponadto, że prawdopodobne jest wystąpienie właśnie takich działań pracodawcy. Zaliczenie informacji o przynależności do związków zawodowych do kategorii danych objętych szczególną ochroną, co miało także miejsce w poprzednim stanie prawnym, zasługuje więc na aprobatę, choć z perspektywy ochrony danych osobowych dziecka w związku ze świadczeniem usług społeczeństwa informacyjnego wydaje się mieć marginalne znaczenie.

Do danych osobowych należących do szczególnych kategorii unijny prawodawca zaliczył także dane dotyczące seksualności lub orientacji seksualnej. W dyrektywie 95/46 i uodo z 1997 r. jako tzw. dane wrażliwe wskazane były informacje o życiu seksualnym. Prawodawca zdecydował się więc niejako na podzielenie tej kategorii na dwie. Choć są powiązane blisko ze sobą, bo odnoszą się do tej samej sfery życia człowieka, zastosowany zabieg można ocenić pozytywnie, ponieważ informacje o życiu seksualnym nie muszą ujawniać orientacji seksualnej i na odwrót[176]. Wątpliwości może budzić to, czemu w rozporządzeniu 2016/679 występuje sformułowanie „dane dotyczące seksualności", skoro w poprzednim stanie prawnym mowa była o „danych o życiu seksualnym" i czy ta zmiana powinna wpływać na sposób rozumienia tej kategorii danych osobowych[177]. Odpowiedź powinna być negatywna, gdyż występująca różnica ponownie jest raczej wynikiem sposobu przetłumaczenia tekstu rozporządzenia 2016/679 na język polski niż intencją unijnego prawodawcy[178].

5.3 Dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa

Stosownie do art. 10 rozporządzenia 2016/679, przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych[179] lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa

[176] M. Kuba, *Komentarz do art. 9 rozporządzenia 2016*/679, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, Lex.
[177] Tamże.
[178] W wersji anglojęzycznej dyrektywy 95/46, jak i rozporządzenia 2016/679, występuje sformułowanie *sex life*.
[179] Początkowo w tym przepisie zamiast pojęcia „czyny zabronione" występowało pojęcie „naruszenia prawa" – zmiana nastąpiła w wyniku sprostowania rozporządzenia 2016/679 z dnia 23 maja 2018 r. (Dz. Urz. UE L 127 z 23.05.2018, s. 2).

członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Ponadto w przypadku rejestrów wyroków skazujących wprowadzono dodatkowe obostrzenie, ponieważ mogą być przetwarzane wyłącznie pod nadzorem władz publicznych. W Polsce do takich rejestrów zalicza się Krajowy Rejestr Karny, prowadzony na podstawie przepisów z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym[180], w którym gromadzone są m.in. dane o osobach umieszczonych w schroniskach dla nieletnich, oraz Rejestr Sprawców Przestępstw na Tle Seksualnym, prowadzony na podstawie ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym[181], w którym również umieszczane są dane dzieci, co budzi wiele uzasadnionych kontrowersji[182].

Zdaniem A. Nerki, przez wyroki skazujące należy rozumieć – na gruncie polskiego prawa – wyroki, o których mowa w art. 413 § 2 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego[183] lub art. 82 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia[184], a ich wskazanie w art. 10 rozporządzenia 2016/679 „zdaje się wykluczać umarzające lub warunkowo umarzające postępowanie albo też uniewinniające (art. 414 kpk), a także orzeczenia dyscyplinarne, jak i sądów koleżeńskich”[185]. Z kolei P. Fajgielski zwraca uwagę na wątpliwości co do poprawności tłumaczenia zwrotu *criminal convictions,* gdyż wydaje się, że w polskiej wersji językowej nastąpiło nadmierne zawężenie, a zakresem zastosowania art. 10 rozporządzenia 2016/679 powinny być objęte także inne niż wyroki skazujące orzeczenia wydane w postępowaniu karnym[186]. Z kolei czynem zabronionym, zgodnie z art. 115 § 1 ustawy z dnia 6 czerwca 1997 r. Kodeks karny[187], jest zachowanie o znamionach określonych w ustawie karnej – jednak nie każdy czyn zabroniony stanowi przestępstwo[188]. Dlatego „czyn zabroniony” jest pojęciem szerszym niż pojęcie „przestępstwo”. Warto zauważyć, że Europejska Rada Ochrony Danych zdaje się rozumieć pojęcie wyroków skazujących oraz czynów zabronionych bardzo szeroko, wręcz rozszerzająco, podając jako przykład takich danych informacje gromadzone przez

[180] T.j. Dz.U. z 2019 r. poz. 1158.
[181] T.j. Dz.U. z 2020 r. poz. 152.
[182] Rzecznik Prawo Obywatelskich podnosi, że umieszczanie danych dzieci w tym rejestrze jest nieproporcjonalnym ograniczeniem ich prawa do prywatności i godzi w zasadę kierowania się dobrem dziecka – por. https://www.rpo.gov.pl/pl/content/16-latka-w-„rejestrze-pedofilow”-rpo-ma-watpliwosci-i%20pisze-do-premiera (dostęp 07.09.2020). Ponieważ przetwarzanie danych osobowych w tym kontekście nie jest związane ze świadczeniem usług społeczeństwa informacyjnego, problem ten nie będzie przedmiotem analizy w niniejszej rozprawie.
[183] T.j. Dz. U. z 2022 r. poz. 1375 z późn. zm., dalej jako kpk.
[184] T.j. Dz.U. z 2022 r. poz. 1124.
[185] A. Nerka, *Komentarz do art. 10 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.
[186] P. Fajgielski, *Ogólne rozporządzenie…*, s. 217.
[187] T.j. Dz.U. z 2022 r. poz. 1138 z późn. zm., dalej jako kk.
[188] Przesądza o tym art. 1 § 2 i 3 kk, por. *Komentarz do art. 115 kpk* [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny. Komentarz. Wyd. 7*, Warszawa 2021, Legalis.

tzw. połączone pojazdy[189], przetwarzane przez organy ścigania w celu wykrycia przekroczenia prędkości lub innych wykroczeń[190].

Pojęcie „środków bezpieczeństwa" jest najbardziej nieostrym elementem zawartym w art. 10 rozporządzenia 2016/679, gdyż nawiązuje do anglosaskiego systemu prawnego[191]. Na gruncie polskiego prawa można przyjąć, że chodzi o środki zabezpieczające prawidłowy przebieg postępowania (np. tymczasowe aresztowanie, poręczenie majątkowe)[192], środki karne w rozumieniu art. 39 kk oraz środki zabezpieczające, o których mowa w art. 93a § 1 kk – ponieważ co do zasady są one orzekane w związku ze skazaniem[193] , czego przykładem jest dozór elektroniczny.

Należy zastanowić się, jaki jest charakter (kategoria) danych osobowych wymienionych w art. 10 rozporządzenia 2016/679. W uodo z 1997 r. dane osobowe dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, pierwotnie stanowiły odrębny od należących do szczególnych kategorii typ danych, objęty wyjątkowym reżimem ochrony – co przejawiało się dopuszczalnością ich przetwarzania wyłącznie na podstawie ustawy. Nowelizacją z 2001 r. dodano je jednak do zawartego w art. 27 ust. 1 katalogu tzw. danych wrażliwych. Ten zabieg ustawodawcy był motywowany problemami, jakie ujawniły się w praktyce stosowania przepisu art. 28 ust. 1 uodo z 1997 r[194]. W razie braku przepisu rangi ustawowej, zezwalającego na takie przetwarzanie, nie istniała bowiem żadna inna przesłanka legalizująca. Ponadto biorąc pod uwagę, że przez mieszczące się w tym rodzaju danych „inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym" należało rozumieć także orzeczenia wydane w postępowaniu cywilnym czy decyzje administracyjne, bez względu na ich przedmiot, objęcie ich tak rygorystycznym ograniczeniem nie zawsze było adekwatne do zagrożeń dla podmiotów danych, a rodziło poważne trudności w funkcjonowaniu wielu podmiotów gospodarczych. Włączenie tego rodzaju danych do katalogu szczególnych kategorii danych otworzyło możliwość ich przetwarzania na podstawie jednej spośród ośmiu możliwych przesłanek.

---

[189] Połączone pojazdy, ang. *connected vehicles*, to pojazdy, które wykorzystują dowolną z wielu różnych technologii komunikacyjnych do komunikacji z kierowcą, innymi samochodami na drodze, infrastrukturą drogową i chmurą obliczeniową – por. http://autocaat.org/Technologies/Automated_and_Connected_Vehicles (dostęp 07.09.2020).

[190] EROD, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications - version for public consultation adopted on 28 January 2020*, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf (dostęp 07.09.2020), s. 11.

[191] P. Litwiński, *Komentarz do art. 10 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis i tam powołana literatura.

[192] P. Fajgielski, *Ogólne rozporządzenie…*, s. 218.

[193] P. Litwiński, *Komentarz do art. 10 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis.

[194] Por. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych…*, Lex.

Na gruncie rozporządzenia 2016/679 ponownie mamy więc do czynienia z oddzieleniem danych dotyczących orzeczeń i środków o charakterze prawnokarnym od danych osobowych należących do szczególnych kategorii. Za takim wnioskiem przemawiają dwie okoliczności. Po pierwsze, te dane nie zostały wymienione w art. 9 zawierającym katalog danych należących do szczególnych kategorii, a jednocześnie prawodawca zdecydował o wprowadzeniu dotyczącej ich regulacji w odrębnej jednostce redakcyjnej, tj. art. 10[195]. Po drugie, w tym przepisie wskazano *expressis verbis*, że odnosi się on do danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa przetwarzanych na podstawie art. 6 ust. 1 – czyli przepisu, który określa przesłanki legalności przetwarzania tzw. zwykłych danych osobowych[196]. Nie można jednak powiedzieć, że prawodawca zrównał status tych danych, ponieważ art. 10 zawiera dodatkowe wymogi, jakie muszą być spełnione, by przetwarzanie danych dotyczących orzeczeń i środków o charakterze prawnokarnym było legalne, dlatego w przypadku zamiaru ich przetwarzania należy uwzględnić wymogi określone zarówno w art. 6 ust. 1, jak i art. 10 rozporządzenia 2016/679. Wobec tego można postawić tezę, że dane, o których mowa w art. 10, stanowią odrębny, specyficzny typ (kategorię) danych osobowych.

5.4 Krajowy numer identyfikacyjny

Przepis art. 87 rozporządzenia 2016/679 wprowadza możliwość ustanowienia w prawie krajowym szczególnych warunków przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym. Stanowi również, że „w takim przypadku krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym używa się wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, które przewiduje niniejsze rozporządzenie". Nie zdecydowano się na wprowadzenie definicji pojęć „krajowy numer identyfikacyjny" i „inny identyfikator o zasięgu ogólnym", dlatego należy je interpretować przez pryzmat regulacji krajowych[197]. Państwa członkowskie mają swobodę w zakresie tworzenia takich identyfikatorów i zasad ich wykorzystywania oraz sposobów ochrony, choć granice tej swobody wyznacza obowiązek zachowania odpowiednich zabezpieczeń w myśl rozporządzenia 2016/679. Innymi słowy art. 87 rozporządzenia 2016/679 można rozumieć w ten sposób, że państwo członkowskie może wprowadzić dodatkowe regulacje, w tym obostrzenia, odpowiadające specyfice stosowania przez nie numeru lub innego identyfikatora, jednak z

[195] O różnicowaniu danych, o których mowa w art. 9 i 10, świadczy także redakcja innych przepisów rozporządzenia 2016/679, np. art. 6 ust. 4 lit. c – „czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych zgodnie z art. 10". Posłużenie się spójnikiem „lub" świadczy o odrębności semantycznej tych pojęć.
[196] P. Fajgielski, *Ogólne rozporządzenie…*, s. 219.
[197] M. Sakowska-Baryła, *Komentarz do art. 87 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.

zachowaniem przynajmniej takiego poziomu ochrony, jaki jest przewidziany w rozporządzeniu 2016/679. Numery czy inne identyfikatory, pozwalające na jednoznaczną identyfikację osoby fizycznej – czy wręcz tworzone właśnie z takim zamysłem – powinny być objęte dodatkową ochroną z uwagi na związane z nimi szczególne zagrożenia, takie jak ryzyko zgromadzenia „praktycznie nieograniczonej ilości danych osobowych, z jednoczesną możliwością ich wykorzystania w każdej chwili, przez każdego, kto dysponuje odpowiednimi urządzeniami technicznymi wyszukującymi dane, w tym związanymi z bankami danych powiązanych z różnego rodzaju identyfikatorami”[198].

W Polsce za najważniejszy krajowy numer identyfikacyjny można uznać numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL), którego zasady i tryb nadawania, a także zakres i zasady rejestracji danych gromadzonych w rejestrze PESEL, określa ustawa z dnia 24 września 2010 r. o ewidencji ludności[199]. Numer PESEL nadawany jest m.in. wszystkim obywatelom Rzeczypospolitej Polskiej, ma specyficzną, ściśle określoną konstrukcję[200] i, o ile nie zaistnieją pewne wyjątkowe przesłanki[201], nie ulega zmianie. Ponadto raz nadany numer PESEL nie może być ponownie przypisany do innej osoby. Stosownie do art. 6 ustawy o ewidencji ludności, obowiązki związane z utrzymaniem i rozwojem rejestru PESEL – w tym zabezpieczeniem gromadzonych w nich danych, ochroną przed nieuprawnionym dostępem do niego[202] – spoczywają na organie prowadzącym rejestr, którym jest minister właściwy do spraw informatyzacji. Przepisy ustawy o ewidencji ludności określają także zasady dostępu do danych zawartych w rejestrze. Przysługuje on przede wszystkim podmiotom publicznym realizującym zadania z zakresu ewidencji ludności, rejestracji stanu cywilnego, organom ścigania, ale nie tylko – także inne osoby i jednostkom organizacyjnym, w przypadku wykazania interesu prawnego lub faktycznego (w tym wypadku pod warunkiem zgody osoby, której dane dotyczą). Trudno zatem w pełni zgodzić się z wyrażonym w literaturze stwierdzeniem, że numer PESEL służy „administracji publicznej do przetwarzania danych o obywatelach jako posiłkowa metoda statystyczna i identyfikacyjna przy jednoczesnym nadrzędnym pojmowaniu danych o podmiocie prawa, a wysławianych na gruncie cywilistycznym. (…) Numer ten (co ważne, jedyny i

[198] Tamże.
[199] T.j. Dz. U. z 2019 r. poz. 1397.
[200] Zgodnie z art. 11 ustawy o ewidencji ludności, numer PESEL jest to jedenastocyfrowy symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, zawierający datę urodzenia, numer porządkowy, oznaczenie płci oraz liczbę kontrolną; przepis określa ponadto sposób kodowania w numerze PESEL tych informacji.
[201] Numer PESEL jest zmieniany w przypadku: sprostowania daty urodzenia; zmiany płci; nadania go na skutek omyłki organu administracji publicznej mającej wpływ na numer PESEL lub wprowadzenia w błąd organu administracji publicznej co do tożsamości osoby (art. 19 ust. 1 ustawy o ewidencji ludności).
[202] W 2017 r. organ nadzorczy, wówczas Generalny Inspektor Ochrony Danych Osobowych, stwierdził uchybienia w procesie przetwarzania danych osobowych w ramach rejestru PESEL i aplikacji, za pośrednictwem której realizowany jest do niego dostęp, i nakazał Ministrowi Cyfryzacji ich usunięcie – decyzja z dnia 12 września 2017 r., sygn. DIS/DEC-1110/17/68986, https://archiwum.giodo.gov.pl/pl/file/12598 (dostęp: 07.09.2020).

niepowtarzalny dla jednostki) ma za zadanie uproszczenie pracy administracji publicznej w kontaktach z obywatelami lub w relacjach między urzędami”[203] – ponieważ pełni także inne funkcje, w tym niekiedy zawarte w nim informacje są wykorzystywane przez podmioty prywatne dla realizacji swoich celów. Regulacje zasad postępowania z numerem PESEL zawarte w ustawie o ewidencji o ludności obejmują jednak, co zrozumiałe w świetle jej zakresu przedmiotowego, mają charakter publicznoprawny. Można więc powiedzieć, że w sferze relacji między podmiotami prywatnymi w Polsce nie wprowadzono szczególnych uregulowań dotyczących przetwarzania numeru PESEL jako krajowego numeru identyfikacyjnego. Nie ma również żadnych przesłanek, by uznać go za dane osobowe należące do szczególnych kategorii, objęte zakazem przetwarzania, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679. Mimo tego wydaje się, że istnieją argumenty przemawiające za objęciem go dodatkową ochroną – przede wszystkim PESEL stanowi dane uławiające dokonanie tzw. kradzieży tożsamości. Prezes UODO podejmuje działania w celu ograniczenia przetwarzania go w różnych obszarach, postulując „pełne wdrożenie art. 87 RODO do polskiego porządku prawnego i idące za tym zwiększenie ochrony numeru PESEL”[204], opowiada się także za niezamieszczaniem w decyzjach administracyjnych numerów PESEL stron[205], choć wydaje się, że pożądane byłoby zintensyfikowanie działań ukierunkowanych na monitorowanie wykorzystywania PESEL przez podmioty prowadzące działalność gospodarczą, ze szczególnym uwzględnieniem przetwarzania numerów PESEL dzieci.

5.5 Pojęcie przetwarzania danych osobowych

Zgodnie z art. 2 ust. 1 rozporządzenia 2016/679, ma ono zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Przetwarzanie danych osobowych jest więc jednym z najważniejszych pojęć – stanowi bowiem podstawowy wyznacznik materialnego zakresu stosowania przepisów rozporządzenia 2016/679. Z kolei pojęcie zbioru danych osobowych utraciło po reformie ochrony danych osobowych istotne znaczenie, jakim cieszyło się w poprzednim stanie prawnym[206]. W rozporządzeniu 2016/679 pojęcie zbioru danych występuje w

[203] K. Biernat, *Komentarz do art. 15 ustawy o ewidencji ludności*, [w:] M. Dobek-Rak, P. Mierzejewski, D. Trzcińska, K. Biernat, *Ustawa o ewidencji ludności. Komentarz*, Warszawa 2013, LEX.

[204] Prezes UODO wypowiedział się negatywnie na temat ujawniania numeru PESEL w certyfikacie podpisu elektronicznego i używania jako identyfikatora w usługach cyfrowych, *PESEL nie musi być publicznie ujawniany*, https://uodo.gov.pl/pl/138/1098 (dostęp: 07.09.2020).

[205] UODO, *Decyzje administracyjne bez numeru PESEL*, https://uodo.gov.pl/pl/138/561, (dostęp: 07.09.2020).

[206] Wówczas przetwarzanie danych osobowych w zbiorze powodowało konkretne obowiązki, których dopełnienie było warunkiem możliwości rozpoczęcia jakichkolwiek działań odnoszących się do danych osobowych, a niespełnienie było zagrożone odpowiedzialnością karną. Takim obowiązkiem było zgłoszenie zbioru danych osobowych do rejestracji Generalnemu Inspektorowi, w trybie określonym w rozdziale 6 uodo z 1997 r., od którego

części normatywnej tylko we wspomnianym wyżej art. 2 ust 1 oraz w art. 4 pkt 6, w którym zostało zdefiniowane jako uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie. W motywie 15 rozporządzenia 2016/679 wskazano wprost, że zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są uporządkowane według określonych kryteriów, nie powinny być objęte jego zakresem. Jednak ze względu na to, że rozporządzenie 2016/679 ma zastosowanie także do danych „mających stanowić część zbioru danych" – a więc pozyskanych w celu utworzenia nowego zbioru lub włączenia ich do już istniejącego – znaczenie powyższego zawężenia wydaje się marginalne, zwłaszcza, gdy mowa o danych znajdujących się w systemach informatycznych. Funkcja wyszukiwania w nich danych osobowych, uporządkowanych według kryteriów – choć może cechować ją różny poziom zaawansowania – występuje praktycznie zawsze. Dodatkowo o znikomym znaczeniu pojęcia zbioru danych świadczy okoliczność, że przepisy rozporządzenia 2016/679 nie różnicują obowiązków związanych z ochroną danych osobowych na przykład ze względu na czas istnienia zbioru danych lub celu jego powstania – co miało miejsce pod rządami uodo z 1997 r. w odniesieniu do tzw. zbiorów „doraźnych"[207]. Obecnie pojęcie zbioru danych ma w rezultacie znaczenie tylko na początkowym etapie dokonywania oceny, czy zamierzone działanie mieści się w materialnym zakresie stosowania rozporządzenia 2016/679.

Przetwarzanie oznacza, w myśl definicji zawartej w art. 4 pkt 2 rozporządzenia 2016/679, operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. W tej definicji można wyodrębnić trzy elementy: określenie, czym w ogóle jest przetwarzanie – operacją

uzależniona była dopuszczalność rozpoczęcia przetwarzania danych osobowych (o ile nie została spełniona jedna z przesłanek wyłączających ten obowiązek). Natomiast w przypadku tzw. danych wrażliwych, ich przetwarzanie było możliwe dopiero po wpisaniu przez GIODO zbioru do ogólnokrajowego, jawnego rejestru zbioru danych osobowych. Zgłoszenie zbioru danych obejmowało m.in. informacje o podstawie prawnej przetwarzania danych osobowych, kategorii osób, których dane dotyczą, rodzaju danych i ich zakresie, sposobie przetwarzania i wdrożonych środkach zabezpieczających dane. Przed wpisaniem zbioru danych osobowych do rejestru GIODO oceniał zgodność planowanego przetwarzania z przepisami o ochronie danych osobowych. Rejestracja zbiorów danych osobowych była zatem jedną z form kontroli instytucjonalnej sprawowanej przez GIODO (por. P. Fajgielski, *Kontrola przetwarzania i ochrony…*, s. 244-247). Niedopełnienie obowiązku zgłoszenia zbioru danych osobowych było zagrożone grzywą, karą ograniczenia wolności albo pozbawienia wolności do roku (art. 53 uodo z 1997 r.). Obowiązek zgłaszania zbiorów danych osobowych do rejestracji wygasł 25.05.2018 r., wraz z rozpoczęciem stosowania rozporządzenia 2016/679, a niezakończone do tego dnia postępowania zostały umorzone na podstawie art. 160 ust. 4 uodo z 2018 r.

[207] W myśl art. 2 ust. 3 uodo z 1997 r., w odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, miały zastosowanie jedynie przepisy rozdziału 5 tej ustawy – określające obowiązki związane z zabezpieczeniem danych osobowych.

lub zestawem operacji; do jakich informacji się odnosi – danych osobowych lub ich zestawów[208]; w jaki sposób może być dokonywane – w sposób zautomatyzowany lub niezautomatyzowany. Jeśli zaistnieją te okoliczności, wówczas można zakwalifikować dane działanie jako przetwarzanie[209]. Analizując przykładowy katalog operacji przetwarzania można dostrzec, że mogą nim być działania realizowane na różnych etapach: począwszy od pozyskania danych osobowych, przez różnego rodzaju czynności wykonywanych na przechowywanych danych, aż po ich usuwanie. Wbrew wykładni językowej przetwarzanie nie jest więc zawężone tylko do działań polegających na przekształcaniu czy opracowywaniu danych osobowych[210]. Nie ma także znaczenia cel, w jakim dane osobowe są zbierane i przechowywane – dlatego nawet samo składowanie danych osobowych w celu archiwalnym oznacza ich przetwarzanie. W orzecznictwie TSUE za przetwarzanie uznano działalność prowadzoną przez wyszukiwarki internetowe, polegającą na zlokalizowaniu informacji opublikowanych lub zamieszczonych w internecie przez osoby trzecie, indeksowaniu ich w sposób automatyczny, czasowym przechowywaniu takich informacji i wreszcie udostępnianiu ich internautom w sposób uporządkowany zgodnie z określonymi preferencjami[211].

Operacją przetwarzania jest więc działanie, które dotyczy danych osobowych; zestaw operacji można rozumieć jako kilka operacji, tworzących pewną całość. Z kolei przez zautomatyzowany sposób przetwarzania rozumie się operacje wykonywane przy użyciu środków służących do automatycznego przetwarzania danych, np. komputerów, systemów informatycznych. *A contrario*, niezautomatyzowana forma przetwarzania, zwana też niekiedy przetwarzaniem „ręcznym" lub „tradycyjnym"[212], to przetwarzanie bez wykorzystania takich urządzeń i systemów, czego przykładem może być gromadzenie dokumentów zawierających dane osobowe w postaci papierowej. Przetwarzanie, które łączy te dwa sposoby, określa się przetwarzaniem w sposób częściowo zautomatyzowany. Rozporządzenie 2016/679 ma zastosowanie do wszystkich trzech sposobów przetwarzania, o czym stanowi jego art. 1 ust. 1. Uzasadnienie takiej decyzji prawodawcy można znaleźć w motywie 15 – jest ona podyktowana dążeniem do zapobiegnięcia ryzyku obchodzenia prawa; „ochrona osób fizycznych powinna być neutralna pod względem technicznym i nie powinna zależeć od stosowanych technik".

[208] Posłużenie się sformułowaniem „zestaw danych" jest kolejnym dowodem na znikome znaczenie pojęcia zbioru danych, jednak wydaje się, że na gruncie art. 4 pkt 2 rozporządzenia 2016/679 uprawnione byłoby odwołanie się właśnie do niego.
[209] W. Chomiczewski, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO...*, s. 187.
[210] *Słownik języka polskiego PWN*, hasło „przetwarzanie", https://sjp.pwn.pl/szukaj/przetwarzanie.html (dostęp: 07.09.2020).
[211] Wyrok TSUE z dnia 13 maja 2014 r. w sprawie C-131/12, Google Spain SL, Google Inc. Przeciwko Agencia Española de Protección de Datos (AEPD), M. C. Gonzálezowi.
[212] P. Fajgielski, *Ogólne rozporządzenie…*, s. 91.

Wyliczenie zawarte w art. 4 pkt 2 rozporządzenia 2016/679 ma charakter wyłącznie przykładowy – nie stanowi więc zamkniętego katalogu operacji, jakie mogą być wykonywane na danych osobowych[213]. Także przed reformą ochrony danych osobowych uważano, że nie jest możliwe opracowanie wyczerpującej listy działań, jakie mogą stanowić przetwarzanie danych osobowych, a obecnie obowiązująca definicja przetwarzania świadczy, że to stanowisko nie straciło na aktualności[214]. Prawodawca zdecydował się na doprecyzowanie znaczenia niektórych operacji przetwarzania z powodu ich szczególnego charakteru, czym podyktowane jest osobne ich potraktowanie – dotyczy to ograniczenia przetwarzania, profilowania oraz pseudonimizacji danych osobowych[215].

Zgodnie z art. 4 pkt 3 rozporządzenia 2016/679, ograniczenie przetwarzania polega na oznaczeniu przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania. Za dodatkowym wyjaśnieniem, czym jest ograniczenie przetwarzania, mogło przemawiać to, że jest to jedno z uprawnień osoby, której dane dotyczą, określonych w rozdziale III rozporządzenia 2016/679. Z tego powodu zasadne jest precyzyjne wskazanie, na czym ograniczenie ma polegać, by sposób realizacji wspomnianego uprawnienia nie budził wątpliwości. Abstrahując od tych przypuszczeń, celem wprowadzania definicji legalnych jest wyjaśnienie pojęć trudnych lub wskazanie sposobu ich rozumienia na gruncie danego aktu prawnego, jeśli odbiega od potocznego. Trudno uznać, że zostało to osiągnięte w przypadku art. 4 pkt 3 rozporządzenia 2016/679. Po pierwsze, definicja jest błędnie skonstruowana przez to, że zarówno w *definiendum*, jak i *definiens*, występuje ten sam wyraz – „ograniczenie". Po drugie, rzeczywistego znaczenia pojęcia „ograniczenia przetwarzania" nie da się odczytać bez lektury art. 18 ust. 2 rozporządzenia 2016/679, co też świadczy o niedoskonałości omawianej definicji legalnej. Stosownie do tego przepisu, jeżeli przetwarzanie zostało ograniczone w wyniku żądania przez osobę, której dane dotyczą, ograniczenia przetwarzania w przypadkach wymienionych w ust. 1 tego przepisu, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego UE lub państwa członkowskiego. Innymi słowy, jeśli osoba, której dane dotyczą, żąda ograniczenia przetwarzania, dopuszczalne jest jedynie ich przechowywanie. Inne operacje są możliwe, ale wyłącznie, jeśli ta osoba wyrazi na nie zgodę[216]. Istotą ograniczenia przetwarzania jest więc

[213] B. Fischer, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.

[214] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, i tam powołana literatura.

[215] W. Chomiczewski, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 187-188.

[216] To obostrzenie nie dotyczy operacji, które są niezbędne m.in. do ustalenia, dochodzenia lub obrony roszczeń.

faktyczne powstrzymanie się od dokonywania niektórych operacji na danych osobowych, a nie jedynie – jak stanowi omawiana definicja – oznaczenie danych przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania. Odnosi się ona *de facto* do czynności poprzedzającej ograniczenie przetwarzania[217]. Oznaczenie danych, jeśli przyjąć, że polega na wyróżnieniu, zaznaczeniu informacji podlegających ograniczeniu przetwarzania, jest zapewne niezbędnym krokiem poprzedzającym rzeczywiste zaniechanie wykorzystania tych danych w inny sposób niż tylko poprzez ich przechowywanie.

Kolejną, zdefiniowaną w rozporządzeniu 2016/679 operacją przetwarzania, jest profilowanie[218]. Zgodnie z art. 4 pkt 4 oznacza ono dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. W świetle tej definicji profilowanie będzie miało miejsce wówczas, gdy zaistnieją kumulatywnie trzy okoliczności: sposób przetwarzania ma postać zautomatyzowaną, profilowaniu podlegają dane osobowe, celem profilowania jest być ocena czynników osobowych osób fizycznych. Grupa Robocza Art. 29 wyjaśniła, że „Zwykła klasyfikacja osób fizycznych ze względu na znane cechy, jak np. wiek, płeć i wzrost, nie musi skutkować profilowaniem. Decydujący będzie cel takiej klasyfikacji. Przykładowo, klasyfikując swoich klientów ze względu na wiek lub płeć, przedsiębiorstwo może kierować się względami statystycznymi, chcąc uzyskać zbiorczy przegląd klientów bez prognozowania lub wyciągania wniosków na temat konkretnej osoby fizycznej. W takim przypadku celem nie jest ocena cech danej osoby fizycznej, a zatem nie ma mowy o profilowaniu”[219]. Profilowanie może być niezależną operacją przetwarzania danych osobowych, ale może też być elementem podejmowania, wobec osoby, której dane dotyczą, decyzji w sposób zautomatyzowany w rozumieniu art. 22 rozporządzenia 2016/679. Profilowanie znajduje zastosowanie w wielu sektorach, przede wszystkim w sektorze bankowym i ubezpieczeniowym, ale także w marketingu i sprzedaży za pośrednictwem sieci teleinformatycznych (*e-commerce*)[220]. Jego podstawowe zalety związane są z możliwością

[217] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis.
[218] Definicja była inspirowana zaleceniami Rady Europy, zawartymi w rekomendacji CM/Rec (2010) 13 Komitetu Ministrów państw członkowskich w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili, przyjętej w dniu 23 listopada 2010 r., https://uodo.gov.pl/pl/file/1425 (dostęp: 07.09.2020).
[219] Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE*, przyjęte w dniu 6 lutego 2018 r., https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (dostęp 07.09.2020), s. 7.
[220] Por. A. Mednis, *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, Warszawa 2019, s. 69-75.

porządkowania i selekcji informacji, ponieważ w społeczeństwie informacyjnym – w związku z możliwością przetwarzania danych na nieznaną wcześniej skalę – obserwuje się ich przesyt, powodujący „szum informacyjny" oraz zatarcie granic między informacją, wiedzą a pozostałym przekazem. Profilowanie opiera się na matematycznych korelacjach między danymi, które wskazują na przyszłe, przewidywane zachowania, jednak jest to proces tylko wspomagany przez technologię, zaś projektuje i ocenia go człowiek[221]. W procesie profilowania kluczową rolę algorytmy i techniki służące eksploracji danych (*data mining*), w tym tzw. uczenie maszynowe (*machine learning*), rozwijane w ramach tzw. sztucznej inteligencji. W zależności od wielu czynników, takich jak np. rozmiar zbiorów danych, ich ilość, dostępny czas obliczeniowy, rodzaj atrybutów (tj. zdefiniowanych cech, podlegających analizie, którym przypisany jest zbiór możliwych wartości), wykorzystywane mogą być różne rodzaje technik i algorytmów (np. algorytmy deterministyczne lub probabilistyczne)[222]. W tym sensie profilowanie stanowi zautomatyzowaną formę przetwarzania danych. Może implikować zagrożenia dla osób, których dane dotyczą – ich rodzaj i skutki będą uzależnione od kontekstu i celów przetwarzania danych – choć jako podstawowe, i jak się wydaje, wspólne dla wszystkich przypadków – wskazuje się ryzyko dyskryminacji i naruszenia autonomii informacyjnej ze względu na nieprzejrzystość profilowania z perspektywy osoby, której dane dotyczą[223]. Jego przyczyną może być jakość danych poddawanych analizie lub wadliwy algorytm, w którym powiela się np. uprzedzenia historyczne[224], kulturowe, stereotypy, będące przekonaniami jego twórców. Nierzadko algorytmy celowo nastawione są na tworzenie profili po to, by następnie oferować określonym kategoriom osób produkty lub usługi, niedostępne dla osób należących do innej kategorii (lub dostępne, lecz na odmiennych warunkach, np. w innej cenie)[225]. Znaczenie zagrożeń i problemów, wynikających z profilowania, rośnie z uwagi na łączenie dużych ilości danych, łatwo dostępnych w internecie[226]. Informacje potrzebne do profilowania, w tym dane osobowe, pochodzą w dużej mierze z serwisów społecznościowych. Okazuje się, że tylko na podstawie wyrażenia, poprzez tzw. polubienie („lajk" – kliknięcie w przycisk „lubię to"), aprobaty wobec określonych treści zamieszczonych na portalu

[221] M. Hildebrandt, *Profiling: From Data to Knowledge. The challenges of a crucial technology*, "Datenschutz und Datensicherheit" 2006, nr 30, s. 548. Na gruncie rozporządzenia 2016/679 profilowanie może odnosić się nie tylko do oceny przyszłych zachowań czy cech osoby fizycznej, ale także przeszłych.
[222] B. Anrig, W. Browne, M. Gasson, *The Role of Algorithms in Profiling*, [w:] M. Hildebrandt, S. Gutwirth (red.), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Dordrecht 2008, s. 65-80 i tam powołana literatura.
[223] K. Szymielewicz, A. Walkowiak, *Autonomia informacyjna w kontekście usług internetowych: o znaczeniu zgody na przetwarzanie danych i ryzykach związanych z profilowaniem*, „Monitor Prawniczy" dodatek: *Aktualne problemy prawnej ochrony danych osobowych 2014*, G. Sibiga (red.), 2014, nr 9, s. 32.
[224] J. Niklas, *Problem dyskryminacji automatycznej – uwagi na tle ogólnego rozporządzenia o ochronie danych osobowych*, „Europejski Przegląd Sądowy" 2019, nr 7, s. 5.
[225] W. Lis, *Zjawisko profilowania jako przejaw naruszenia prawa do prywatności w środowisku cyfrowym*, [w:] K. Chałubińska-Jentkiewicz, K. Kakareko, J. Sobczak (red.), *Prawo prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017, s. 178.
[226] W. Chomiczewski, *Profilowanie w ogólnym rozporządzeniu o ochronie danych*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *Polska i europejska reforma…*, s. 128.

Facebook, jego użytkownicy profilowani są pod kątem m.in. preferencji seksualnych, poglądów politycznych, czy nawet pochodzenia etnicznego, a ocena tych cech okazała się w wielu przypadkach prawidłowa po ich porównaniu z innymi danymi wolontariuszy biorących udział w badaniu, w tym wynikami testów psychometrycznych (dla przykładu, prawidłowo rozróżniono mężczyzn homoseksualnych i heteroseksualnych w 88% przypadków)[227]. Profil nierzadko tworzy się z połączenia pochodzących z różnych źródeł informacji o konkretnej osobie, zatem nie jest tworzony tylko w oparciu o dane, które zostały dostarczone profilującemu podmiotowi bezpośrednio przez osobę, której dane dotyczą – wykorzystywane są także dane zebrane przez inne podmioty[228]. Uzasadnione wątpliwości może budzić to, czy przeciętna osoba, a zwłaszcza taka, która nie jest i nie chce być użytkownikiem mediów społecznościowych (nie posiada konta w tych serwisach), ma świadomość, że podczas przeglądania w internecie witryn zawierających tzw. wtyczki (*plug-ins*), informacje o jej sposobie korzystania ze strony są przekazywane dostawcy tej wtyczki[229], co może prowadzić do przetwarzania danych osobowych. Czy może zdawać sobie z tego sprawę dziecko, nawet sprawnie poruszające się w internecie i posługujące się urządzeniami, za pośrednictwem których uzyskuje do niego dostęp? Te obawy stanowią główny argument przemawiający za objęciem dzieci szczególną ochroną w przypadku profilowania, na co prawodawca zwrócił uwagę w motywie 38 rozporządzenia 2016/679: „Szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych. Taka szczególna ochrona powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich". Wobec tego pogłębionej analizy wymaga to, w jaki sposób w kontekście profilowania ta szczególna ochrona ma być realizowana i czy jest ona skuteczna.

---

[227] M. Kosinski, D. Stillwell, T. Graepel, *Private traits and attributes are predictable from digital records of human behavior*, "Proceedings of the National Academy of Sciences" 2013, nr 15, s. 5803.

[228] Por. X. Konarski, *Profilowanie danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych osobowych – dotychczasowy i przyszły stan prawny w UE oraz w Polsce*, [w:] G. Sibiga (red.), *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016,* Warszawa 2016, s. 48.

[229] Ten problem stał się przedmiotem pytania prejudycjalnego, skierowanego w do TSUE przez jeden z niemieckich sądów. Witryny internetowe mogą zawierać treści pochodzące z innych źródeł, takie jak filmy, zdjęcia, informacje czy wtyczki (przyciski). Treści te wstawia operator witryny. Wstawiając je, zamieszcza link (odnośnik) do treści zewnętrznych. Działa to w ten sposób, że przeglądarka internetowa pobiera treści z innej strony i wstawia je w miejscu witryny przeglądanej przez użytkownika. By mogło to nastąpić (zadziałać prawidłowo) przeglądarka przesyła do serwera dostawcy treści adres IP komputera użytkownika oraz dane techniczne przeglądarki, a także informacje dotyczące treści, które mają być wyświetlone. Trybunał orzekł m.in., że operatora witryny, który umieszcza we wspomnianej witrynie wtyczkę społecznościową, można uznać za administratora danych w rozumieniu art. 2 lit. d) dyrektywy 95/46. Jego odpowiedzialność jest jednak ograniczona do operacji lub do zestawu operacji przetwarzania danych osobowych, której lub których cele i sposoby rzeczywiście on określa, mianowicie gromadzenia danych i ich ujawniania poprzez transmisję (wyrok TSUE z dnia 29 lipca 2019 r. w sprawie C-40/17, Fashion ID GmbH & Co.KG przeciwko Verbraucherzentrale NRW eV).

Ostatnią ze zdefiniowanych operacji przetwarzania danych osobowych jest pseudonimizacja. W myśl art. 4 pkt 5 rozporządzenia 2016/679 oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Pseudonimizację można rozumieć, biorąc także pod uwagę normę ISO/IEC 29100, jako zabieg, który sprawia, że dane osobowe pozwalające na zidentyfikowanie osoby fizycznej, są zastąpione tzw. aliasem (np. identyfikatorem)[230]. Pseudonimizacji można dokonać np. poprzez szyfrowanie[231], pamiętając, że w świetle art. 4 pkt 5 rozporządzenia 2016/679 klucz deszyfrujący (informacja kryptograficzna pozwalająca na przywrócenie danym ich pierwotnej postaci) powinien być przechowywany w innym miejscu. Pseudonimizacja jest więc procesem odwracalnym[232], którego celem jest, na co wskazuje motyw 28, ograniczenie ryzyka naruszenia praw i wolności osób, których dane są przetwarzane, a z perspektywy podmiotów zobowiązanych do zabezpieczenia danych osobowych, pomoc w wywiązaniu się z obowiązku ochrony danych. Pseudonimizacja została wymieniona w art. 32 ust. 1 lit. a rozporządzenia 2016/679 jako jedno z zabezpieczeń danych osobowych, choć jego stosowanie nie jest obowiązkowe w każdym przypadku, gdy są one przetwarzane – zasadność wprowadzenia takiego środka ochrony uzależniona jest od czynników wskazanych w tym przepisie, m.in. charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych. Przykładową zaletą stosowania pseudonimizacji jest to, że w razie nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych poddanych temu procesowi, osoba, która nie posiada informacji pozwalających na jego odwrócenie (np. klucza deszyfrującego), nie będzie mogła się z nimi zapoznać. Informacje poddane pseudonimizacji wciąż są jednak danymi osobowymi, o czym przesądza motyw 26 rozporządzenia 2016/679 – trudno zatem zgodzić się z wyrażonym w doktrynie poglądem, że „informacja spseudonimizowana stanowi swoiste stadium pośrednie pomiędzy informacjami anonimowymi a danymi osobowymi”[233].

Od pojęcia pseudonimizacji należy odróżnić termin „anonimizacja”. Anonimizacja wprawdzie nie pojawia się w rozporządzeniu 2016/679 jako odrębna operacja przetwarzania (w

[230] L. Kępa, *Bezpieczeństwo danych osobowych. Podejście oparte na ryzyku*, Warszawa 2019, Legalis.
[231] Szerzej na temat technik pseudonimizacji por. ENISA, *Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymization*, https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions (dostęp: 07.09.2020), s. 19-31.
[232] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis.
[233] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis.

motywie 26 mowa jedynie o danych „zanonimizowanych"), może mieć jednak duże znaczenie praktyczne. Anonimizacja polega na pozbawieniu danych osobowych cech, które pozwalają na zidentyfikowanie konkretnej osoby fizycznej – to znaczy na takim przetworzeniu danych, po którym nie będzie możliwe powiązanie posiadanych informacji z żadną osobą. Konieczne jest podkreślenie, że anonimizacja, w przeciwieństwie do pseudonimizacji, jest procesem nieodwracalnym. Anonimizacja może być przydatna w sytuacji, gdy niektóre informacje w dalszym ciągu pozostają użyteczne, lecz do realizacji celu, do którego mają być wykorzystane, nie jest konieczne (lub wręcz nie jest dopuszczalne) przetwarzanie danych osobowych. Skutki anonimizacji są tożsame z usunięciem danych osobowych, a zatem zaprzestaniem ich przetwarzania, co powoduje, że rozporządzenie 2016/679 nie będzie miało zastosowania do takich informacji, nawet jeśli przed anonimizacją stanowiły dane osobowe podlegające przewidzianej w nim ochronie[234].

6. Dziecko jako podmiot danych

Już pod rządami dyrektywy 95/46 i uodo z 1997 r. nie budziło wątpliwości, że ochrona danych osobowych przysługuje każdej osobie fizycznej, nie różnicując jej poziomu ze względu na jakiekolwiek kryteria. Innymi słowy, nie była ona uzależniona od obywatelstwa, zdolności do czynności prawnych, wieku ani żadnych innych czynników[235]. Było więc oczywiste, że prawo do ochrony danych osobowych przysługuje także dzieciom, choć przepisy nie wprowadzały żadnych szczególnych rozwiązań odnoszących się do przetwarzania ich danych osobowych, ani nie wskazywały, kiedy osobę fizyczną należy uznać za dziecko.

Zgodnie z art. 1 ust. 1 rozporządzenia 2016/679, jego przepisy dotyczą ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu danych osobowych. W art. 1 ust. 2 podkreślono, że rozporządzenie 2016/679 chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych. Dodatkowe wskazówki interpretacyjne zawiera motyw 14 rozporządzenia 2016/679, w którym wyjaśniono, że „Ochrona zapewniana niniejszym rozporządzeniem powinna mieć zastosowanie do osób fizycznych - niezależnie od ich obywatelstwa czy miejsca zamieszkania - w związku z przetwarzaniem ich danych osobowych. Niniejsze rozporządzenie nie dotyczy przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących

[234] Patrz motyw 26 rozporządzenia 2016/679.
[235] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych…*, Lex. Wyjątkiem może być różnicowanie intensywności ochrony danych dotyczących osób publicznych (powszechnie znanych) lub pełniących funkcje publiczne – szerzej na ten temat por. M. Sakowska-Baryła, *Dostęp do informacji publicznej a ochrona danych osobowych*, Wrocław 2014; P. Szustakiewicz, *Ograniczenia dostępu do informacji publicznej w świetle najnowszego orzecznictwa sądów administracyjnych*, [w:] A. Mednis (red.), *Prywatność a jawność…*, Legalis.

osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej”[236].

Przepisy o ochronie danych osobowych nie definiują pojęcia „osoba fizyczna”, dlatego w ustaleniu jego znaczenia bierze się pod uwagę krajowe regulacje odnoszące się do tego zagadnienia, czyli przepisy prawa cywilnego[237]. W ich świetle nie ulega wątpliwości, że osobą fizyczną jest człowiek. Stosownie do art. 8 §1 kc, każdy człowiek od chwili urodzenia ma zdolność prawną, która jest rozumiana jako możność bycia podmiotem praw i obowiązków o charakterze cywilnoprawnym[238]. Zdolność prawna nazywana jest kategorią bierną, ponieważ nie wymaga żadnych działań ze strony podmiotu, którego dotyczy, a ponadto przysługuje z mocy prawa – wynika z faktu bycia człowiekiem[239]. Jej uzyskanie jest bezwarunkowe – nie jest uzależnione od spełnienia żadnych kryteriów, np. dotyczących stanu zdrowia fizycznego czy psychicznego[240].

W kontekście zdolności prawnej w doktrynie prawa cywilnego prezentowanych jest wiele różnych poglądów na temat statusu dziecka poczętego – *nasciturusa*. Wśród nich wyróżnić można

[236] Ciekawie kształtowało się, jeszcze przed obowiązywaniem rozporządzenia 2016/679, podejście do ochrony danych osobowych osoby fizycznej prowadzącej działalność gospodarczą, a także przepisy regulujące ujawnianie danych osobowych w Centralnej Ewidencji i Informacji o Działalności Gospodarczej – ustawodawca przyjmował bowiem skrajnie różne rozwiązania - por. P. Fajgielski, *Ochrona danych osobowych przedsiębiorcy będącego osobą fizyczną*, [w:] M. Zdyb, E. Kruk, G. Lubeńczuk (red.), *Dysfunkcje publicznego prawa gospodarczego*, Warszawa 2018, Legalis. Obecnie nie jest już kwestionowane przysługiwanie osobom fizycznym prowadzącym działalność gospodarczą ochrony przewidzianej w rozporządzeniu 2016/679. Pierwsza administracyjna kara pieniężna nałożona na jego podstawie przez Prezesa UODO (w wysokości 943.470,00 zł) dotyczyła właśnie niedopełnienia wobec osób fizycznych prowadzących działalność gospodarczą, a także osób, które ją zawiesiły, tzw. obowiązku informacyjnego, stosownie do art. 14 ust. 1 i 2 rozporządzenia 2016/679 – mowa o decyzji Prezesa UODO z dnia 15 marca 2019 r., ZSPR.421.3.2018, https://uodo.gov.pl/decyzje/ZSPR.421.3.2018 (dostęp: 24.06.2020). Wprawdzie w wyniku zaskarżenia tej decyzji przez administratora sąd uchylił ją częściowo, m.in. w zakresie nałożenia kary, potwierdził jednak prawidłowość stanowiska Prezesa UODO, że osobom fizycznym prowadzącym działalność gospodarczą przysługują uprawnienia wynikające z rozporządzenia 2016/679, także jeśli dane pochodzą ze źródeł powszechnie dostępnych (w tym przypadku z Centralnej Ewidencji i Informacji o Działalności Gospodarczej) – wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 11 grudnia 2019 r., sygn. II SA/Wa 1030/19, http://orzeczenia.nsa.gov.pl/doc/30EDD316DA (dostęp: 24.06.2020). Innym interesującym zagadnieniem jest interpretacja wspomnianych w motywie 14 „danych kontaktowych osoby prawnej”, które nie są objęte ochroną. O ile nie budziło większych wątpliwości to, że informacje, takie jak adres siedziby, nazwa osoby prawnej (lub jednostki organizacyjnej nieposiadającej osobowości prawnej), numer telefonu czy adres poczty elektronicznej, który nie zawiera w sobie imienia i nazwiska żadnej osoby, mieszczą się w tym pojęciu i nie podlegają ochronie danych osobowych, to dyskusyjne było to, czy wyjęte są spod niej również dane osobowe osób reprezentujących, np. członków zarządu spółki kapitałowej czy pełnomocników. Stanowisko w tej sprawie zajęła KE, a w ślad za nią Prezes UODO, opowiadając się za ochroną danych dotyczących tych osób jako osób fizycznych, choć z uwzględnieniem pewnych ograniczeń uzasadnionych bezpieczeństwem obrotu gospodarczego – por. UODO, *Co z obowiązkiem informacyjnym wobec członków zarządu osób prawnych?*, https://uodo.gov.pl/pl/225/1577 (dostęp: 07.09.2020).

[237] Należy jednak zasygnalizować, że prawidłowość przenoszenia wprost instytucji prawa cywilnego na grunt ochrony danych osobowych może budzić wątpliwości. Zdaniem K. Pormeister i Ł. Drożdżowskiego, posłużenie się przez prawodawcę w rozporządzeniu 2016/679 pojęciem „osoba fizyczna” nie oznacza, że chciał on wyznaczyć w ten sposób początek i koniec ochrony (na moment urodzenia się żywego człowieka i jego śmierci), a jedynie w sposób wyraźny zaakcentować wyłączenie spod niej osób prawnych – por. K. Pormeister, Ł. Drożdżowski, *Protecting the Genetic Data of Unborn Children: A Critical Analysis*, “European Data Protection Law Review” 2018, nr 1, s. 59.

[238] R. Strugała, *Komentarz do art. 8 kc*, [w:] E. Gniewek, P. Machnikowski (red.), *Kodeks cywilny. Komentarz,* wyd. 9, Warszawa 2019, Legalis.

[239] J. Regan, *Komentarz do art. 8 kc*, [w:] M. Załucki (red.), *Kodeks cywilny. Komentarz*, wyd. 2, Warszawa 2019, Legalis.

[240] T. Sokołowski, *Komentarz do art. 8 kc*, [w:] A. Kidyba (red.), *Kodeks cywilny. Komentarz. Tom I. Część ogólna*, wyd. II, Warszawa 2012, LEX.

trzy główne nurty: pierwszy, zgodnie z którym *nasciturusowi* nie przysługuje zdolność prawna; drugi, w którym uznaje się, że *nasciturusowi* przysługuje warunkowa zdolność prawna (uzależniona od tego, czy nastąpi urodzenie się żywego noworodka); trzeci, którego zwolennicy uważają, że *nasciturusowi* należy przyznać pewien zakres ogólnej i bezwzględnej zdolności prawnej – zwłaszcza w odniesieniu ochrony dóbr osobistych[241]. Słusznie moim zdaniem podnosi się w literaturze, że „Przyznanie zdolności prawnej człowiekowi od chwili urodzenia nie oznacza, że prawu cywilnemu obojętna jest sytuacja prawna człowieka, która powstaje przed jego urodzeniem. Nie chodzi przy tym tyle o jego sytuację prawną po urodzeniu, ile o zabezpieczenie jego praw, które powstają wskutek zdarzeń mających miejsce przed jego urodzeniem, a które niezmiernie często rzutują na sytuację osoby fizycznej nie tylko bezpośrednio po tym fakcie, ale często wywierają wpływ na całe przyszłe życie człowieka”[242]. Dają temu wyraz przepisy, które wprost świadczą o woli ustawodawcy, by *nasciturus* posiadał warunkową zdolność prawną – np. na gruncie prawa spadkowego[243], nawiązując do wywodzącej się z prawa rzymskiego zasady *nasciturus pro iam nato habetur, quotiens de commodis eius agitur*[244], prawa zobowiązań, gdzie zgodnie z art. 446^1 kc, z chwilą urodzenia dziecko może żądać naprawienia szkód doznanych przed urodzeniem, czy też prawa rodzinnego, którego przepisy odnoszą się do *nasciturusa* i służą zabezpieczeniu praw dziecka[245].

Warto zwrócić uwagę na orzecznictwo – wyrok z 4.04.1966 r., w którym SN stwierdził, że „dziecko poczęte, jeżeli urodzi się żywe, musi być traktowane z punktu widzenia prawa na równi z dzieckiem już urodzonym, jeżeli sfery ich uprawnień są zbieżne ze sobą”[246]. Należy też podkreślić, że „Wymienione wyraźnie w przepisach ustawowych przyszłe prawa nasciturusa nie wyczerpują ich katalogu. Dla ustalenia, czy określone, przyszłe prawo dziecka nienarodzonego istnieje i podlega ochronie, decydujące znaczenie ma ocena sytuacji, z której prawo takie może wynikać, przy uwzględnieniu zasady ochrony dobra dziecka. (…) Określone prawa wynikają zatem nie z normy art. 8 k.c., gdyż przepis ten nie reguluje kwestii praw nasciturusa, ale kwestię

---

[241] M. Pazdan, *Komentarz do art. 8 kc*, [w:] K. Pietrzykowski (red.), *Kodeks cywilny tom I. Komentarz. Art. 1–449[10]*, wyd. 10, Warszawa 2020, Legalis, i tam powołana literatura.
[242] S. Kalus, *Komentarz do art. 8 kc*, [w:] M. Fras, M. Habdas (red.), *Kodeks cywilny. Komentarz. Tom I. Część ogólna (art. 1-125)*, Warszawa 2018, LEX.
[243] Por. art. 927 § 2 kc.
[244] F. Longchamps de Bérier, *The status of a bearer of rights within the European legal tradition: the tradition of Rome and Jerusalem – a case study*, “Fundamina” 2013, nr 19, s. 353-356.
[245] Art. 75 § 1 ustawy z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy (T.j. Dz.U. z 2020 r. poz. 1359 z późn. zm.), dalej jako: krio, przewidujący możliwość uznania ojcostwa przed urodzeniem się dziecka już poczętego; art. 182 krio, zgodnie z którym dla dziecka poczętego, lecz jeszcze nieurodzonego, ustanawia się kuratora, jeżeli jest to potrzebne do strzeżenia przyszłych praw dziecka.
[246] Wyrok SN z dnia 04.04.1966 r., II PR 139/66, LEX; podobnie wyrok SN z dnia 26.09.1996 r., III ARN 40/96, LEX; odmiennie wyrok WSA w Białymstoku z dnia 27.10.2005 r., II SA/Bk 503/05, http://orzeczenia.nsa.gov.pl/doc/274E7CE73D (dostęp: 07.09.2020), w którym stwierdzono, że w aktualnym stanie prawnym „możność warunkowego stania się podmiotem praw przez *nasciturusa* dopuszczalna jest jedynie wówczas, gdy wynika to wprost z przepisów szczególnych”.

zdolności prawnej, lecz z przepisów szczególnych, które dotyczą jedynie praw przyszłych, nabywanych przez dziecko dopiero po urodzeniu. Chodzi zatem o zabezpieczenie i ochronę praw dziecka poczętego, w oderwaniu od zagadnienia zdolności prawnej”[247].

W literaturze z zakresu ochrony danych osobowych również rozważano, jak należy traktować informacje o *nasciturusie* – czy należy traktować je jak dane osobowe. Zdaniem A. Drozda, do momentu urodzenia informacje dotyczące *nasciturusa* podlegają ochronie jako dane osobowe jego matki, zaś od momentu urodzenia się żywego dziecka można mówić „o danych osobowych dziecka, którymi są także informacje z okresu prenatalnego”[248]. Za uznaniem informacji pochodzących z okresu prenatalnego za dane osobowe w przypadku urodzenia się żywego dziecka opowiadają się też inni przedstawiciele doktryny[249]. Ten pogląd zasługuje moim zdaniem na aprobatę. Informacje o *nasciturusie* dotyczą najczęściej stanu jego zdrowia – wyników badań, przeprowadzonych procedur medycznych i leczenia, danych genetycznych[250], a także danych biometrycznych, wizerunku[251] – co jest szczególnie istotne przy coraz powszechniejszym stosowaniu badań ultrasonograficznych w technologii trójwymiarowej, pozwalających nawet na odtworzenie rysów twarzy[252], czy w czterowymiarowej, tj. gdy nagrywany jest krótki film, ukazujący precyzyjnie wygląd dziecka i jego zachowania – który może być następnie, przykładowo, opublikowany na portalu społecznościowym przez rodziców. Pozbawienie człowieka ochrony praw i wolności w związku z przetwarzaniem danych pozyskanych na najwcześniejszym etapie jego życia byłoby nie do pogodzenia z celami, jakie przyświecają przepisom o ochronie danych osobowych, oraz z samą definicją danych osobowych. Ponadto stoję na stanowisku, że ze względu na niemożność przewidzenia, czy *nasciturus* urodzi się żywy – co sprawiłoby, że informacje z okresu prenatalnego stałyby się danymi osobowymi – powinny być one od początku objęte swoistym domniemaniem, iż stanowią dane osobowe. Komitet Ministrów Rady Europy w swoich rekomendacjach traktujących o danych medycznych opowiedział się za

[247] Wyrok WSA we Wrocławiu z dnia 08.02.2006 r., IV SA/Wr 798/04, LEX.
[248] A. Drozd, *Pojęcie danych osobowych…*, s. 29.
[249] Por. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, Legalis; P. Fajgielski, *Ogólne rozporządzenie…*, s. 107; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis; B. Fischer, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis. Przeciwny pogląd zdają się przedstawiać D. Lubasz, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, P. Makowski, K. Witkowska-Nowakowska, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, LEX.
[250] Szerzej na ten temat por. K. Pormeister, Ł. Drożdżowski, *Protecting the Genetic Data…*, s. 54.
[251] Por. J. Haberko, *Udostępnianie i publikowanie wizerunku nasciturusa, noworodka i małego dziecka w świetle zasady dobra dziecka*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny” 2013, zeszyt 3, s. 60.
[252] E. Ferenc-Szydełko, *Wizerunek dziecka jako dobro prawnie chronione. Wybrane zagadnienia*, [w:] M. Andrzejewski (red.), *Księga jubileuszowa prof. dr hab. Tadeusza Smyczyńskiego*, Toruń 2008, s. 43.

uznaniem takich danych o *nasciturusie* za dane osobowe, zaznaczając przy tym, że ich ochrona powinna być porównywalna do ochrony danych dotyczących dziecka[253].

Zgodnie z motywem 27 preambuły rozporządzenia 2016/679, nie ma ono zastosowania do danych dotyczących osób zmarłych. Powtórzono to zastrzeżenie jeszcze dwukrotnie, w motywach 158 i 160, w kontekście przetwarzania danych osobowych do celów archiwalnych, badań historycznych i badań genealogicznych. Wyłączenie spod ochrony danych osobowych informacji o zmarłych wydaje się naturalną konsekwencją przyjęcia, że przysługuje ona osobom fizycznym. Zdolność prawna ustaje w chwili śmierci człowieka. Od tego momentu nie można mówić o istnieniu osoby fizycznej – pozostałości po niej stanowią zwłoki[254]. Dane osobowe mogą być zatem informacjami wyłącznie o żyjącym człowieku i tylko jemu przysługuje ochrona związana z ich przetwarzaniem, przewidziana w rozporządzeniu 2016/679, w tym możliwość realizacji określonych w nim uprawnień, co uzasadnia przyjęcie chwili śmierci jako kresu ochrony[255]. W motywie 27 zaznaczono jednak, że państwa członkowskie mogą przyjąć przepisy o przetwarzaniu danych osobowych osób zmarłych – pozostawiono im zatem swobodę w tym zakresie. W Polsce za taki wyjątek NSA uznał objęcie, na mocy art. 71 ustawy z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni Przeciwko Narodowi Polskiemu[256], ochroną danych osobowych przewidzianą w rozporządzeniu 2016/679 informacji gromadzonych w Bazie Materiału Genetycznego, prowadzonej przez Prezesa Instytutu Pamięci Narodowej, w której znajdują się dane o osobach zmarłych i o osobach żyjących[257]. Orzeczenie może jednak budzić kontrowersje, ponieważ wykładnia językowa i celowościowa art. 71 ustawy o IPN – który brzmi: „W działalności Instytutu Pamięci określonej w art. 1 przepisy rozporządzenia 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 04.05.2016, str. 1) stosuje się do prowadzenia Bazy" – skłania do wniosku, że zamiarem ustawodawcy było wskazanie zadania Instytutu Pamięci Narodowej, które musi być realizowane zgodnie z przepisami rozporządzenia 2016/679 i wyłącznie stosowania go w przypadku pozostałej działalności, aniżeli zamierzone objęcie informacji o zmarłych ochroną przewidzianą przez rozporządzenie 2016/679. Za taką interpretacją przemawia także okoliczność, że w przepisach dotyczących prowadzenia Bazy Materiału Genetycznego ustawodawca

[253] Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997), http://hrlibrary.umn.edu/instree/coerecr97-5.html (dostęp: 07.09.2020).
[254] M. Pazdan, *Komentarz do art. 8 kc*, [w:] K. Pietrzykowski (red.), *Kodeks cywilny…*, Legalis.
[255] P. Fajgielski, *Ogólne rozporządzenie…*, s. 107.
[256] T.j. Dz.U. z 2023 r. poz. 102, dalej jako: „ustawa o IPN".
[257] Wyrok NSA z dnia 25.08.2020 r., I OSK 3325/19, http://orzeczenia.nsa.gov.pl/doc/FCE8475960 (dostęp: 07.09.2020).

przewidział szczególne uprawnienia związane z przetwarzaniem i ochroną danych wskazując wprost, że mają one zastosowanie do informacji o osobach fizycznych (por. art. 53f ust. 3-6 ustawy o IPN). Mając na uwadze treść motywu 27 preambuły do rozporządzenia 2016/679, objęcie ochroną danych osobowych informacji o osobach zmarłych powinno wynikać wprost z przepisów poświęconych temu zagadnieniu.

Warto zasygnalizować też problem dotyczący tzw. treści cyfrowych pozostałych po osobie zmarłej, które mogą obejmować zbiór opublikowanych na portalach społecznościowych informacji, zdjęć, filmów, odnoszących się do niej, a także członków jej rodziny lub znajomych. Potencjalne rozwiązania dotyczące dysponowania tymi treściami po śmierci osoby, która je rozpowszechniła, przeważnie są rozważane w kontekście prawa spadkowego[258]. Na gruncie ochrony danych osobowych fakt śmierci osoby, która opublikowała informacje o innym żyjącym człowieku, nie przekreśla możliwości wykonywania przez niego uprawnień na podstawie rozporządzeniu 2016/679. Rozwiązania przyjęte w rozporządzeniu 2016/679 nie powinny być jednak w obecnym stanie prawnym, z wyżej wskazanych powodów, wykorzystywane w odniesieniu do przetwarzania informacji o osobie zmarłej, np. w celu doprowadzenia do ich usunięcia na podstawie art. 17 rozporządzenia 2016/679[259].

Podsumowując, ochrona danych osobowych przysługuje żyjącemu człowiekowi, a za jej początek można uznać – w zależności od przyjętego stanowiska i okoliczności – moment poczęcia lub urodzenia się żywego człowieka, zaś za koniec – chwilę jego śmierci. Poruszając się w tak zakreślonych ramach czasowych należy zastanowić się, jak zdefiniować kluczowe w niniejszej rozprawie pojęcie „dziecko". Zgodnie z definicjami podanymi w słownikach języka polskiego, dzieckiem jest „człowiek od urodzenia do wieku młodzieńczego"[260] czy też „niedorosły człowiek"[261]. Wyróżnia się pięć faz rozwoju dziecka: okres niemowlęcy (od urodzenia do połowy 2. roku życia), okres poniemowlęcy (2.–3. rok życia), okres wczesnego dzieciństwa (3.–6. rok życia), okres wczesnoszkolny (późnego dzieciństwa, dziewczęta 7.–10., chłopcy 7.–12. rok życia), okres dojrzewania płciowego (dziewczęta 11.–16., chłopcy 13.–18. rok życia)[262]. Wyznaczenie

[258] M. Załucki, *Śmierć a dane w systemach teleinformatycznych – przyczynek do dyskusji*, [w:] K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Media elektroniczne. Współczesne problemy prawne*, Warszawa 2016, Legalis; M. Mądel, *Następstwo prawne treści cyfrowych na wypadek śmierci*, Warszawa 2018, Legalis; P. Budrewicz, *Postanowienia dotyczące dziedziczenia profilu zawarte w regulaminie portalu Facebook a prawo polskie*, „Prawo mediów elektronicznych" 2018, nr 3; K. Osajda, Prawo spadkowe (w) przyszłości. Perspektywy rozwoju prawa spadkowego, „Monitor Prawniczy" 2019, nr 2.

[259] Za uznaniem, w ograniczonym zakresie, prawa do prywatności, a pośrednio także ochrony danych osobowych dotyczących osoby zmarłej, opowiada się E. Harbinja, *Post-mortem privacy 2.0: theory, law, and technology*, „International Review of Law, Computers & Technology" 2017, nr 31; argumenty za rozszerzeniem ochrony na zmarłych – w świetle Konstytucji – podaje I. Lipowicz, *Konstytucyjne podstawy ochrony danych osobowych*, [w:] P. Fajgielski (red.), *Ochrona danych osobowych w Polsce…*, s. 48.

[260] *Internetowy słownik j. polskiego PWN*, https://sjp.pwn.pl/szukaj/dziecko.html (dostęp: 07.09.2020).

[261] Wielki Słownik Języka Polskiego, https://wsjp.pl/index.php?id_hasla=5040&id_znaczenia=2574901&l=5&ind=0 (dostęp: 07.09.2020).

[262] *Encyklopedia PWN*, https://encyklopedia.pwn.pl/haslo/dziecko;4008095.html, (dostęp: 07.09.2020).

tych etapów związane jest z psychofizycznym rozwojem dziecka, w którym „zmienia się zakres jego samoświadomości, działań, jakie może samodzielnie podejmować w celu obrony przysługujących mu praw, jak również obowiązków, jakie winno wypełniać w stosunku do rodziny, grupy etnicznej czy państwa”[263]. Zarówno w prawie polskim, prawie innych państw jak i międzynarodowym, występuje wiele definicji dziecka, a każda z nich przyjmowana jest na potrzeby danego aktu prawnego lub dziedziny prawa i funkcjonuje co do zasady tylko na tym gruncie[264]. Niektóre akty prawne, choć mają podstawowe znaczenie dla ochrony dziecka, w ogóle nie definiują, kto nim jest.

Konstytucja statuuje ciążący na państwie obowiązek ochrony praw dziecka. Zgodnie z jej art. 72, każdy ma prawo żądać od organów władzy publicznej ochrony dziecka przed przemocą, okrucieństwem, wyzyskiem i demoralizacją. Dziecko, które jest pozbawione opieki rodzicielskiej, ma prawo do opieki i pomocy władz publicznych. W toku ustalania praw dziecka, organy publiczne oraz osoby odpowiedzialne za dziecko są obowiązane do wysłuchania i w miarę możliwości uwzględnienia zdania dziecka. Przepis art. 72 ust. 4 Konstytucji stanowi, że kompetencje i sposób powoływania Rzecznika Praw Dziecka określa ustawa. Jest to organ, którego zadaniem jest ochrona praw – czy szerzej – dobra dziecka, jako wartości chronionej konstytucyjnie[265]. Powołanie Rzecznika Praw Dziecka – jako niezależnego od Rzecznika Praw Obywatelskich organu – świadczy o nadaniu prawom dziecka istotnej rangi i dążeniu ustawodawcy do zapewnienia im należytej ochrony[266]. Dziecko jest podmiotem wszystkich praw i wolności konstytucyjnych[267], w tym prawa do ochrony prywatności i danych osobowych. W Konstytucji nie zostało jednak zdefiniowane pojęcie dziecka, fundamentalne dla określenia kręgu podmiotów objętych ochroną. Zdaniem B. Banaszaka dzieckiem jest osoba niedojrzała, a zatem niepełnoletnia[268]. Ten wniosek wywodzi z art. 48 ust. 1 Konstytucji, który stanowi, że rodzice mają prawo do wychowania dzieci zgodnie z własnymi przekonaniami. Z kolei władza rodzicielska trwa, stosownie do art. 92 krio, do uzyskania przez dziecko pełnoletności. Pełnoletność uzyskuje się wraz z ukończeniem osiemnastego roku życia lub przez zawarcie związku małżeńskiego[269], który w szczególnych przypadkach i za zgodą sądu opiekuńczego, może

[263] D. Kuźnicka, *Prawo do tożsamości jako prawo dziecka – wybrane zagadnienia*, „Folia Iuridica Universitatis Wratislaviensis” 2016, nr 5, s. 184.
[264] B. Olszewski, *Uniwersalna definicja dziecka?*, „Przegląd Prawa i Administracji” 2011, nr 85, s. 209; M. Szuba, *Definicja dziecka na gruncie art. 304[5] kodeksu pracy – na tle porównawczym*, „Roczniki Administracji i Prawa” 2018, nr XVIII, s. 338.
[265] W. Borysiak, *Komentarz do art. 72 Konstytucji RP*, [w:] M. Safjan, L. Bosek (red.), Konstytucja RP..., Legalis.
[266] P. Jaros, *Rzecznik Praw Dziecka w Polsce: ukształtowanie Rzecznika Praw Dziecka w Polsce jako organu państwowego, komentarz do ustawy o Rzeczniku Praw Dziecka*, Warszawa 2013, s. 64.
[267] Tamże.
[268] B. Banaszak, *Komentarz do art. 48 i art. 72 Konstytucji*, Konstytucja Rzeczypospolitej Polskiej. Komentarz. Wyd. 2, Warszawa 2012, Legalis.
[269] Art. 10 kc.

zawrzeć kobieta po ukończeniu szesnastego roku życia[270]. Przepisy krio wyznaczają zatem w ten sposób kres trwania okresu dzieciństwa. Natomiast w ustawie z dnia 6 stycznia 2000 r. o Rzeczniku Praw Dziecka[271] zdefiniowano pojęcie dziecka, które ma podstawowe znaczenie dla wyznaczenia zakresu jego ochrony, ponieważ wprost określa jej początek i koniec[272]. W myśl art. 2 ust. 1 uRPD, dzieckiem jest każda istota ludzka od poczęcia do osiągnięcia pełnoletności. Ustawodawca określił więc początek i koniec szczególnej ochrony, wyznaczając dwa punkty brzegowe: moment poczęcia oraz osiągnięcie pełnoletności. Definicję tę wyróżnia spośród innych regulacji nazwanie dzieckiem wprost także dziecka w łonie matki – jest ona zatem bardzo szeroka i budząca kontrowersje, ze względu na niespójność z innymi regulacjami, głównie dotyczącymi zdolności prawnej, możliwości legalnego przerywania ciąży czy penalizacją dokonania takiego czynu niezgodnie z ustawą[273]. Jej zastosowanie jest jednak ograniczone – w orzecznictwie wyrażono stanowisko, że nie obowiązuje na gruncie innej ustawy ze względu odmienny zakres jej regulacji[274]. Biorąc pod uwagę szerokie uprawnienia Rzecznika Praw Dziecka, uważam, że trudno zgodzić się, iż definicja z art. 2 ust. 1 uRPD nie powinna oddziaływać na wykładnię innych przepisów. Uprawnienia Rzecznika Praw Dziecka zostały wskazane w art. 10 uRPD. Zalicza się do nich m.in. możliwość zbadania każdej sprawy na miejscu – nawet bez uprzedzenia, żądanie wszczęcia określonych postępowań lub branie w nich udziału, żądanie od organów władzy publicznej, organizacji lub instytucji złożenia wyjaśnień, udzielenia informacji lub udostępnienia akt i dokumentów. Podmioty te są z kolei obowiązane do współdziałania z Rzecznikiem Praw Dziecka i udzielania mu pomocy, co polega w szczególności na zapewnieniu mu dostępu do akt i dokumentów badanej sprawy, udzielaniu żądanych informacji i wyjaśnień, w tym dotyczących podstawy faktycznej i prawnej rozstrzygnięć. Rzecznik Praw Dziecka może zatem podejmować działania wobec podmiotów o zróżnicowanym zakresie kompetencji – w tym posiadających uprawnienia o charakterze władczym i niewładczym – wynikających z różnych przepisów prawa. Jeśli działania Rzecznika Praw Dziecka mają być skuteczne i realnie oddziaływać na stan przestrzegania praw dziecka, definicja zawarta w art. 2 ust. 1 uRPD powinna być podstawowym wyznacznikiem zakresu jego ochrony, obowiązującym na różnych płaszczyznach.

Na gruncie prawa międzynarodowego przyjmowanie instrumentów dotyczących ochrony praw dziecka ma swoje źródło w przekonaniu, że „dziecko z powodu niedojrzałości fizycznej i umysłowej wymaga szczególnej opieki i troski, a także odpowiedniej opieki prawnej zarówno

[270] Art. 10 §1 krio.
[271] T.j. Dz.U. z 2023 r., poz. 292, dalej jako: uRPD.
[272] P. Jaros, *Rzecznik Praw Dziecka…*, s. 79.
[273] Por. M. Rzewuski, *Definicja dziecka w Polsce. Uwagi de lege lata i de lege ferenda,* "Rejent" 2007, nr 7, s. 190.
[274] Wyrok WSA w Gliwicach z dnia 09.05.1997 r., IV SA/Gl 284/06, LEX.

przed urodzeniem, jak i po urodzeniu”[275]. O prawach dziecka traktują różne dokumenty i umowy międzynarodowe powstałe w ramach systemu ochrony ONZ[276], jednak nie definiują one pojęcia „dziecko” – dlatego za kluczowy akt prawny odnoszący się do omawianego zagadnienia należy uznać Konwencję o prawach dziecka[277], przyjętą przez Zgromadzenie Ogólne ONZ dnia 20 listopada 1989 r. W jej rozumieniu dziecko oznacza każdą istotę ludzką w wieku poniżej osiemnastu lat, chyba że wcześniej uzyska ono pełnoletność. Tak sformułowana definicja nie rozstrzyga, czy dzieckiem jest także *nasciturus*, co stanowi kompromis przeciwstawnych w tym przedmiocie stanowisk państw-stron konwencji, jednak ze względu na szerokie znaczenie terminu „istota ludzka” oraz odwołanie się do Deklaracji Praw Dziecka – w której preambule wyrażono *expressis verbis*, że ochrona przysługuje dziecku także przed urodzeniem – zdaniem T. Smyczyńskiego, KPD „jest podstawą do wykładni ku obronie życia dziecka poczętego”[278]. Również zdaniem B. Olszewskiego omawianą definicję należy rozpatrywać łącznie z treścią Deklaracji Praw Dziecka[279]. Choć te wypowiedzi odnoszą się przede wszystkim do problematyki ochrony życia dziecka, mają znaczenie także dla postrzegania ochrony innych jego praw i wolności – np. wolności od arbitralnej lub bezprawnej ingerencji w sferę jego życia prywatnego[280].

KPD ma istotne znaczenie dla ochrony praw dziecka także w ramach systemu ochrony Rady Europy. Wypracowana w Radzie Europy najważniejsza umowa międzynarodowa – Konwencja o ochronie praw człowieka i podstawowych wolności z dnia 4 listopada 1950 r.[281] – ma zapewniać każdemu człowiekowi, będącemu pod jurysdykcją państw-stron, ochronę opisanych w niej praw i wolności. Bezsporne jest więc, że przewidziana w tej konwencji ochrona przysługuje także dziecku, choć nie zawiera ona szczegółowych postanowień odnoszących się do niego, ani też go nie definiuje. Rada Europy opracowuje i wdraża swoje strategie ochrony praw dziecka, niemniej jednak jej działalność w tym obszarze bazuje na KPD[282]. Mimo, że to w dorobku Rady Europy znajduje się pierwsza konwencja regulująca ochronę osób fizycznych w związku z przetwarzaniem danych osobowych – konwencja 108 – nie zawiera ona szczególnych rozwiązań

[275] Preambuła Deklaracji Praw Dziecka, uchwalonej przez Zgromadzenie Ogólne ONZ w dniu 20 listopada 1959 r., http://libr.sejm.gov.pl/tek01/txt/onz/1959.html (dostęp: 07.09.2020).
[276] Warto zwrócić przede wszystkim uwagę na Powszechną Deklarację Praw Człowieka z 10.12.1948 r., Międzynarodowy Pakt Praw Gospodarczych, Społecznych i Kulturalnych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz. U. z 1977 r., nr 38 poz. 169).
[277] Dz.U. z 1991 r., Nr 120, poz. 526, dalej: KPD. Warto podkreślić, że prace nad konwencją zainicjowała w 1978 r. Polska, przedstawiając jej projekt przygotowany przez polskich prawników - L. Wiśniewski, *Geneza Konwencji o Prawach Dziecka i stosunek jej norm do innych aktów prawa międzynarodowego*, [w:] T. Smyczyński (red.), *Konwencja o prawach dziecka. Analiza i wykładnia*, Poznań 1999, s. 13.
[278] T. Smyczyński, *Pojęcie dziecka i jego podmiotowość*, [w:] T. Smyczyński (red.), *Konwencja o prawach dziecka…*, s. 41.
[279] B. Olszewski, *Uniwersalna definicja…*, s. 208.
[280] Art. 16 ust. 1 Konwencji o prawach dziecka.
[281] Dz.U. z 1993 r., Nr 61, poz. 284.
[282] Strategia Rady Europy na rzecz praw dziecka (2016-2021), https://rm.coe.int/strategia-rady-europy-na-rzecz-praw-dziecka-2016-2021-/1680931c80 (dostęp: 07.09.2020), s. 4.

odnoszących się do ochrony danych osobowych dotyczących dzieci. Protokół zmieniający konwencję, otwarty obecnie do ratyfikacji, tzw. konwencja 108+, ma zmienić art. 15 m.in. poprzez dodanie wzmianki o konieczności zwrócenia przez organy nadzorcze szczególnej uwagi na kwestie ochrony danych osobowych dzieci – lecz nie podjęto próby dookreślenia, kto jest dzieckiem. Warto jednak zwrócić uwagę, że w rekomendacjach Komitetu Ministrów Rady Europy poświęconych ochronie praw dziecka w środowisku cyfrowym – rozumianym jako technologie informacyjne i komunikacyjne (ICT), w tym internet, mobilne technologie i urządzenia, a także sieci cyfrowe, bazy danych, treści i usługi – na potrzeby tego dokumentu za dziecko uznano każdą osobę przed ukończeniem 18. roku życia[283].

Unia Europejska w obszarze związanym z prawami człowieka, w tym dziecka, w znacznej mierze bazuje na dorobku Rady Europy i orzecznictwie Europejskiego Trybunału Praw Człowieka[284]. Karta Praw Podstawowych UE nie określa, kim jest dziecko, choć kilkukrotnie użyto w niej pojęć „dzieci" i „każde dziecko" – przede wszystkim należy zwrócić uwagę na art. 24. Ustalenie ich znaczeń musi być więc dokonywane w drodze wykładni w odniesieniu do konkretnego stanu faktycznego i zmieniającego się kontekstu oraz funkcji tych terminów, co zdaniem S. Majkowskiej-Szulc i M. Tomaszewskiej „służy więc uniknięciu groźby zawężenia treści norm wynikających z tego przepisu, a w konsekwencji ma zapobiegać zawężaniu zakresu ochrony dziecka"[285]. Jednocześnie autorki te wskazują, że przepisy KPP były inspirowane KPD, dlatego stosując wykładnię historyczną można uznać, że zasadne jest stosowanie przyjętego w tej konwencji kryterium w definiowaniu pojęcia dziecka na gruncie art. 24 KPP[286].

Definicja dziecka zawarta w art. 1 KPD odegrała istotną rolę w toku prac nad unijną reformą ochrony danych osobowych. W uzasadnieniu do projektu rozporządzenia 2016/679, zawartym we wniosku KE z 2012 r., wskazano, że definicja dziecka (która pojawiła się w projekcie) została zaczerpnięta właśnie z KPD. Dano temu wyraz w motywie 29, który stanowił, że „Aby stwierdzić, czy dana osoba jest dzieckiem, w niniejszym rozporządzeniu należy przyjąć definicję określoną w Konwencji Narodów Zjednoczonych o prawach dziecka". Z kolei definicja dziecka zawarta w części normatywnej nie była jednak identyczna jak definicja w KPD, wbrew temu, czego można było spodziewać się po uzasadnieniu do projektu i motywie 29. Zgodnie z art. 4 pkt 18 projektu, dziecko miało oznaczać „każdą osobę w wieku poniżej 18 lat". Przyjęto zatem

[283] Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 04.07.2018, https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html (dostęp: 07.09.2020).
[284] J. Hołda, *Prawa człowieka w Unii Europejskiej*, [w:] J. Hołda, Z. Hołda, D. Ostrowska, J. A. Rybczyńska, *Prawa człowieka. Zarys wykładu*, Warszawa 2011, s. 74.
[285] S. Majkowska-Szulc, M. Tomaszewska, *Komentarz do art. 24 Karty Praw Podstawowych UE*, [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, Warszawa 2020, Legalis.
[286] Tamże.

wyłącznie kryterium wieku, a zupełnie pominięto kryterium osiągnięcia pełnoletności, do którego odwołuje się KPD. Jednak po kilkuletnim procesie legislacyjnym, w 2016 r. Parlament Europejski i Rada przyjęły ostateczny tekst aktu, w którym zrezygnowano z wprowadzenia definicji tego pojęcia i z odwołania w motywie 29 do KPD. Przyczyn można upatrywać w braku jednolitego stanowiska państw członkowskich UE. O ile zgadzam się, że zaproponowana przez KE definicja dziecka wymagała dopracowania – moje wątpliwości budzi przede wszystkim oparcie jej wyłącznie na kryterium wieku – to jej całkowite usunięcie oceniam negatywnie. Stanowi to poważne zagrożenie dla realizacji podstawowego celu reformy – jakim jest dążenie do wyeliminowania różnic w poziomie ochrony danych osobowych w UE, co uzasadniać miało zastąpienie dyrektywy rozporządzeniem – czyli przejście od harmonizacji prawa do jego ujednolicenia w tej dziedzinie. Brak jednoznacznej definicji dziecka może przykładowo powodować różnice w interpretacji organów nadzorczych ds. ochrony danych osobowych w poszczególnych państwach i podejściu podmiotów zobowiązanych do ochrony danych osobowych, co z kolei może skutkować różnym poziomem ochrony i zniweczyć postulat zapewnienia spójnej, skutecznej ochrony danych osobowych dziecka. Uważam, że recypowanie definicji dziecka z KPD byłoby pożądane i uzasadnione, ponieważ ma ona charakter uniwersalny – stronami tej konwencji jest 196 państw[287] – co oznacza, że jej postanowienia są szeroko akceptowane. Świadczy o tym również to, że stanowią swoisty wzorzec dla rozwiązań tworzonych w ramach Rady Europy czy Unii Europejskiej. Dlatego w niniejszej rozprawie będę posługiwać się pojęciem dziecka w znaczeniu nadanym mu w art. 1 KPD.

7. Świadczenie usług społeczeństwa informacyjnego jako szczególny kontekst przetwarzania danych osobowych dziecka

Za autora terminu „społeczeństwo informacyjne" uważa się Tadao Umesao, który użył tego określenia w 1963 r. w odniesieniu do japońskiej gospodarki, opierającej się na informacji i technologiach, zaś za jego popularyzatora – Kenichi Koyamę[288]. Społeczeństwo informacyjne doczekało się wielu różnych definicji, na podstawie których można zrekonstruować jego charakterystyczne cechy: oparcie gospodarki na informacji, która jest głównym czynnikiem jej rozwoju; zbieranie, przechowywanie informacji na nieznaną wcześniej skalę i przesyłanie ich za pośrednictwem szybkich sieci dzięki dynamicznemu rozwojowi technologii informacyjno-komunikacyjnych; umiejętność korzystania z tych technologii i uzyskiwania dostępu do

[287] Informacja o statusie ratyfikacji dostępna jest na stronie internetowej Wysokiego Komisarza Narodów Zjednoczonych do spraw praw człowieka: https://indicators.ohchr.org (dostęp: 29.08.2020).
[288] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999, s. 42.

informacji przez członków społeczeństwa[289]. Zgodnie z definicją przedstawioną w strategii opracowanej przez polski rząd w 2008 r., społeczeństwo informacyjne to takie, „w którym przetwarzanie informacji z wykorzystaniem technologii informacyjnych i komunikacyjnych stanowi znaczącą wartość ekonomiczną, społeczną i kulturową"[290]. Zwrócenie uwagi na te trzy obszary jest w pełni uzasadnione. Rozwój społeczeństwa informacyjnego wpływa bowiem na wszystkie sfery życia ludzi – sposób spędzania wolnego czasu, w tym rozrywkę i kulturę, relacje z innymi, model konsumpcji, pracę[291] – np. sposób jej wykonywania (przez coraz większą automatyzację), formę zatrudnienia, środowisko, w jakim jest świadczona[292]. Zainteresowanie tematyką społeczeństwa informacyjnego wzrosło w ciągu ostatnich kilkunastu lat, w związku z rozwojem gospodarki cyfrowej w Europie i aktywnością legislacyjną w UE w tym obszarze. Gospodarką cyfrową określa się gospodarkę bazującą na informacji, której przepływ nie jest „fizyczny", lecz odbywa się poprzez internet[293]. W 2000 r. 25% informacji było przechowywanych w postaci cyfrowej, zaś w 2007 r. odsetek ten wzrósł do 94%; moc obliczeniowa komputerów podwaja się co ok. 18 miesięcy[294], co obrazuje prędkość zmian.

Społeczeństwo informacyjne nie posiada definicji legalnej w przeciwieństwie do terminu „usługa społeczeństwa informacyjnego". Zgodnie z art. 4 pkt 25 rozporządzenia 2016/679, usługa społeczeństwa informacyjnego oznacza usługę w rozumieniu art. 1 ust. 1 lit. b dyrektywy 2015/1535 – czyli każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. Przepis art. 1 ust. 1 lit. b dyrektywy 2015/1535 w dalszej części doprecyzowuje (a przynajmniej wydaje się, że taki był zamiar prawodawcy) znaczenie poszczególnych elementów tej definicji. Stosownie do podpunktów i-iii, świadczenie usługi „na odległość" oznacza, że jest ona świadczona bez równoczesnej obecności stron; „drogą elektroniczną" – czyli usługa jest wysyłana i odbierana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania danych, a także jest całkowicie przesyłana, kierowana i otrzymywana za pomocą

[289] J. S. Nowak, *Społeczeństwo informacyjne - geneza i definicje*, [w:] P. Sienkiewicz, J. S. Nowak (red.), *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*, Katowice 2008, s. 25-34.
[290] Ministerstwo Spraw Wewnętrznych i Administracji, *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013*, przyjęta w grudniu 2008 r., http://www.umwd.dolnyslask.pl/fileadmin/user_upload/spoleczenstwo_informacyjne/dokumenty/Strategia_Rozwoju_Spoleczenstwa_Informacyjnego_w_Polsce.pdf (dostęp: 23.09.2020).
[291] Przykładem jest świadczenie pracy w formie zdalnej, która zyskała na popularności z powodu pandemii wirusa SARS-CoV-2 jako jeden ze sposobów na ograniczenie kontaktów między ludźmi i zmniejszenie liczby zakażeń. W czerwcu 2020 r. pracę w tej formie wykonywało 10,2% pracujących (Główny Urząd Statystyczny, *Wpływ epidemii COVID-19 na wybrane elementy rynku pracy w Polsce w II kwartale 2020 r.*, https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5820/4/2/1/wplyw_epidemii_covid-19_na_wybrane_elementy_rynku_pracy_w_polsce_w_drugim_kwartale_2020.pdf, dostęp: 23.09.2020).
[292] K. Śledziewska, R. Włoch, *Gospodarka cyfrowa. Jak nowe technologie zmieniają świat*, Warszawa 2020, s. 160.
[293] D. Tapscott, *Gospodarka cyfrowa. Nadzieje i niepokoje Ery Świadomości Systemowej*, Warszawa 1998, s. 7.
[294] D. Batorski (red.), *Cyfrowa gospodarka. Kluczowe trendy rewolucji cyfrowej. Diagnoza, prognozy, strategie reakcji*, Warszawa 2012, s. 46.

kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych; „na indywidualne żądanie odbiorcy usług" – oznacza, że usługa świadczona jest poprzez przesyłanie danych na indywidualne żądanie. Można mówić o indywidualnym żądaniu np. wówczas, gdy usługobiorca decyduje „kiedy, gdzie, ale także o jakiej konkretnej treści lub zawartości usługa ma być świadczona"[295].

Warto zwrócić szczególną uwagę na rozumienie przesłanki odpłatności – świadczenia usługi za wynagrodzeniem. TSUE przyjmuje jej szeroką interpretację, uznając, że warunek odpłatności jest spełniony także, gdy „usługodawca otrzymuje wynagrodzenie nie od usługobiorcy, lecz z przychodów uzyskiwanych z reklam emitowanych na stronie internetowej"[296], a także, gdy „bezpłatnie realizowane świadczenie jest wykonywane przez usługodawcę w celach reklamowych w odniesieniu do dóbr sprzedawanych lub usług świadczonych przez tego usługodawcę, gdyż koszt tej działalności jest wówczas zawarty w cenie sprzedaży tych dóbr lub usług"[297]. Do spełnienia tej przesłanki nie jest zatem konieczne wypłacanie usługodawcy wynagrodzenia przez wszystkie osoby, które z niej korzystają[298]. Taką interpretację przyjął belgijski organ nadzorczy ds. ochrony danych osobowych, który za usługę społeczeństwa informacyjnego uznał ankietę na temat samopoczucia uczniów, przeprowadzaną przez szkołę za pośrednictwem szkolnej, internetowej platformy[299]. Korzystanie z niej przez uczniów nie było odpłatne, jednak szkoła zawarła odpłatną umowę powierzenia przetwarzania danych osobowych z podmiotem zewnętrznym, dotyczącą tej platformy. Trudno jednak zgodzić się z tym stanowiskiem w zakresie kwalifikacji szkolnej ankiety jako usługi społeczeństwa informacyjnego, ponieważ organ pominął, trafny w świetle orzecznictwa TSUE[300] argument, że należy uwzględnić kontekst danej działalności, zwłaszcza, jeśli jest prowadzona w ramach realizacji zadań publicznych, określonych w przepisach prawa. Zgadzam się więc ze

[295] D. Lubasz, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 313.
[296] Wyrok TSUE z dnia 11.09.2014 r., C-291/13.
[297] Wyrok TSUE z dnia 15.09.2016 r., C-484/14.
[298] Wyrok TSUE z dnia 03.12.2020 r., C-62/19 i tam powołane wcześniejsze orzecznictwo.
[299] Decyzja *Autorité de protection des données* z dnia 16.06.2020 r., https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Beslissing_GK_31-2020_NL.pdf (dostęp: 20.06.2020).
[300] TSUE w wyroku z dnia 27.09.1988 r. w sprawie 263/86, stwierdził, że „17. Zasadnicza cecha wynagrodzenia wynika zatem z faktu, że stanowi ono świadczenie za daną usługę i jest zwykle uzgadniane między jej wykonawcą a odbiorcą. 18. Cecha ta nie występuje jednak w przypadku przedmiotów nauczanych w ramach krajowego systemu oświatowego. Przede wszystkim, ustanawiając i utrzymując taki system, państwo nie dąży do prowadzenia działalności obliczonej na zysk, ale wypełnia swoje obowiązki wobec własnej ludności w dziedzinie społecznej, kulturowej i oświatowej. Po drugie, przedmiotowy system jest zasadniczo finansowany ze środków publicznych a nie przez uczniów czy ich rodziców. 19. Na charakter tej działalności nie wypływa fakt, że uczniowie czy ich rodzice muszą niekiedy wnosić opłaty za nauczanie czy wpisowe wnosząc pewien wkład na pokrycie kosztów działania systemu".

stwierdzeniem, że „Usługi edukacji na odległość świadczone przez publiczne uczelnie oraz jednostki oświatowe nie będą więc stanowić usługi społeczeństwa informacyjnego”[301].

Szerokie rozumienie przesłanki świadczenia usługi za wynagrodzeniem zasługuje na aprobatę z powodu powszechnego zjawiska tzw. monetyzacji danych osobowych. Polega ono na tym, że dane osobowe traktuje się jako zasób gospodarczy, który można przekazać w zamian za świadczenie bezpłatnej usługi – innymi słowy, „zapłacić” za nią swoimi danymi osobowymi[302]. W takiej sytuacji, chociaż użytkownik nie ponosi kosztów w wymiarze ekonomicznym, jego dane osobowe są przetwarzane w szeroko pojętych celach marketingowych, nierzadko również przez podmioty współpracujące z dostawcą usługi, któremu przynosi to wymierne korzyści biznesowe. Uzasadnione wątpliwości budzi to, czy takie działanie jest przejrzyste dla użytkownika – w szczególności, gdy jest nim dziecko, np. grające w gry dostępne na internetowej platformie.

Przesłanka odpłatności została całkowicie pominięta przez polskiego ustawodawcę w ustawie, która miała implementować dyrektywę 2000/31 do polskiego porządku prawnego, czyli uśude. Ustawodawca wprowadził w niej definicję świadczenia usługi drogą elektroniczną. Zgodnie z art. 2 pkt 4 uśude, świadczeniem usługi drogą elektroniczną jest wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne. Mimo, że obie definicje są bardzo podobne, nie można ich uznać za tożsame – ich zakresy znaczeniowe „pozostają w stosunku krzyżowania”[303]. W sytuacji, gdy dana usługa będzie mieściła się zarówno w pojęciu usługi społeczeństwa informacyjnego, jak i świadczenia usługi drogą elektroniczną, zastosowanie znajdą także w adekwatnym zakresie przepisy uśude. Pojęcie usługi społeczeństwa informacyjnego powstało w prawie UE i ma charakter autonomiczny[304]. Ponadto, usługa społeczeństwa informacyjnego stanowi rodzaj usługi w rozumieniu art. 56 i 57 TFUE[305].

---

[301] P. Polański, *Europejskie prawo handlu elektronicznego. Mechanizm regulacji usług społeczeństwa informacyjnego*, Warszawa 2014, Legalis. Z tych względów przetwarzanie danych osobowych dzieci przez placówki oświatowe, w tym zdalne kształcenie uczniów, nie będzie przedmiotem analizy w niniejszej rozprawie.

[302] EIOD negatywnie odniósł się do propozycji przyjęcia wprost takiej możliwości jako rodzaju świadczenia (Opinion 8/2018 on the legislative package “A New Deal for Consumers”, https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf, dostęp: 23.09.2020), co zaproponowała KE w strategii „Nowy ład dla konsumentów” - chociaż jak wynika z uzasadnienia, celem KE było rozszerzenie ochrony konsumentów na „usługi bezpłatne” (Komunikat KE z dnia 11.04.2018 r. do Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego „Nowy ład dla konsumentów”, COM(2018) 183 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52018DC0183#footnote23, dostęp: 23.09.2020).

[303] K. Chałubińska-Jentkiewicz, J. Taczkowska-Olszewska, *Komentarz do art. 2 uśude*, *Świadczenie usług…*, Legalis.

[304] B. Fischer, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.

[305] EROD, *Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie*

Kluczowe znaczenie dla rozumienia pojęcia usługi społeczeństwa informacyjnego ma więc orzecznictwo TSUE. Termin ten występuje w wielu aktach prawnych, lecz przez to, że stanowi już część *acquis communautaire*[306], w kolejnych nie definiuje się go ponownie, lecz odsyła do dyrektywy, w której uczyniono to po raz pierwszy. Tak też jest w przypadku rozporządzeniu 2016/679, które stosowane jest bezpośrednio i nakazuje rozumieć usługę społeczeństwa informacyjnego zgodnie z definicją zawartą w unijnej dyrektywie, dlatego na gruncie ochrony danych osobowych zasadne jest odwoływanie się do niej wprost.

W załączniku I do dyrektywy 2015/1535 zawarto wykaz przykładowych usług, które nie mieszczą się w pojęciu usługi społeczeństwa informacyjnego. Znalazły się w nim usługi, które choć są świadczone przy wykorzystaniu urządzeń elektronicznych, nie spełniają przesłanki związanej z odległością (gdyż wymagają fizycznej obecności dostawcy i odbiorcy – np. „rezerwacja biletu lotniczego w biurze podróży przy fizycznej obecności klienta za pomocą sieci komputerowej"); z drogą elektroniczną (np. „dystrybucja banknotów i biletów przez automaty", usługi telefonii głosowej, telefaksowe, teleksowe[307] – porady prawne, lekarskie, marketing bezpośredni); a także świadczenia na indywidualne żądanie, czyli polegające na przesyłaniu danych bez indywidualnego zamówienia, których odbiór jest możliwy jednocześnie przez nieograniczoną liczbę odbiorców (np. przesyłanie sygnału radiowego). Przykładowo, usługą społeczeństwa informacyjnego nie jest usługa polegająca na udostępnieniu pasażerom aplikacji na smartfon, dzięki której możliwe jest m.in. nawiązywanie kontaktów pomiędzy kierowcami a osobami chcącymi skorzystać z przewozu, ponieważ jest nierozerwalnie związana z ofertą indywidualnego transportu miejskiego – a zatem stanowi „integralną część złożonej usługi, której głównym elementem jest usługa przewozowa"[308].

Znając przykłady usług, które nie są usługami społeczeństwa informacyjnego, konieczne jest zadanie pytania, co zatem mieści się w tym pojęciu. O niektórych usługach społeczeństwa informacyjnego i specyficznych dla nich regulacjach w zakresie odpowiedzialności traktują art. 12-14 dyrektywy 2000/31[309]. Do tego rodzaju usług prawodawca zaliczył transmisję w sieci telekomunikacyjnej informacji przekazanych przez usługobiorcę (w tym automatyczne, pośrednie

swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, wersja 2.0 przyjęta 8 października 2019 r., https://edpb.europa.eu/our-work-tools/our-documents/leitlinien/guidelines-22019-processing-personal-data-under-article-61b_en (dostęp: 23.09.2020).

[306] I. Wróbel, *Pojęcie usługi społeczeństwa informacyjnego w prawie wspólnotowym*, „e-Biuletyn Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej" 2017, nr 4, http://www.bibliotekacyfrowa.pl/Content/22509/Pojecie_uslugi_spoleczenstwa_informacyjnego.pdf (dostęp: 23.09.2020).

[307] Usługi tego rodzaju, polegające na przesyłaniu wiadomości, które były drukowane na długich rolkach papieru, zostały wycofane pod koniec lat 90. XX w. i zastąpione faksem (M. Płociński, *Dalekopis - historia teleksu*, „Rzeczpospolita" 08.02.2012, https://www.rp.pl/artykul/809032-Dalekopis---historia-teleksu.html, dostęp: 23.09.2020).

[308] Wyrok TSUE z dnia 10.04.2018 r., C-320/16, Uber France SAS.

[309] Przepisy te zostały implementowane przez uśude w art. 12-14.

i krótkotrwałe przechowywanie tej informacji dokonywane w celu usprawnienia późniejszej transmisji informacji na żądanie innych usługobiorców – tzw. *caching*), zapewnianie dostępu do sieci telekomunikacyjnej, przechowywanie informacji przekazanych przez usługobiorcę (tzw. *hosting*). *Hosting* jest podstawowym elementem świadczenia usług w chmurze obliczeniowej (tzw. *cloud computing*). Istnieje wiele definicji pojęcia „chmura obliczeniowa". W niniejszej rozprawie będę posługiwała się nim w rozumieniu zgodnym z następującą definicją: „Chmura obliczeniowa to zorientowany na usługach i oparty na internecie sposób świadczenia usług teleinformatycznych na żądanie"[310]. Tak pojmowaną chmurę obliczeniową można uznać za typowy przykład usługi społeczeństwa informacyjnego. W poszukiwaniu innych warto sięgnąć do motywu 18 dyrektywy 2000/31 – wskazano w nim: sprzedaż towarów przez internet (choć z zastrzeżeniem, że wyłączona jest z tego dostawa towarów lub świadczenie usług nie za pośrednictwem internetu), oferowanie informacji (także handlowych), narzędzia umożliwiające szukanie, dostęp oraz pozyskiwanie danych.

W orzecznictwie TSUE za usługę społeczeństwa informacyjnego uznano usługę polegającą na umożliwieniu, za pośrednictwem platformy elektronicznej, nawiązania kontaktu między potencjalnymi najemcami a wynajmującymi, którzy oferują krótkoterminowe zakwaterowanie[311]; umożliwieniu, poprzez aplikację na smartfony, nawiązania kontaktów między osobami chcącymi odbyć podróż taksówką a kierowcami taksówek (z zastrzeżeniem, że podmiot świadczący usługę zawarł z kierowcami umowę o świadczenie usług, lecz nie określa warunków świadczonych przez nich usług przewozu)[312], umożliwieniu, za pośrednictwem podłączonego do internetu komputera, smartfonu czy tabletu, połączeń z numerem stacjonarnym lub komórkowym z wykorzystaniem technologii VoIP[313]. W literaturze jako przykłady usług społeczeństwa informacyjnego wymienia się „usługi finansowe online (bankowość internetowa, sprzedaż ubezpieczeń), sprzedaż innych usług, np. turystycznych lub wywoływania zdjęć przesłanych elektronicznie, sklepy internetowe, np. sprzedaż książek i muzyki w księgarniach internetowych, sprzętu elektronicznego, ubrań, kosmetyków, prenumerata gazet online, sprzedaż aplikacji mobilnych"[314].

Niewątpliwie do usług społeczeństwa informacyjnego można zaliczyć portale społecznościowe[315]. Przez portal rozumie się powszechnie serwis internetowy, w ramach którego

[310] A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018, s. 93.
[311] Wyrok TSUE z dnia 19.12.2019 r., C-390/18.
[312] Wyrok TSUE z dnia 03.12.2020 r., C-62/19.
[313] Wyrok TSUE z dnia 05.06.2019 r., C-142/18 (dot. funkcji SkypeOut, dostępnej w ramach oprogramowania Skype).
[314] B. Fischer, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.
[315] Grupa Robocza Art. 29, *Opinia nr 5/2009 w sprawie portali społecznościowych*, przyjęta 12.06.2009 r., https://archiwum.giodo.gov.pl/pl/1520022/2988 (dostęp: 23.09.2020), s. 5.

udostępniane są różnorodne usługi sieciowe[316]. Portal społecznościowy stanowi „internetową platformę komunikacyjną umożliwiającą osobom dołączenie do grupy lub stworzenie sieci podobnie myślących użytkowników", który charakteryzuje zazwyczaj tworzenie profilu użytkownika poprzez podanie swoich danych osobowych, umożliwienie publikowania różnych treści (np. zdjęć, filmów, artykułów, zapisków z pamiętnika), tworzenie sieci znajomych[317]. Do przykładowych form interakcji można zaliczyć komentowanie opublikowanych informacji w sposób werbalny i niewerbalny (np. poprzez ich oznaczenie ikoną, która ma wyrażać odczucia odbiorcy, taką jak znany z portalu Facebook przycisk „Lubię to!"). Zdaniem A. Zalewskiej-Bochenko, „Istotą portali społecznościowych jest możliwość wymiany informacji pomiędzy użytkownikami, dzielenia się z innymi swoimi zainteresowaniami, budowania pozytywnego wizerunku tak osoby prywatnej, jak i firmy"[318]. Istnieją różne rodzaje portali społecznościowych, które są przykładowo adresowane do określonych grup osób (np. portale branżowe, portale dla dzieci), mają służyć ściśle określonym celom (np. tzw. portale kariery, platformy sprzedażowe).

Warto rozważyć także, czy do usług społeczeństwa informacyjnego można zaliczyć usługi związane z IoT. Składają się na nie dwa komponenty: pierwszy, fizyczny, czyli samo urządzenie, np. zabawka, oraz drugi, pozwalający na korzystanie z jej zaawansowanych funkcji, np. aplikacja umożlwiająca prowadzenie komunikacji z dzieckiem, jednocześnie przesyłająca dane do zewnętrznego serwisu lub, przykładowo, udostępniająca nagrane wypowiedzi dziecka rodzicom, również za pośrednictwem tej aplikacji[319]. Drugi z ww. komponentów, spełniający przesłanki z art. 1 ust. 1 lit. b dyrektywy 2015/1535, należy uznać za usługę społeczeństwa informacyjnego.

Świadczenie usług społeczeństwa informacyjnego można uznać za szczególny kontekst przetwarzania danych osobowych dziecka ze względu na związane z nimi specyficzne ryzyka. Zaliczyć można do nich przede wszystkim zbieranie wielu danych osobowych, które nierzadko nie są niezbędne do świadczenia usługi, lecz są wykorzystywane w celu dalszego przetwarzania w celach marketingowych bez świadomości osoby, której dotyczą. Wykorzystanie danych osobowych w celu dopasowania treści wyświetlanych do domniemanych preferencji użytkowników portali społecznościowych może kreować ich zainteresowania i wpływać na ich rozwój, prowadzić do dyskryminacji czy wykluczenia[320]. Dlatego warto zasygnalizować problem

[316] P. Fajgielski, *Funkcjonowanie portali społecznościowych – wybrane problemy prawne*, [w:] G. Szpor, W. R. Wiewiórowski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usłu*g, Warszawa 2012, s. 134.
[317] Grupa Robocza Art. 29, *Opinia nr 5/2009…,* s. 5.
[318] A. Zalewska-Bochenko, *Portale społecznościowe jako element społeczeństwa informacyjnego*, „Studia Informatica Pomerania" 2016, nr 2.
[319] A. Rywczyńska, P. Jaroszewski, *Internet zabawek. Wsparcie dla rozwoju dziecka czy zagrożenie*, Warszawa 2018, s. 7.
[320] EROD, *Guidelines 8/2020 on the targeting of social media users*, wersja do publicznych konsultacji, przyjęta 02.09.2020r., https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf (dostęp: 23.09.2020), s. 7.

zbierania danych osobowych należących do szczególnych kategorii – przekazywanych świadomie, np. w przypadku opisywania na portalu społecznościowym swoich przekonań religijnych, ale także – jak się zdaje nie do końca świadomie – np. publikując zdjęcie z wizerunkiem twarzy, które następnie dzięki technikom biometrycznym pozwala na automatyczne wyszukanie tej samej osoby na wielu innych zdjęciach. Jednym z większych problemów usług społeczeństwa informacyjnego, w szczególności portali społecznościowych, jest publikowanie danych osobowych dotyczących innych osób, często nawet nie będących jego użytkownikami. Najlepszym i bardzo niepokojącym przykładem może być publikacja zdjęć dziecka przez jego rodzinę. Zjawisko to, ze względu na skalę i niefrasobliwość wielu rodziców, doczekało się powstania określenia *sharenting,* będącego połączeniem dwóch wyrazów: *share* – dzielić się, rozpowszechniać oraz *parenting* – rodzicielstwo[321]. Termin ten ma wydźwięk pejoratywny, ponieważ wiele zdjęć czy filmów publikowanych przez rodziców może ośmieszać czy wręcz upokarzać dziecko[322]. Na występowanie problemu niewłaściwego sprawowania obowiązków przez przedstawicieli ustawowych dzieci w kontekście przetwarzania ich danych z wykorzystaniem komputerów uwagę zwrócił już na początku lat 80. XX w. J. Kosik[323].

Przetwarzanie danych osobowych dziecka w związku ze świadczeniem usług społeczeństwa informacyjnego, ze względu na zakres, rodzaj dokonywanych operacji, skalę i skutki potencjalnych naruszeń praw i wolności – które nie są do końca możliwe do przewidzenia, a jednocześnie mogą być nieodwracalne i wpływać na resztę jego życia – powoduje, że interes dziecka powinien być paradygmatem przetwarzania i ochrony danych osobowych. Zgodnie z motywem 38 rozporządzenia 679/2018, dzieci wymagają szczególnej ochrony danych osobowych, która „powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich". Interes dziecka można utożsamiać z pojęciem dobra dziecka[324], które „powinno być brane pod uwagę podczas stosowania każdego przepisu prawa mającego związek z sytuacją dziecka jako dobro nadrzędne"[325]. Dobro dziecka jest klauzulą generalną[326], zatem ustalenie jego znaczenia możliwe jest w odniesieniu do konkretnego stanu

[321] A. Borkowska, M. Witkowska, *Sharenting i wizerunek dziecka w sieci. Poradnik dla rodziców*, Warszawa 2020, s. 7.
[322] Np. jeśli film przedstawia dziecko z poplamionymi spodniami, które nie zdążyło do toalety – tamże, s. 8.
[323] J. Kosik, *Komputer i prawa dziecka*, „Acta Universitatis Wratislaviensis" 1981, nr 582. Choć zasygnalizowane przez tego autora obszary ryzyka zmieniły się od tamtego czasu diametralnie, istota problemu wydaje się podobna.
[324] W. Stojanowska, *Dobro dziecka jako instrument wykładni norm konwencji o prawach dziecka oraz prawa polskiego i jako dyrektywa jego stosowania*, [w:] T. Smyczyński (red.), *Konwencja o prawach dziecka...*, s. 84. Odmiennie poglądy na temat relacji pojęcia „interes dziecka" a „dobro dziecka" por. R. Łukasiewicz, *Dobro dziecka a interesy innych podmiotów w polskiej regulacji prawnej przysposobienia*, Warszawa 2019, s. 68-70.
[325] W. Stojanowska, *Dobro dziecka…*, s. 81.
[326] Wyrok TK z dnia 28 kwietnia 2003 r., K 18/02, Dz.U. 2003 nr 83, poz. 772.

faktycznego. W literaturze wielokrotnie podejmowano próby zdefiniowania tego pojęcia, w których przeważnie wskazywano na następujące wartości: zapewnienie dziecku prawidłowego rozwoju fizycznego, psychicznego, emocjonalnego oraz intelektualnego[327]. Ochrona praw dziecka związanych z przetwarzaniem jego danych osobowych niewątpliwie jest przejawem realizacji zasady dobra dziecka, gdyż potencjalne naruszenia w tym obszarze mogą mieć ujemny wpływ na wszystkie wyżej wymienione aspekty jego życia.

[327] M. Bieszczad, *Dobro dziecka jako klauzula generalna – ustalenie znaczenia pojęcia dobra dziecka w XXI w.*, „Monitor Prawniczy" 2019, nr 17, s. 948.

ROZDZIAŁ II
ZASADY PRZETWARZANIA DANYCH OSOBOWYCH DZIECKA W ZWIĄZKU ZE ŚWIADCZENIEM USŁUG SPOŁECZEŃSTWA INFORMACYJNEGO

1. Charakter ogólnych zasad przetwarzania danych osobowych i podmioty zobowiązane do ich przestrzegania

Podobnie jak przed reformą, szczególne znaczenie w interpretacji przepisów o ochronie danych osobowych mają ogólne zasady przetwarzania. Zdaniem P. Fajgielskiego, szczególny charakter tych zasad polega na tym, że stanowią normy nadrzędne, a odczytywanie innych, dotyczących danych osobowych, powinno odbywać się w zgodzie z nimi[328]. Takie rozumienie zasad ogólnych przyjął Prezes UODO, podkreślając, że mają one „charakter podstawowy w odniesieniu do całej regulacji", a ponadto „nadrzędną moc i wyznaczające kierunek działania administratora w realizacji jego zadań wynikających z przepisów prawa"[329].

Obecnie ogólne zasady przetwarzania określa art. 5 ust. 1 rozporządzenia 2016/679. Obowiązek wykazywania ich przestrzegania przez administratora wynika z art. 5 ust. 2 rozporządzenia 2016/679 i motywu 74 jego preambuły. W myśl art. 4 pkt 7 rozporządzenia 2016/679, administratorem jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych[330]. Zdaniem M. Czerniawskiego, należy przez to rozumieć faktyczne, władcze decydowanie o tym, co dzieje się z danymi osobowymi[331]. Podobne stanowisko prezentują komentatorzy[332] i EROD, która wyjaśnia, że chodzi o wpływ na przetwarzanie danych osobowych polegający na wykonywaniu uprawnień decyzyjnych (*an exercise of decision-making power*) – tj.

[328] P. Fajgielski, *Zasady ogólne przetwarzania i ochrony danych osobowych*, [w:] G. Goździewicz, M. Szabłowska (red.), *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów*, Toruń 2008, s. 17.
[329] Decyzja Prezesa UODO z dnia 18.10.2019 r., sygn. ZSPU.421.3.2019, https://uodo.gov.pl/decyzje/ZSPU.421.3.2019 (dostęp: 07.02.2021).
[330] Definicja administratora nie uległa istotnym zmianom w wyniku reformy ochrony danych osobowych, dlatego można posiłkować się orzecznictwem i dorobkiem doktryny powstałym wcześniej, pod rządami uodo z 1997 r. i dyrektywy 95/46 – K. Witkowska-Nowakowska, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 214; E. Kulesza, *Nowe obowiązki administratorów danych osobowych w świetle RODO*, [w:] M. A. Mielczarek, T. Wyka (red.), *Administrator i inspektor ochrony danych osobowych. Pozycja prawna*, Warszawa 2019, s. 25.
[331] M. Czerniawski, *Instytucja współadministrowania a pojęcie „ustalania" celów i sposobów przetwarzania danych osobowych – zarys problemu*, [w:] W. R. Wiewiórowski, H. Wolska (red.), *Rok RODO*, Warszawa 2019, s. 18.
[332] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis; B. Fischer, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.

decydowaniu o kluczowych elementach przetwarzania[333], czyli jego celach i sposobach. Celem, zgodnie z definicją słownikową, jest to, do, do czego się dąży; czemu coś ma służyć[334]. Innymi słowy, definiując cel przetwarzania, należy odpowiedzieć na pytanie, po co dane mają być przetwarzane[335]. Z kolei sposoby przetwarzania, to wszystkie środki, jakie mają mu służyć – czyli przede wszystkim środki techniczne (np. sprzęt i oprogramowanie wykorzystywane do przetwarzania) i organizacyjne (np. określenie, kto ma dostęp do danych osobowych, jak długo będą przetwarzane)[336].

Pomijając sytuacje, w których status administratora został wprost nadany określonemu podmiotowi w przepisach prawa[337], co dotyczy przeważnie podmiotów publicznych, należy go ustalić w każdym indywidualnym przypadku, mając na uwadze faktyczne okoliczności przetwarzania danych osobowych[338]. Zadanie prawidłowego określenia statusu (roli) należy do samego podmiotu, który ma zamiar przetwarzać dane osobowe. Musi on zatem dokonać swoistej samooceny, kierując się kryteriami wyznaczonymi przez rozporządzenie 2016/679. EROD wskazuje na konieczność uwzględnienia kontekstu przetwarzania danych osobowych i podaje przykłady typowych relacji między podmiotem a osobami, których dane dotyczą, w których występuje on w roli administratora – mianowicie są to relacje pracodawca-pracownik; stowarzyszenie-jego członkowie; przedsiębiorstwo-jego klienci[339]. W przypadku usługi społeczeństwa informacyjnego, która jest świadczona przez dostawcę (usługodawcę) osobom fizycznym, w tym dzieciom, administratorem co do zasady jest ten dostawca. Przykładem może być świadczenie usługi polegającej na umożliwieniu przechowywania plików w chmurze czy przetwarzanie przez dostawcę portalu społecznościowego danych osobowych użytkownika, podanych przez niego w celu rejestracji i założenia konta[340], gdy dochodzi do zawarcia umowy o świadczenie usług drogą elektroniczną[341]. TSUE za administratora uznał operatora wyszukiwarki internetowej w odniesieniu do przetwarzania danych osobowych polegającego na zlokalizowaniu informacji opublikowanych lub zamieszczonych w sieci przez osoby trzecie, indeksowaniu ich w

[333] EROD, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, version 1.0 adopted on 02 September 2020, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en (dostęp: 05.02.2021), s. 10.
[334] *Internetowy słownik języka polskiego PWN*, https://sjp.pwn.pl/szukaj/cel.html (dostęp: 05.02.2021).
[335] EROD, *Guidelines 07/2020…*, s. 11.
[336] Grupa Robocza Art. 29, *Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający"*, przyjęta w dniu 16 lutego 2010 r., https://archiwum.giodo.gov.pl/pl/1520057/3595 (dostęp: 05.02.2021), s. 15.
[337] Taką możliwość przewiduje art. 4 pkt 5 rozporządzenia 2016/679, który stanowi, że jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
[338] B. Fischer, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.
[339] EROD, *Guidelines 07/2020…*, s. 11.
[340] M. Brzozowska, *Ochrona danych osobowych w sieci*, Wrocław 2012, s. 236.
[341] T. Izydorczyk, *Media społecznościowe a ochrona danych osobowych*, [w:] M. Gumularz, P. Kozik (red.), *Ochrona danych osobowych w marketingu i sprzedaży*, Warszawa 2019, Legalis.

sposób automatyczny, czasowym przechowywaniu takich informacji i ich udostępnianiu internautom w sposób uporządkowany zgodnie z określonymi preferencjami[342].

Dostawca usługi, mimo, że przetwarza dane osobowe, może nie występować w roli administratora, jeśli przetwarza je w imieniu innego podmiotu, będącego administratorem – czyli wykonuje operacje na danych osobowych w ramach powierzenia przetwarzania, jako podmiot przetwarzający w rozumieniu art. 4 pkt 8 rozporządzenia 2016/679. Przykładowo, taka sytuacja będzie miała miejsce, jeśli podmiot-administrator podejmie decyzję o korzystaniu z narzędzi oferowanych przez dostawcę usług w chmurze do realizacji zdefiniowanych przez siebie celów przetwarzania danych osobowych[343], innymi słowy okoliczność korzystania z chmury tych celów nie modyfikuje[344]. Wprawdzie art. 5 ust. 2 rozporządzenia 2016/679 stanowi, że to administrator jest zobowiązany do przestrzegania wszystkich zasad przetwarzania danych osobowych, nie oznacza to, że nie dotyczą one podmiotu przetwarzającego. Administrator może powierzyć, na podstawie umowy[345] przetwarzanie danych osobowych takiemu podmiotowi przetwarzającemu, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia 2016/679 i chroniło prawa osób, których dane dotyczą (art. 28 ust. 1 rozporządzenia 2016/679). Ponadto podmiot przetwarzający ma obowiązek pomagania administratorowi w wywiązywaniu się przez niego z obowiązków związanych z ochroną danych osobowych, np. stosownie do art. 28 ust. 3 lit. f rozporządzenia 2016/679 wspiera go w przeprowadzeniu oceny skutków dla ochrony danych osobowych. Źródłem obowiązków ciążących na podmiocie przetwarzającym będzie zatem częściowo zawarta z administratorem umowa powierzenia przetwarzania danych osobowych, a częściowo przepisy rozporządzenia 2016/679, w tym niektóre spośród ustanowionych w art. 5 zasad przetwarzania danych osobowych[346].

Jeżeli dochodzi do wspólnego ustalania celów i sposobów przetwarzania przez dwóch lub więcej administratorów, wówczas zachodzi relacja współadministrowania. Wspólne decydowanie o tym, co dzieje się z danymi osobowymi, jest wyznacznikiem zaistnienia relacji współadministrowania – warunkiem *sine qua non* nie jest natomiast posiadanie dostępu do danych

[342] Wyrok TSUE z dnia 13 maja 2014 r. w sprawie C-131/12, Google Spain SL, Google Inc. Przeciwko Agencia Española de Protección de Datos (AEPD), M. C. Gonzálezowi.
[343] EROD, *Guidelines 07/2020…*, s. 25.
[344] A. Krasuski, *Chmura obliczeniowa…,* s. 383. To stanowisko może być w mojej ocenie przyjęte także w odniesieniu do innych usług społeczeństwa informacyjnego.
[345] Lub, zgodnie z art. 28 ust. 3 rozporządzenia 2016/679, na podstawie innego wiążącego instrumentu prawnego, np. porozumienia administracyjnego w przypadku podmiotów wykonujących zadania administracji publicznej – por. M. Młotkiewicz, *Powierzenie przetwarzania w sektorze publicznym na wybranych przykładach*, „Informacja w administracji publicznej" 2020, nr 2, s. 23.
[346] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis

osobowych przez każdego ze współadministratorów[347]. Zgodnie z art. 26 rozporządzenia 2016/679, współadministratorzy w drodze wspólnych uzgodnień określają zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków. Zgodnie z wyrokiem TSUE, który zapadł wprawdzie na gruncie dyrektywy 95/46, lecz zawiera ustalenia przydatne w pewnym zakresie również w aktualnym stanie prawnym, „istnienie wspólnej odpowiedzialności niekoniecznie przekłada się na jednakową odpowiedzialność różnych podmiotów w odniesieniu do tego samego przetwarzania danych osobowych. Wręcz przeciwnie, podmioty te mogą być zaangażowane na różnych etapach tego przetwarzania i w różnym stopniu, tak że poziom odpowiedzialności każdego z nich należy oceniać przy uwzględnieniu wszystkich istotnych okoliczności danej sprawy”[348]. Wspólne uzgodnienia powinny obejmować przynajmniej kwestie związane z wykonywaniem przez osobę, której dane dotyczą, przysługujących jej praw, oraz obowiązkami w zakresie informowania o przetwarzaniu danych osobowych, o których mowa w art. 13 i 14 rozporządzenia 2016/679. Przepis art. 26 rozporządzenia 2016/679 stanowi ponadto, że współadministratorzy mogą wskazać punkt kontaktowy dla osób, których dane dotyczą, co nie wyklucza wykonywania przysługujących im uprawnień wobec każdego ze współadministratorów. W praktyce wymaga to bieżącej współpracy między tymi podmiotami, odpowiedniego przygotowania organizacyjnego i akceptacji tego, że działania w tym zakresie będą realizowane w imieniu własnym oraz pozostałych współadministratorów[349]. Wspólne uzgodnienia mogą dotyczyć także innych zagadnień, a o ich zakresie decydują strony. Dla przykładu, zasadne może być określenie, który ze współadministratorów jest odpowiedzialny za usunięcie danych osobowych lub zniszczenie nośników, które je zawierają, a także w jaki sposób, gdy cel przetwarzania zostanie już osiągnięty. Choć rozporządzenie 2016/679 nie narzuca formy wspólnych uzgodnień współadministratorów, nie ulega wątpliwości, że powinny być one wiążące dla stron[350], dlatego wskazane jest zawarcie umowy w formie pisemnej.

Na gruncie rozporządzenia 2016/679 występują zatem trzy rodzaje ról, w jakich może występować podmiot zobowiązany do jego przestrzegania – administrator, współadministrator lub podmiot przetwarzający. Można też ewentualnie mówić o podziale dychotomicznym, jeśli przyjmie się, że współadministrowanie jest jedynie pewnym wariantem administrowania. Wydaje się, że w przypadku portali społecznościowych prawidłowe ustalenie ról podmiotów uczestniczących w przetwarzaniu danych osobowych za ich pośrednictwem, a w rezultacie określenie, kto jest odpowiedzialny za ich ochronę i przestrzeganie zasad przetwarzania, jest

[347] Wyrok TSUE z dnia 05.06.2018 r. w sprawie C-210/16, Wirtschaftsakademie Schleswig-Holstein GmbH.
[348] Wyrok TSUE z dnia 29.07.2019 r. w sprawie C-40/17, Fashion ID GmbH & Co. KG.
[349] K. Gałęzowska, *Współadministrowanie danymi osobowymi – wybrane problemy prawne*, [w:] M. A. Mielczarek, T. Wyka (red.), *Administrator i inspektor…,* s. 76.
[350] EROD, *Guidelines 07/2020…*, s. 43.

bardziej skomplikowane niż w przypadku innych usług społeczeństwa informacyjnego, dlatego warto poświęcić im szczególną uwagę. Oprócz typowej relacji, jaka powstaje między dostawcą usługi a użytkownikiem-osobą fizyczną, możliwe jest bowiem zaistnienie innych. Wiele portali oferuje funkcję utworzenia profilu przedsiębiorstwa (przedsiębiorcy), popularnie określanego jako *fanpage*, w celu promowania ich produktów i usług. Niektórym przedsiębiorcom profil na portalu społecznościowym zastępuje stronę internetową i jest głównym miejscem, w którym prezentowana jest ich oferta i nawiązywane są relacje z klientami. Portale umożliwiają też prowadzenie kampanii reklamowych, w których użytkownik-przedsiębiorca może zdefiniować wg określonych przez siebie kryteriów – choć w granicach, w jakich jest to możliwe na danym portalu, najczęściej poprzez wiek, płeć, miejsce zamieszkania, a także zainteresowania, „wywnioskowane" przez portal społecznościowy w wyniku śledzenia aktywności użytkowników poprzez pliki *cookies*[351] – grupę odbiorców, którym będzie wyświetlać się jego reklama. W wyroku w sprawie C-210/16 TSUE orzekł, że podmiot prowadzący *fanpage* na portalu społecznościowym jest administratorem, a przez przyczynianie się w ww. sposób do przetwarzania danych osobowych osób odwiedzających tę stronę ponosi wspólną odpowiedzialność z dostawcą portalu[352]. Podobne stanowisko zajął TSUE w sprawie C-40/17, dotyczącej zamieszczania na stronach internetowych wtyczek, dostarczanych przez inny niż operator witryny podmiot, stwierdzając, że wspólnie z nim odpowiada za przestrzeganie przepisów o ochronie danych osobowych w zakresie operacji przetwarzania polegającej na przesyłaniu danych za pośrednictwem wtyczki[353]. Obydwa orzeczenia zapadły przed reformą ochrony danych osobowych, na podstawie dyrektywy 95/46, zatem powstaje pytanie, czy powyższe ustalenia można wprost przenieść na płaszczyznę rozporządzenia 2016/679 i instytucję współadministrowania. Kwestia ta budzi wątpliwości. Konstytutywnym elementem współadministrowania jest bowiem wspólne ustalanie z innym podmiotem celów i sposobów przetwarzania. Trudno mówić o zaistnieniu tej przesłanki w przypadku, gdy potencjalnie każdy operator witryny może w dowolnym momencie zamieścić na swojej stronie wtyczkę społecznościową, jednocześnie nie wiedząc, jakiego rodzaju operacje i w jakich celach będą wykonywane na danych po otrzymaniu ich przez dostawcę wtyczki, lub gdy podmiot prowadzący *fanpage* korzysta z raportów przygotowanych przez portal społecznościowy, ale nie ma wpływu na uwarunkowania pozyskania i analizy danych źródłowych. W sytuacji, w której nie jest możliwe poznanie szczegółów i przeanalizowanie konsekwencji przetwarzania, trudno mówić o możliwości rzetelnego wypełnienia obowiązków wynikających z rozporządzenia 2016/679. Nie

[351] Ten mechanizm, na przykładzie portalu Facebook, opisuje T. Izydorczyk, *Media społecznościowe…*, Legalis.
[352] Wyrok TSUE z dnia 05.06.2018 r. w sprawie C-210/16, Wirtschaftsakademie Schleswig-Holstein GmbH.
[353] Wyrok TSUE z dnia 29.07.2019 r. w sprawie C-40/17, Fashion ID GmbH & Co. KG.

można jednak zignorować racjonalnych dążeń przedsiębiorcy do osiągnięcia zysku poprzez promocję i sprzedaż produktów lub usług, co jest możliwe dzięki dotarciu ze swoją ofertą do jak najszerszego grona konsumentów, w tym także poprzez media społecznościowe. Rozwiązaniem problemu mogłoby być, po pierwsze, bardziej transparentne działanie podmiotów-dostawców wtyczek, m.in. operatorów portali społecznościowych, po drugie, umożliwienie operatorom witryn indywidualnego konfigurowania działania danej wtyczki. Wówczas dwie strony – operator witryny i dostawca wtyczki – miałyby realny wpływ na to, w jaki sposób przetwarzane są dane osobowe, a wprowadzenie odpowiednich ustawień można byłoby uznać za wspólne uzgodnienia współadministratorów. Wymaga to jednak gotowości dostawców wtyczek do pewnych ustępstw związanych z zakresem zbieranych informacji i ich wykorzystywaniem, co byłoby szczególnie pożądane w przypadku przetwarzania danych osobowych dzieci. W obecnym stanie prawnym wydaje się najbardziej prawidłowe uznanie, że operator portalu społecznościowego i użytkownik-przedsiębiorca prowadzący na nim swój *fanpage* są odrębnymi administratorami, którzy ponoszą odpowiedzialność za ochronę danych osobowych w zakresie, w jakim faktycznie ustalają cele i sposoby ich przetwarzania.

Innym istotnym wątkiem w ustaleniu ról podmiotów jest problem przetwarzania danych osobowych dotyczących osób, które nie są użytkownikami portalu społecznościowego (nie założyły w nim konta). Można wyróżnić dwa źródła pozyskiwania ich danych – wykorzystanie tzw. technologii śledzących (pliki *cookies*, wtyczki), o czym była mowa powyżej, oraz publikacja informacji przez inną osobę będącą użytkownikiem. Co do zasady, zgodnie z art. 2 ust. 2 lit. c rozporządzenia 2016/679, nie ma ono zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze. Rozumie się przez nie działalność pozostającą bez związku z działalnością zawodową lub handlową, np. podtrzymywanie więzi społecznych oraz aktywność internetową podejmowaną w ramach takiej działalności[354]. Mogą jednak zdarzyć się wyjątki i przepisy o ochronie danych osobowych będą miały zastosowanie do działań użytkownika portalu – zdaniem Grupy Roboczej Art. 29 wtedy, gdy świadomie nie ograniczył dostępu do publikowanych przez siebie treści wyłącznie do grona znajomych[355]. Niderlandzki sąd orzekł, że publikowanie przez babcię zdjęć jej wnuka na portalach Facebook i Pinterest, w świetle braku dostatecznych informacji na temat ustawień widoczności jej profilu, a także ustalenia czy dane tego dziecka mogą być indeksowane przez wyszukiwarkę i przetwarzane przez podmioty trzecie – partnerów biznesowych operatora portalu – jest objęte

[354] Patrz motyw 18 preambuły rozporządzenia 2016/679.
[355] Grupa Robocza Art. 29, *Opinia nr 5/2009*..., s. 7. Jak słusznie podkreśla Grupa Robocza Art. 29, nie wyłącza to odpowiedzialności na zasadach ogólnych, np. z tytułu naruszenia dóbr osobistych.

zakresem rozporządzenia 2016/679[356]. W sprawie niedotyczącej wprawdzie usług społeczeństwa informacyjnego, lecz istotnej dla wykładni przesłanki przetwarzania w ramach czynności o czysto osobistym lub domowym charakterze, TSUE orzekł, że nadzór kamer wideo umieszczonych na domu rodzinnym i obejmujący nie tylko teren prywatnej posesji, ale też częściowo przestrzeń publiczną (drogę publiczną i wejście do innego domu), jest skierowany poza sferę prywatną osoby dokonującej w ten sposób przetwarzania danych i przez to nie powinien być rozumiany jako taka czynność[357]. Można zatem wywieść, że istotny jest krąg osób, których dane są przetwarzane lub którym, w przypadku portali społecznościowych i innych usług społeczeństwa informacyjnego, dane są ujawniane.

W kontekście portali społecznościowych warto jeszcze zwrócić uwagę na dodatkowe aplikacje, które są udostępniane użytkownikom za ich pośrednictwem. Dostawcami aplikacji mogą być podmioty niezależne od operatora portalu, a ich cele i funkcje bardzo zróżnicowane – dzieci mogą interesować zwłaszcza gry. W opinii Grupy Roboczej Art. 29 dostawcy takich aplikacji również mogą być administratorami i rekomendowane jest wprowadzenie dla nich ograniczeń w dostępie do danych przetwarzanych przez portal[358].

Od dodatkowych aplikacji dostępnych na portalach należy odróżnić samodzielne, które można pobrać na urządzenie i które również należą do usług społeczeństwa informacyjnego. Ich przeznaczenie jest praktycznie nieograniczone – mogą dotyczyć wszystkich dziedzin życia, w tym szczególnie delikatnej sfery emocjonalnej. Przykładowo, istnieją aplikacje: do medytacji dla dzieci; pomagające stworzyć pamiętnik – „dziennik szczęścia"; zachęcające dzieci do aktywności fizycznej dzięki filmom tanecznym i ćwiczeniom jogi; wspierające budowanie odporności na stres i umiejętności radzenia sobie w trudnych sytuacjach (co ciekawe, ta aplikacja adresowana jest do dzieci poniżej 5. roku życia)[359], czy edukacyjne, np. pomagające w nauce języków obcych. Szczególnym typem aplikacji są służące do obsługi (czy powiązane z obsługą) zabawek interaktywnych (mieszczących się w pojęciu *IoT*), które niekiedy mają nawet funkcję nagrywania „rozmów" z dzieckiem[360]. Administratorem danych przetwarzanych za pośrednictwem tej

---

[356] Wyrok Sądu Rejonowego Gelderland z dnia 13.05.2020 r. w sprawie nr C/05/368427, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBGEL:2020:2521&showbutton=true&keyword=AVG, informacje o tym orzeczeniu w j. angielskim dostępne są na stronie https://gdprhub.eu/index.php?title=Rb._Gelderland_-_C/05/368427 (dostęp: 08.02.2021). Sprawą interesowały się media – zwracano uwagę na znaczenie tego orzeczenia w budowaniu świadomości użytkowników internetu na temat publikowania wizerunku innych osób, BBC News 21.05.2020, *Grandmother ordered to delete Facebook photos under GDPR*, https://www.bbc.com/news/technology-52758787 (dostęp: 21.05.2020).

[357] Wyrok TSUE z dnia 11.12.2014 r. w sprawie C-212/13 F. Ryneš.

[358] Grupa Robocza Art. 29, *Opinia nr 5/2009…*, s. 10.

[359] Przykłady pochodzą z przewodnika po aplikacjach dla dzieci, opracowanego przez organizację non-profit Internet Matters, https://www.internetmatters.org/pl/resources/wellbeing-apps-guide-for-kids/ (dostęp: 08.02.2021).

[360] Jest to wyjątkowo kontrowersyjny przykład zbierania danych osobowych dziecka. W 2017 r. głośna była sprawa lalki „My friend Cayla". Jak informowała agencja Reuters, jej używanie w Niemczech zostało zabronione, ponieważ w ocenie niemieckiej Federalnej Agencji ds. Sieci (*Bundesnetzagentur*) istniejące podatności oprogramowania powodowały poważne zagrożenie ujawnienia danych osobowych dzieci, Reuters 17.12.2017, *Germany bans talking*

aplikacji jest jej dostawca, ponieważ to on decyduje o celach i sposobach przetwarzania. Jest to więc podmiot, który powinien przestrzegać zasad przetwarzania i ochrony danych osobowych.

2. Zasada zgodności z prawem, rzetelności i przejrzystości

Zasada zgodności z prawem, rzetelności i przejrzystości została określona w art. 5 ust. 1 lit. a rozporządzenia 2016/679. Zgodnie z nią, dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. W istocie dyrektywa ta składa się z trzech elementów o fundamentalnym znaczeniu dla ochrony danych osobowych dziecka.

O zgodności z prawem (legalności) przetwarzania można mówić wówczas, gdy spełniona jest przynajmniej jedna z przesłanek uprawniających administratora do przetwarzania danych osobowych, o których mowa w art. 6, 9 i 10 rozporządzenia 2016/679. Niektóre z nich, np. art. 6 ust. 1 lit. c rozporządzenia 2016/679, odsyłają do innych przepisów prawa krajowego i unijnego – nie są więc przesłankami „samodzielnymi" – przetwarzanie musi być zgodne z tymi przepisami. Dotyczy to zarówno przepisów materialnych, proceduralnych, bez względu na ich rangę (czyli także np. rozporządzeń jako aktów wykonawczych względem ustaw)[361]. Należy jednak podkreślić, że nawet w przypadku przesłanki „samodzielnej", jaką jest np. zgoda na przetwarzanie danych osobowych, administrator jest zobowiązany zapewnić, by przetwarzanie nie naruszało praw osób, których dane dotyczą, wynikających z innych przepisów, np. dotyczących ochrony konsumentów. Innymi słowy, nawet pozyskanie zgody na przetwarzanie danych osobowych, którego okoliczności naruszają przepisy inne niż dotyczące ochrony danych osobowych (a z czego może nie zdawać sobie sprawy osoba, która tej zgody udzieliła, zwłaszcza, gdy jest dzieckiem), nie uczyni tego przetwarzania zgodnym z prawem.

Rzetelność, zgodnie z definicją słownikową, oznacza zgodność z prawdą, wiarygodność; odpowiadanie wymaganiom[362]. W anglojęzycznej wersji rozporządzenia 2016/679 użyto wyrazu *fairness*, którego znaczenie zgodnie ze słownikiem Cambridge należy odczytywać jako „sprawiedliwość"; traktowanie każdego w ten sam sposób[363]. Różnice występują jednak także w pozostałych wersjach językowych[364], przy czym w kilku dostrzeżono nawiązanie do koncepcji

doll Cayla, citing security risk, https://www.reuters.com/article/us-germany-cyber-dolls-idUSKBN15W20Q (dostęp: 08.02.202)

[361] P. Fajgielski, *Ogólne rozporządzenie…*, s. 145.

[362] *Internetowy słownik języka polskiego PWN*, https://sjp.pwn.pl/szukaj/rzetelność.html (dostęp: 07.02.2021).

[363] *Cambridge Dictionary,* https://dictionary.cambridge.org/pl/dictionary/english-polish/fairness (dostęp: 07.02.2021).

[364] Szczegółową analizę przeprowadził G. Malgieri, *The concept of Fairness in the GDPR. A linguistic and contextual interpretation*, [w:] *FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, Nowy Jork 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3517264 (dostęp: 07.02.2021).

bona fides, zwłaszcza w wersji niemieckojęzycznej (*nach Treu und Glauben*)[365]. Niuanse wynikające z różnic w tłumaczeniu powodują trudności w odczytaniu właściwego znaczenia zasady rzetelności. Co ważne, nie jest ona nowością w prawie ochrony danych osobowych – pojawiła się już w konwencji 108 i dyrektywie 95/46. Wymóg rzetelnego przetwarzania danych osobowych wynika także z art. 8 ust. 2 KPP. Wykładnia systemowa i celowościowa prowadzą zdaniem G. Malgieri do wniosku, że istotą zasady rzetelności jest wyważenie interesów administratora i osoby, której dane dotyczą, gdzie kluczowe jest wzięcie pod uwagę skutków przetwarzania oraz złagodzenie ewentualnego, niesprawiedliwego zakłócenia równowagi, zaistniałego w sytuacji „bezbronności" (*vulnerability*)[366]. Należy zgodzić się z tymi wnioskami wziąwszy pod uwagę, że ryzyko wystąpienia stanu „bezbronności" po stronie dziecka jako osoby, której dane dotyczą, w związku ze świadczeniem usług społeczeństwa informacyjnego, jest wysokie. „Bezbronność" dziecka może wynikać, przykładowo, z braku wiedzy, doświadczenia życiowego, z przesadnej ufności, charakterystycznej dla dzieci ciekawości świata i dążenia do poznawania nowych rzeczy. W porównaniu do sytuacji dziecka i sytuacji administratora-przedsiębiorcy oferującego usługę społeczeństwa informacyjnego, brak równowagi między tymi podmiotami jest oczywisty. Podobnie klarowny jest brak równowagi między interesem administratora, który ma w pierwszym rzędzie wymiar ekonomiczny[367], a interesem dziecka, który, w uproszczeniu, można określić jako prawidłowy rozwój. Zauważył i podkreślił to w motywie 75 preambuły rozporządzenia 2016/679 prawodawca unijny, zaliczając dzieci do osób „wymagających szczególnej opieki" (*vulnerable natural persons*) i wymieniając przetwarzanie ich danych osobowych jako kryterium, które powinien wziąć pod uwagę administrator analizując stopień ryzyka naruszenia praw lub wolności osób, których dane dotyczą, które może wystąpić w związku z przetwarzaniem danych osobowych.

Warto zasygnalizować, że rzetelność jest szczególnie istotna w badaniach dotyczących rozwoju tzw. sztucznej inteligencji, w kontekście etyki stosowania opartych na niej rozwiązań i zapobieganiu dyskryminacji[368]. Tam, gdzie do analizy opartej na danych osobowych dziecka wykorzystywane są algorytmy, zasada rzetelności powinna być wiodącą, a regulacje odnoszące

[365] Szerzej na ten temat por. P. Fajgielski, *Rzetelność jako ogólna zasada przetwarzania danych osobowych*, „Gdańskie Studia Prawnicze" 2021, nr 4, s. 14.
[366] G. Malgieri, *The concept of Fairness in the GDPR. A linguistic and contextual interpretation*, [w:] *FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, Nowy Jork 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3517264 (dostęp: 07.02.2021).
[367] Co więcej, dostrzega się ryzyko, że przedsiębiorca o dominującej pozycji, którego model biznesowy opiera się na przetwarzaniu danych osobowych, może intencjonalnie naruszać przepisy o ich ochronie w celu pozyskania jeszcze większej ilości danych jako najcenniejszych aktywów, źródła jego pozycji – por. I. Małobęcka-Szwast, *Naruszenie prawa ochrony danych osobowych jako nadużycie pozycji dominującej? Postępowanie Bundeskartellamt przeciwko Facebookowi*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2018, nr 8, s. 143.
[368] Berkman Klein Center, *Fairness and AI*, https://medium.com/berkman-klein-center/fairness-and-ai-c5596faddd20 (dostęp: 21.04.2020).

się do tej problematyki powinny przewidywać wymóg uwzględnienia wyjątkowej sytuacji dzieci podczas przeprowadzenia testu równowagi.

Zasada przejrzystości oznacza, że przetwarzanie danych osobowych powinno odbywać w sposób transparentny i zrozumiały dla osób, których dane dotyczą[369]. Zdaniem Grupy Roboczej Art. 29 istotą zasady przejrzystości jest to, „że osoba, której dane dotyczą, powinna zawsze być w stanie z wyprzedzeniem określić zakres i skutki przetwarzania i że nie powinna zostać później zaskoczona informacją, w jaki sposób wykorzystano jej dane osobowe"[370]. Choć zasada przejrzystości ma zastosowanie do wszystkich aspektów przetwarzania danych osobowych, przede wszystkim determinuje sposób komunikacji administratora z osobą, której dane dotyczą. Stosownie do art. 12 ust. 1 i motywu 39 preambuły rozporządzenia 2016/679, jest on zobowiązany do przekazywania informacji we wszystkich sprawach związanych z danymi osobowymi w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, w szczególności, gdy informacje są kierowane do dziecka. Dodatkowo w motywie 50 preambuły rozporządzenia 2016/679 zaakcentowano, że o spełnieniu generalnego wymogu posługiwania się jasnym i prostym językiem w przypadku komunikatów dotyczących przetwarzania danych osobowych dzieci można mówić wówczas, gdy są one sformułowane w taki sposób, by dziecko mogło je bez trudu zrozumieć. Grupa Robocza Art. 29 udzieliła ogólnych wskazówek dotyczących komunikatów, a także odniosła się do problemu porozumiewania się z dziećmi. Jej zdaniem opracowując każdą informację, bez względu na to, kto będzie jej adresatem, nie należy stosować złożonych struktur zdaniowych i językowych, posługiwać się pojęciami wieloznacznymi czy abstrakcyjnymi, językiem specjalistycznym (np. prawnym, technicznym) nadużywać strony biernej i rzeczowników. Informacje powinny być przekazane w języku, jakim posługują się osoby, do których jest kierowana[371]. Ponadto istotne jest graficzne wyodrębnienie poszczególnych fragmentów, np. poprzez wypunktowania i wcięcia w tekście[372]. Natomiast w przypadku dzieci, konieczne jest ponadto zwrócenie uwagi na odpowiedni do ich wieku styl, ton wypowiedzi i słownictwo – za wzór stawiane jest opracowanie KPD w wersji przyjaznej dzieciom[373]. Grupa Robocza Art. 29 zachęca także do przedstawiania informacji przy użyciu grafik, np. piktogramów,

[369] P. Drobek, *Komentarz do art. 5 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 328.
[370] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679* przyjęte dnia 29 listopada 2017 r. (zmienione i przyjęte w dniu 11 kwietnia 2018 r.), https://www.uodo.gov.pl/pl/3/1343 (dostęp: 07.02.2021), s. 8.
[371] Niderladzki organ nadzorczy stwierdził naruszenie przez TikTok Inc. art. 12 ust. 1 rozporządzenia 2016/679, polegające na zamieszczeniu w aplikacji TikTok – z której korzystają dzieci mieszkające w Niderlandach – polityki prywatności wyłącznie w j. angielskim i nałożył na ten podmiot administracyjną karę pieniężną w wysokości 750 tys. euro (decyzja *Autoriteit Persoonsgegevens* z dnia 09.04.2021 r., https://www.autoriteitpersoonsgegevens.nl/en/news/tiktok-fined-violating-children's-privacy, dostęp: 01.08.2021).
[372] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości...,* s. 11.
[373] UN Convention on the Rights of the Child in Child Friendly Language, https://sites.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf (dostęp: 07.02.2021).

komiksów, kreskówek czy animacji[374]. Podobne rozwiązania w przypadku komunikatów kierowanych do dzieci w wieku 6-9 lat rekomenduje brytyjski organ nadzorczy ds. ochrony danych osobowych[375]. Słusznie zauważa, że poziom szczegółowości i forma przedstawienia informacji powinna być dostosowana do wieku dziecka[376]. W przypadku najmłodszych dzieci, które nie umieją jeszcze czytać, Grupa Robocza Art. 29 i brytyjski organ sugerują opracować komunikaty skierowane do opiekunów prawnych. Z kolei w przypadku dzieci powyżej 5 roku życia, ICO sugeruje dwutorowe informowanie o przetwarzaniu danych osobowych dziecka – opracowanie dwóch odrębnych komunikatów dla opiekuna prawnego i dziecka[377], a nie tylko skierowanego do dziecka. Takie rozwiązanie zasługuje na aprobatę. Informacje przekazane opiekunowi prawnemu mogą być wówczas bardziej szczegółowe i skomplikowane, a dzięki dostępowi do nich będzie mógł świadomie zdecydować, czy chce podjąć dodatkowe działania (np. porozmawiać z dzieckiem, ustalić z nim zasady korzystania z usługi, doprowadzić do zaprzestania korzystania z niej lub w ogóle tego nie rozpocząć). Komunikaty mogą być także przekazywane w formie dźwiękowej, co będzie odpowiednim rozwiązaniem w przypadku urządzeń nieposiadających ekranu, na którym można wyświetlić informację w formie pisemnej[378], takich jak interaktywne zabawki.

3. Podstawy dopuszczalności przetwarzania danych osobowych jako element realizacji zasady zgodności z prawem

Podstawy dopuszczalności przetwarzania danych osobowych określa enumeratywnie art. 6 lit. a-f rozporządzenia 2016/679. Musi zaistnieć przynajmniej jedna z wymienionych w nim przesłanek, by przetwarzanie danych osobowych było zgodne z prawem[379]. Należą do nich sytuacje, w których: osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów; przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy; przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze; przetwarzanie jest niezbędne do

[374] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…,* s. 13.
[375] ICO, *Age appropriate design: a code of practice for online services*, https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf (dostęp: 07.02.2021), s. 41.
[376] ICO wyróżnił pięć przedziałów wiekowych na potrzeby dostosowania poziomu trudności komunikatów o ochronie danych osobowych do możliwości zrozumienia ich przez dzieci: 0-5 lat (przedpiśmienność i wczesna umiejętność czytania oraz pisania); 6-9 lat (pierwsze lata szkoły podstawowej); 10-12 lat (lata przejściowe); 13-15 lat (młodsze nastolatki); 16-17 lat (starsze nastolatki - zbliżające się do dorosłości), tamże.
[377] ICO, *Age appropriate design…,* s. 41.
[378] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…,* s. 14.
[379] A. Nerka, M. Sakowska-Baryła, *Komentarz do art. 6 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.

ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej; przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią[380]. Przesłanki uprawniające administratora do przetwarzania danych osobowych są więc ściśle powiązane z celem, jakiemu przetwarzanie ma służyć. Określenie, która przesłanka jest adekwatna w konkretnym przypadku, jest obowiązkiem administratora – jak wyjaśnia EROD, „Rozpoczynając działalność, która wiąże się z przetwarzaniem danych osobowych, administrator musi zawsze poświęcić pewien czas na zastanowienie się, jaka byłaby odpowiednia zgodna z prawem podstawa planowanego przetwarzania”[381].

W przypadku niektórych rodzajów danych osobowych i operacji przetwarzania prawodawca przewidział dodatkowe, szczególne przesłanki, których spełnienie jest niezbędne, by można mówić o zadośćuczynieniu przez administratora zasadzie zgodności z prawem. Dotyczy to przetwarzania danych osobowych należących do szczególnych kategorii – których zakaz przetwarzania jest uchylony wyłącznie, jeśli zostanie spełniony przynajmniej jeden z warunków wymienionych w art. 9 ust. 2 rozporządzenia 2016/679; przetwarzania danych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa – co odbywa się na podstawie art. 6 rozporządzenia 2016/679, lecz z zastrzeżeniem dodatkowych warunków wynikających z jego art. 10; podejmowania decyzji w sposób zautomatyzowany – okoliczności uchylające zakaz takiego przetwarzania reguluje art. 22 ust. 2 rozporządzenia 2016/679; przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych – czemu poświęcony jest rozdział V rozporządzenia 2016/679.

Biorąc pod uwagę specyfikę świadczenia usług społeczeństwa informacyjnego, kluczowe znaczenie mają przesłanki wymienione w art. 6 ust. 1 lit. a, b, f rozporządzenia 2016/679 (zgoda na przetwarzanie danych osobowych, zawarcie i wykonanie umowy, realizacja prawnie usprawiedliwionego interesu administratora lub strony trzeciej). Choć podstawy prawne przetwarzania danych osobowych dzieci i dorosłych są identyczne, mogą w niektórych

[380] Zgodnie z art. 4 pkt 10 rozporządzenia 2016/679, przez „stronę trzecią” należy rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

[381] EROD, *Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679*, przyjęte 04.05.2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (dostęp: 07.02.2021), s. 5.

przypadkach występować istotne różnice w ich stosowaniu[382], co będzie przedmiotem analizy w dalszej części rozprawy.

3.1 Przetwarzanie na podstawie zgody

Stosownie do art. 6 ust. 1 lit. a rozporządzenia 2016/679, przetwarzanie jest zgodne z prawem, jeśli osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów. W art. 4 pkt 15 rozporządzenia 2016/679 zdefiniowano, czym jest zgoda osoby, której dane dotyczą – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. Z tej definicji wynikają cztery cechy zgody, które muszą wystąpić łącznie: dobrowolność, konkretność, świadomość, jednoznaczność okazanej woli-przyzwolenia na przetwarzanie.

Dobrowolność zgody polega na tym, że osoba, której dane dotyczą, ma faktyczną (a nie tylko pozorną) swobodę w podjęciu decyzji o wyrażeniu lub odmowie wyrażenia zgody, co jest przejawem jej prawa do sprawowania kontroli nad własnymi danymi w ramach autonomii informacyjnej. Ze zgodą, która nie jest dobrowolna, mamy do czynienia, gdy jest ona „wymuszona" przez administratora – gdy np. zamieszcza on oświadczenie o wyrażeniu zgody w niepodlegających negocjacjom warunkach świadczenia usługi[383]. W motywach 42 i 43 preambuły do rozporządzenia 2016/679 wyjaśniono, że wyrażenie zgody nie jest dobrowolne, jeśli osoba nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji, a także gdy nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo, że do jej wykonania zgoda nie jest niezbędna[384]. Także art. 7 ust. 4 rozporządzenia 2016/679 nakazuje uwzględnienie w szczególności, czy od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy. Ponadto zgoda nie powinna być podstawą przetwarzania w sytuacji, gdy istnieje wyraźny brak równowagi między osobą, której dane dotyczą, w

[382] A. Blecher-Prigat, *Children's Right to Privacy*, [w:] J. G. Dwyer (red.), *The Oxford Handbook of Children and the Law*, Oksford 2019, s. 366.
[383] EROD, *Wytyczne 05/2020…*, s. 8.
[384] EROD jako przykład braku dobrowolności wyrażenia zgody opisuje *casus* aplikacji mobilnej do obróbki zdjęć, która wymaga od użytkownika wyrażenia zgody na przetwarzanie danych osobowych do celów reklamy behawioralnej oraz na umożliwienie lokalizacji poprzez GPS – co nie jest niezbędne do świadczenia podstawowej usługi, lecz odmowa wyrażenia zgody powoduje, że użytkownik traci w ogóle możliwość korzystania z aplikacji, tamże.

szczególności, gdy administrator jest organem publicznym. Innym typowym przykładem relacji, w której zachodzi brak równowagi i oparcie przetwarzania na zgodzie jest bardzo ograniczone, jest stosunek pracy – ze względu na zależność pracownika od pracodawcy może wręcz oznaczać naruszenie praw pracownika[385]. Chodzi więc o rodzaj uzależnienia osoby fizycznej (np. jej sytuacji ekonomicznej) od administratora – co więc zasadniczo nie będzie dotyczyło usług społeczeństwa informacyjnego.

Konkretność zgody jest ściśle powiązana z zasadą ograniczenia celu i oznacza, że dla osoby, która ma udzielić zgody, cel przetwarzania jej danych ma być jasny i precyzyjnie określony. Zgoda na przetwarzanie musi odnosić się dokładnie do określonego przetwarzania danych i nie jest dopuszczalne jej wywnioskowanie z treści wyrażenia woli mającego inny cel[386]. Innymi słowy nie może być dorozumiana. EROD wymienia trzy warunki, jakie musi spełnić administrator przy okazji pozyskiwania zgody, by spełnić wymóg jej konkretności: konieczne jest określenie celu (jako zabezpieczenie przed jego zmianą); formułowanie zapytań o zgodę w sposób szczegółowy (tj. pozyskiwanie zgody na przetwarzanie w odmiennych celach w oddzielnych oświadczeniach – niełączeniu ich w jedno); zachowanie wyraźnego oddzielenia informacji związanych z uzyskaniem zgody od innych informacji[387]. Taki obowiązek wynika z art. 7 ust. 2 rozporządzenia 2016/679, który stanowi, że przy wyrażaniu zgody poprzez pisemne oświadczenie, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

Wymóg świadomej zgody wynika z kolei z zasady przejrzystości. O świadomej zgodzie (wyrażonej w sposób świadomy) można mówić wówczas, gdy osoba jest uprzedzona o kluczowych uwarunkowaniach planowanego przetwarzania, zanim jej udzieli. W opinii EROD, w celu umożliwienia wyrażenia zgody w sposób świadomy, niezbędne jest podanie przez administratora informacji o: tożsamości administratora; celu każdej operacji przetwarzania, w odniesieniu do której prosi się o zgodę; rodzaju danych, których dotyczy zgoda; prawie do wycofania zgody; wykorzystywaniu danych do celów zautomatyzowanego podejmowania decyzji zgodnie z art. 22 ust. 2 lit. c rozporządzenia 2016/679 (o ile dotyczy); informacje dotyczące możliwych zagrożeń związanych z przekazywaniem danych do państw trzecich, jeśli odbywa się to mimo braku decyzji stwierdzającej odpowiedni stopień ochrony oraz o odpowiednich zabezpieczeniach zgodnie z art. 46 rozporządzenia 2016/679[388]. Wątpliwości może budzić to, czy EROD słusznie rozszerza zakres informacji, które są niezbędne do pozyskania świadomej zgody,

[385] Wyrok NSA z 06.09.2011 r., I OSK 1476/10, http://orzeczenia.nsa.gov.pl/doc/9CACE93D95 (dostęp: 07.02.2021).
[386] Wyrok TSUE z dnia 01.10.2019 r., C-673/17, Planet49 GmbH.
[387] EROD, *Wytyczne 05/2020*…, s. 15.
[388] Tamże, s. 16.

skoro w motywie 42 preambuły rozporządzenia 2016/679 unijny prawodawca wyjaśnił, że aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych, a ponadto w motywie 32 wskazał, że w przypadku wyrażenia zgody w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy. Przekazanie zbyt wielu informacji umieszczonych bezpośrednio przy oświadczeniu o wyrażeniu zgody (lub w jego treści) może bowiem spowodować efekt odwrotny od zamierzonego, tj. trudność w ich zrozumieniu czy niechęć do zapoznania się z nimi ze względu na objętość tekstu, a w rezultacie pominięcie go i bezrefleksyjne wyrażenie zgody w celu szybkiego uzyskania dostępu do usługi – zwłaszcza, że administrator ma obowiązek przekazania dużo szerszych informacji o przetwarzaniu danych osobowych na podstawie art. 13 i 14 rozporządzenia 2016/679[389]. Na ryzyko „przeładowania informacyjnego" zwraca uwagę sama EROD w wytycznych o zasadzie przejrzystości, pisząc, że należy tego unikać i pożądane jest stosowanie tzw. warstwowego informowania, które może polegać na odsyłaniu do poszczególnych tematów umieszczonych w tzw. polityce prywatności[390] lub wyświetlaniu pogrupowanych tematycznie treści po ich rozwinięciu przez użytkownika.

Wymóg jednoznaczności przyzwolenia na przetwarzanie danych osobowych sprowadza się do określenia, w jakiej formie i w jaki sposób może nastąpić wyrażenie zgody. Przepis art. 4 pkt 11 rozporządzenia 2016/679 wymienia dwie możliwości: formę oświadczenia lub wyraźnego działania potwierdzającego. Motyw 32 preambuły rozporządzenia 2016/679 dostarcza istotnych wskazówek interpretacyjnych. Wyjaśniono w nim, że wyrażenie zgody może nastąpić, przykładowo, w formie pisemnego (w tym elektronicznego) lub ustnego oświadczenia, a w przypadku przeglądania strony internetowej – na zaznaczeniu okienka wyboru. Oświadczenie o wyrażeniu zgody pozyskiwane drogą elektroniczną przybiera więc najczęściej postać deklaracji o udzieleniu zgody, którą można złożyć poprzez zaznaczenie odpowiedniego pola wyboru (*checkbox*). Nie może być ono domyślnie zaznaczone, ponieważ zgoda pozyskana w ten sposób jest nieważna – nawet, jeśli była techniczna możliwość odznaczenia tego okienka przez użytkownika w celu odmówienia wyrażenia zgody[391] lub gdy domyślnie zaznaczone oświadczenie było elementem umowy, którą podpisała osoba, której dane dotyczą[392]. Podobnie nie można uznać, że osoba wyraziła zgodę, jeśli zapytana o to, milczała (nie podjęła żadnych działań). Interesującym zagadnieniem jest druga z dopuszczalnych form wyrażenia zgody – „wyraźne działanie potwierdzające" („zgoda przez działanie"). W przypadku usług społeczeństwa

[389] Ten problem zostanie szerzej omówiony w rozdziale III niniejszej rozprawy.
[390] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości*…, s. 21.
[391] Wyrok TSUE z dnia 01.10.2019 r., C-673/17, Planet49 GmbH.
[392] Wyrok TSUE z dnia 11.11.2020 r., C-61/19, Orange România SA.

informacyjnego wyrażenie zgody może nastąpić poprzez wybór ustawień technicznych, lub też na innym zachowaniu, z którego bez wątpienia wynika zgoda na przetwarzanie danych osobowych (motyw 32 preambuły rozporządzenia 2016/679). Oznacza to dużą elastyczność administratora w stosowaniu innowacyjnych sposobów pozyskiwania zgody, co potwierdzają wytyczne EROD. Podano w nich przykłady czynności, które mogą stanowić wyrażenie zgody na przetwarzanie danych osobowych, o ile osoba, której dane dotyczą, nie ma żadnych wątpliwości co do ich skutków, tj. administrator w klarowny sposób poinformował ją o tym. Takimi czynnościami może być „przesunięcie paska na ekranie, machnięcie przed inteligentną kamerą, obrócenie smartfona zgodnie z ruchem wskazówek zegara lub zakreślenie ósemki"[393]. Za wyrażenie zgody nie można natomiast uznać przeglądania, przewijania strony internetowej, ponieważ trudno odróżnić takie działanie od innych reakcji użytkownika[394].

Pozyskanie zgody w formie elektronicznej, np. poprzez formularz znajdujący się na stronie internetowej, zazwyczaj odbywa się bez jakiejkolwiek weryfikacji tożsamości osoby, która go wypełnia. Z tego względu jako dobrą praktykę można potraktować przynajmniej ogólną weryfikację, np. poprzez wysłanie e-maila na adres podany przez osobę, która wyraziła zgodę[395]. Jest to działanie, które może uchronić przed naruszeniami różnego rodzaju, czego przykładem jest przypadek wysłania przez zakład ubezpieczeń dokumentacji na błędny adres e-mail, podany przez samego klienta. Prezes UODO stanął na stanowisku, że skoro administrator dopuszcza możliwość prowadzenia komunikacji poprzez pocztę elektroniczną, powinien wdrożyć środki w celu zminimalizowania ryzyka związanego z podaniem przez klienta błędnego adresu np. poprzez wprowadzenie jego weryfikacji[396].

3.1.1 Zgoda na przetwarzanie danych osobowych dziecka

W poprzednim stanie prawnym zgoda na przetwarzanie danych osobowych również stanowiła jedną z przesłanek legalizujących przetwarzanie danych osobowych, choć kwestia jej wyrażenia przez dziecko w zasadzie nie była uregulowana[397]. Przepis art. 7 pkt 5 uodo z 1997 r. stanowił m.in., że zgoda osoby, której dane dotyczą, jest oświadczeniem woli, zaś jego treścią jest

[393] EROD, *Wytyczne 05/2020…*, s. 21.
[394] Tamże.
[395] P. Fajgielski, *Zgoda udzielana na przetwarzanie danych osobowych udzielana w Internecie*, [w:] G. Szpor (red.), *Internet. Ochrona wolności, własności i bezpieczeństwa*, Warszawa 2011, s. 39.
[396] Decyzja Prezesa UODO z dnia 09.12.2020 r., DKN.5131.5.2020, https://uodo.gov.pl/decyzje/DKN.5131.5.2020 (dostęp: 07.02.2021).
[397] Za wyjątkiem wzmianki w art. 27 ust. 2 pkt 3 uodo z 1997 r. o tym, że przetwarzanie tzw. danych wrażliwych jest dopuszczalne, jeśli jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora.

zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. W literaturze zaprezentowano trzy różne możliwe koncepcje odnoszące się do charakteru prawnego zgody na przetwarzanie danych osobowych: 1. oświadczenie woli niebędące czynnością prawną[398]; 2. czynność prawna, której trzonem jest zgoda uprawnionego; 3. jednostronna czynność prawna, której trzonem jest zgoda uprawnionego[399]. Zdaniem T. Szewca, zgoda jest jednostronną, upoważniającą czynnością prawną[400] i ten pogląd wydaje się najbardziej trafny, choć trzeba zaznaczyć, że kwestia ta nie została rozstrzygnięta jednoznacznie przez doktrynę. Aprobata tego stanowiska wydaje się jednak uprawniona w świetle definicji czynności prawnej, zgodnie z którą „jest to skonstruowana przez system prawny czynność konwencjonalna podmiotu prawa cywilnego, której treść określa – co najmniej w podstawowym zakresie – jej konsekwencje prawne"[401], a także stwierdzenia, że „Celem i istotą zgody, mającej na celu stworzenie doniosłego prawnie stosunku upoważnienia jest to, iż poprzez jej udzielenie adresat uzyskuje uprawnienia (upoważnienia) do określonego w treści zgody postępowania"[402]. W ocenie prawnej skuteczności zgody można brać pod uwagę zdolność do czynności prawnych osoby ją udzielającej[403]. W uodo z 1997 r. (ani innej ustawie) nie było przepisu, który regulowałby zdolność wyrażenia zgody na przetwarzanie danych osobowych przez dziecko, co przemawia za stosowaniem ogólnych reguł przyjętych w kc[404].

Stosownie do art. 12 kc, nie mają zdolności do czynności prawnych osoby, które nie ukończyły lat trzynastu, oraz osoby ubezwłasnowolnione całkowicie. Ograniczoną zdolność do czynności prawnych mają małoletni, którzy ukończyli lat trzynaście, oraz osoby ubezwłasnowolnione częściowo (art. 15 kc), zaś pełną zdolność do czynności prawnych nabywa się z chwilą uzyskania pełnoletności (art. 11 kc).

Zgodnie z art. 14 §1 kc, czynność prawna dokonana przez osobę, która nie ma zdolności do czynności prawnych, jest nieważna. Przepis ten dotyczy czynności prawnych jednostronnych i dwustronnych, rozporządzających i zobowiązujących, które dokonane przez osobę nieposiadającą zdolności do czynności prawnych, są dotknięte nieważnością bezwzględną i nie mogą być

[398] Tak też J. Barta i R. Markiewicz argumentując, że o zdolności do wyrażenia zgody nie decydowałby wiek (czy fakt ubezwłasnowolnienia), lecz ocena, czy określona osoba jest w stanie ocenić i zrozumieć istotę zgody, jej znaczenie i skutki. Jeśli nie, zdaniem tych autorów niezbędna byłaby zgoda przedstawiciela ustawowego - J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, s. 341.
[399] R. Adamus, *Zgoda na przetwarzanie danych osobowych osoby nieposiadającej pełnej zdolności do czynności prawnych*, „Gazeta Sądowa" 2005, nr 2, s. 23 i tam powołana literatura.
[400] T. Szewc, *Zgoda na przetwarzanie danych osobowych*, „Państwo i Prawo" 2008, nr 2, s. 90.
[401] Z. Radwański, K. Mularski, [w:] Z. Radwański, A. Olejniczak (red.), *Prawo cywilne - część ogólna. System Prawa Prywatnego. Tom 2*, wyd. III, Warszawa 2019, s. 59.
[402] Z. Banaszczyk, [w:] M. Safjan (red.), *Prawo cywilne - część ogólna. System Prawa Prywatnego. Tom 1*, wyd. II, Warszawa 2012, s. 996.
[403] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, s. 404.
[404] Tamże, s. 342.

konwalidowane[405], nawet w wyniku potwierdzenia przez przedstawicieli ustawowych. Nieważność bezwzględna oznacza, że czynność prawna nie wywołuje skutków prawnych z mocy prawa (*ipso iure*) i to od chwili jej dokonania (*ab initio*)[406]. Oznacza to, że zgoda na przetwarzanie danych osobowych wyrażona przez dziecko, które nie ukończyło trzynastu lat, obarczona jest takim właśnie skutkiem. Administrator, który przetwarza dane osobowe w takim przypadku, czyni to z naruszeniem zasady zgodności z prawem – art. 5 ust. 1 lit. a i art. 6 ust. 1 rozporządzenia 2016/679[407]. Powstaje pytanie, kto zatem może skutecznie wyrazić zgodę na przetwarzanie danych osobowych dziecka.

Zgodnie z art. 98 §1 krio, rodzice są przedstawicielami ustawowymi dziecka pozostającego pod ich władzą rodzicielską i jeżeli dziecko pozostaje pod władzą rodzicielską obojga rodziców, każde z nich może działać samodzielnie jako przedstawiciel ustawowy dziecka[408]. Reprezentacja dziecka jest jednym z elementów władzy rodzicielskiej[409]. W razie ustanowienia przez sąd opiekuńczy opieki dla dziecka, dziecko reprezentuje opiekun – przepisy o władzy rodzicielskiej stosuje się odpowiednio (art. 155 §2 krio). Ze względu na brak szczegółowych regulacji reprezentacji dziecka przez opiekuna, traktowana jest analogicznie jak zastępowanie go przez rodziców[410]. Czynność prawna dokonana przez przedstawiciela w granicach umocowania pociąga za sobą skutki bezpośrednio dla reprezentowanego (art. 95 §2 kc). Zgodę na przetwarzanie danych osobowych dziecka może zatem wyrazić jego przedstawiciel ustawowy.

Bardziej skomplikowana jest sytuacja osób posiadających ograniczoną zdolność do czynności prawnych. Co do zasady, do ważności czynności prawnej, przez którą osoba ograniczona w zdolności do czynności prawnych zaciąga zobowiązanie lub rozporządza swoim prawem, potrzebna jest zgoda jej przedstawiciela ustawowego (art. 17 kc). Powstają jednak wątpliwości, czy wyrażenie zgody na przetwarzanie danych osobowych stanowi zaciągnięcie zobowiązania – czy można za nie uznać znoszenie faktu przetwarzania danych osobowych[411]. Zdaniem T. Szewca należy udzielić odpowiedzi negatywnej, a tym samym uznać, *a contrario* do art. 17 kc, że dziecko, które ukończyło trzynasty rok życia, może skutecznie wyrazić zgodę na

[405] T. Sokołowski, *Komentarz do art. 14 kc*, [w:] A. Kidyba (red.), *Kodeks cywilny…*, s. 83.
[406] Wyrok Sądu Apelacyjnego w Warszawie z dnia 13 grudnia 2018 r., VI ACa 744/18, http://orzeczenia.waw.sa.gov.pl/content/$N/154500000003003_VI_ACa_000744_2018_Uz_2018-12-13_002 (dostęp: 07.02.2021).
[407] W przypadku przetwarzania danych osobowych należących do szczególnych kategorii – art. 9 ust. 2 lit. a rozporządzenia 2016/679.
[408] Wyjątki, irrelewantne z punktu widzenia przedmiotu niniejszej rozprawy, określa art. 98 §2 krio.
[409] S. Grobel, *Treść władzy rodzicielskiej*, [w:] J. M. Łukasiewicz (red.), *Instytucje prawa rodzinnego*, Warszawa, 2014, s. 192.
[410] J. Gajda, *Komentarz do art. 155 krio*, [w:] K. Pietrzykowski (red.), *Kodeks rodzinny i opiekuńczy. Komentarz*, Warszawa 2020, Legalis.
[411] R. Adamus, *Zgoda na przetwarzanie…*, s. 24.

przetwarzanie swoich danych osobowych[412]. Należy też zauważyć, że przepis art. 17 kc nie dotyczy czynności jednostronnych. Traktuje o nich art. 19 kc, który stanowi, że jeżeli osoba ograniczona w zdolności do czynności prawnych dokonała sama jednostronnej czynności prawnej, do której ustawa wymaga zgody przedstawiciela ustawowego, czynność jest nieważna. Czyli w razie braku takiego wymogu wynikającego z ustawy, dziecko, które ukończyło trzynasty rok życia, może skutecznie wyrazić zgodę na przetwarzanie swoich danych osobowych. Pod rządami uodo z 1997 r. R. Adamus – zauważając, że „konstrukcje cywilistyczne nie zawsze są idealnie dopasowane do istoty danych osobowych" – opowiedział się za uzyskiwaniem zgody na przetwarzanie danych osobowych osoby o ograniczonej zdolności do czynności prawnych zarówno jej przedstawiciela ustawowego, jak i samej osoby, której dane dotyczą[413]. Innym rozważanym w doktrynie rozwiązaniem było przyjęcie, że zgodę wyraża przedstawiciel ustawowy, czemu może jednak sprzeciwić się osoba o ograniczonej zdolności do czynności prawnych[414]. Obydwa stanowiska mogą powodować duże praktyczne wątpliwości, zwłaszcza pamiętając o tym, że dziecko znajduje się pod władzą rodzicielską do uzyskania pełnoletności.

Nie sposób pominąć przy tych rozważaniach doniosłych okoliczności życiowych, w których dziecko może samodzielnie decydować o swoim losie (lub przynajmniej współuczestniczyć w podjęciu decyzji), a także ponosić poważne prawne konsekwencje swoich działań. Pacjent, który ukończył szesnaście lat, ma prawo do wyrażenia zgody na przeprowadzenie badania lub udzielenie innych świadczeń zdrowotnych, a ponadto do wyrażenia sprzeciwu co do udzielenia świadczenia zdrowotnego, pomimo zgody przedstawiciela ustawowego lub opiekuna faktycznego – w takim przypadku wymagane jest zezwolenie sądu opiekuńczego[415]. W przypadku eksperymentu medycznego z udziałem dziecka, które ukończyło trzynasty rok życia, wymagana jest jego zgoda oraz zgoda przedstawiciela ustawowego, a jeżeli między tymi osobami nie ma porozumienia, sprawę rozstrzyga sąd opiekuńczy[416]. Należy też zasygnalizować kwestię odpowiedzialności karnej dziecka. Zgodnie z art. 10§1 kk, na zasadach określonych w tym kodeksie odpowiada ten, kto popełnia czyn zabroniony po ukończeniu 17 lat. Co więcej, w szczególnie uzasadnionych przypadkach – stanowiących istotne odstępstwo – odpowiedzialność karną może ponieść osoba, która ukończyła piętnaście lat (art. 10 §2 kk). Osiągnięcie określonego wieku jest jedną z przesłanek zdolności do zawinienia, czyli możliwości przypisania winy osobie,

[412] T. Szewc, *Zgoda na przetwarzanie…*, s. 90; podobne stanowisko wydają się reprezentować M. Giermak, M. Sofronów, *Zgoda na przetwarzanie danych osobowych dzieci w serwisach społecznościowych w kontekście zmian prawa europejskiego*, „Monitor Prawniczy" 2017, nr 2, s. 96.
[413] R. Adamus, *Zgoda na przetwarzanie…,* s. 24.
[414] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, s. 342.
[415] Art. 17 ust. 1 i 3 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, t.j. Dz.U. z 2020 r. poz. 849.
[416] Art. 25 ust. 3 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty, t.j. Dz. U. z 2020 r. poz. 514 z późn. zm.

ponieważ rozumie ona znaczenie czynu i może pokierować swoim postępowaniem[417]. W tym świetle należy zastanowić się, czy faktycznie zgoda na przetwarzanie danych osobowych – gdy chodzi o jej wyrażenie przez dziecko, które ukończyło trzynasty rok życia – powinna być wyrażana (lub aprobowana) przez jego przedstawiciela ustawowego.

3.1.2 Zgoda na przetwarzanie danych osobowych dziecka w związku ze świadczeniem usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku

Zgodnie z motywem 38 preambuły rozporządzenia 2016/679, zgoda osoby sprawującej władzę rodzicielską lub opiekę nie powinna być konieczna w przypadku usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku. Natomiast w części normatywnej nie ma choćby wzmianki na temat przetwarzania danych osobowych na potrzeby tego rodzaju usług – nie zostały one również zdefiniowane. Usługa profilaktyczna lub doradcza może stanowić usługę społeczeństwa informacyjnego, jeśli spełnia przesłanki, o których mowa w art. 1 ust. 1 lit. b dyrektywy 2015/1535[418].

Wprowadzenie ww. zastrzeżenia nastąpiło w wyniku poprawki Parlamentu Europejskiego. U jej źródła leżało przekonanie, że dziecko powinno mieć dostęp do pomocy w trudnych sytuacjach – takich jak przemoc – bez zgody czy wręcz nawet wiedzy przedstawiciela ustawowego[419]. Jest to zgodne ze stanowiskiem Grupy Roboczej Art. 29, która wskazała, że „W skrajnych przypadkach zasada najlepiej pojętego interesu dziecka może również być sprzeczna z wymogiem wydania zgody przez jego prawnych przedstawicieli. Najlepiej pojęty interes dziecka również w tej sytuacji musi być nadrzędny, jeżeli na przykład zagrożona jest nienaruszalność fizyczna lub psychiczna dziecka”[420]. Takie podejście zasługuje na aprobatę – zwłaszcza, gdy dziecko szuka ochrony w związku z działaniem lub zaniechaniem przedstawiciela ustawowego. Na krytykę zasługuje jednak to, że tak istotny problem został zaadresowany w lakoniczny sposób i to wyłącznie w jednym z motywów preambuły rozporządzenia 2016/679. Niesienie pomocy w sytuacjach kryzysowych może wiązać się z przetwarzaniem szerokiego zakresu danych osobowych, w tym szczególnych kategorii danych osobowych. Podmiot, który oferuje takie wsparcie i ustala cele oraz sposoby przetwarzania danych osobowych, jako administrator jest oczywiście zobowiązany do przestrzegania rozporządzenia 2016/679, nie mniej

[417] A. Grześkowiak, *Komentarz do art. 10 kk*, [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny…,* Legalis.
[418] Usługą społeczeństwa informacyjnego nie będzie zatem np. udzielanie pomocy dziecku poprzez tzw. telefon zaufania.
[419] M. Macenaite, E. Kosta, *Consent for processing children's personal data in the EU: following in US footsteps?*, "Information & Communications Technology Law" 2017, nr 2, s. 163.
[420] Grupa Robocza Art. 29, *Opinia w sprawie ochrony danych osobowych dzieci (Ogólne wytyczne i szczególny przypadek szkół)*, przyjęta dnia 11 lutego 2009 r., https://archiwum.giodo.gov.pl/pl/1520022/2991 (dostęp: 07.02.2021), s. 6.

wydaje się zasadne dookreślenie warunków przetwarzania danych osobowych do celów świadczenia usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku – a być może także zawężenie kręgu podmiotów, które mogą to czynić wyłącznie za zgodą dziecka i bez wiedzy przedstawiciela ustawowego. Posłużenie się wyłącznie kryterium przedmiotowym (rodzaj usług – choć też określony zbyt ogólnie), z pominięciem podmiotowego (kto może świadczyć usługę) i ewentualnych dodatkowych warunków, może rodzić ryzyko nadużyć, a realizacja założenia KE, że „celem takich usług jest ochrona i działanie w najlepszym interesie dziecka"[421] może być zagrożona. Należy zgodzić się ze stanowiskiem brytyjskiego organu nadzorczego, zgodnie z którym za usługę profilaktyczną lub doradczą oferowaną bezpośrednio dziecku, niewymagającą zgody przedstawiciela ustawowego, nie można uznać usług takich jak np. aplikacje ogólnie związane ze zdrowiem, kondycją fizyczną lub dobrym samopoczuciem[422], jednak brak szczegółowych regulacji prawnych sprawia, że może to budzić wątpliwości i być kwestionowane przez przedsiębiorców, którym zależy na jak najłatwiejszym prowadzeniu działalności gospodarczej.

3.1.3 Zgoda na przetwarzanie danych osobowych dziecka w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku

Przepis art. 8 rozporządzenia 2016/679 stanowi, że „Jeżeli zastosowanie ma art. 6 ust. 1 lit. a), w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody. Państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat". Przepis ten reguluje okoliczności, w których zgoda dziecka jest skuteczna; jakiego rodzaju (kategorii) danych osobowych może dotyczyć; kiedy wymagana jest zgoda lub aprobata przedstawiciela ustawowego[423]; w jakim zakresie mogą być przetwarzane dane osobowe dziecka w związku z wyrażeniem zgody lub aprobatą przedstawiciela ustawowego; zawiera też klauzulę kompetencyjną dla państw członkowskich, pozwalającą na określenie w prawie krajowym innej granicy wieku dziecka, od którego może ono samodzielnie, skutecznie wyrazić zgodę na

[421] KE, *Czy dozwolone jest gromadzenie danych dotyczących dzieci?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_pl (dostęp: 07.02.2021).
[422] ICO, *Age appropriate design…*, s. 17.
[423] Wprawdzie w rozporządzeniu 2016/679 mowa jest o „osobie sprawującej władzę rodzicielską lub opiekę nad dzieckiem", to nie ulega wątpliwości, że chodzi o osobę, która jest uprawniona do reprezentowania dziecka, zatem w świetle terminologii stosowanej w kc i krio uprawnione jest określanie tej osoby jako „przedstawiciel ustawowy".

przetwarzanie swoich danych osobowych, pod warunkiem, że nie będzie ona niższa niż trzynaście lat.

Należy wyraźnie zaznaczyć, że przepis art. 8 ust. 1 rozporządzenia 2016/679 reguluje wyłącznie kwestię zgody na przetwarzanie danych osobowych dziecka w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku – nie dotyczy wszystkich okoliczności, w których dane osobowe dziecka mogą być potencjalnie przetwarzane na podstawie zgody[424] – nie kreuje ogólnych warunków wyrażenia zgody przez dziecko[425]. Co więcej, nie obejmuje nawet wszystkich usług społeczeństwa informacyjnego – a jedynie te, które są oferowane bezpośrednio dziecku[426], choć jak słusznie zauważa E. Kosta, nie ma przeszkód, by art. 8 ust. 1 rozporządzenia 2016/679 miał zastosowanie do usług, które są oferowane zarówno dzieciom, jak i dorosłym[427]. Dodanie w art. 8 ust. 1 rozporządzenia 2016/679 do pojęcia usług społeczeństwa informacyjnego sformułowania „oferowanych bezpośrednio dziecku" można poczytywać jako próbę jego zawężenia – wyłączenie z zakresu tego przepisu usług, które choć mogą stanowić usługi społeczeństwa informacyjnego w rozumieniu art. 1 ust. 1 lit. b dyrektywy 2015/1535, z oczywistych względów nie są i nie mogą być adresowane do dzieci (np. internetowe portale z filmami pornograficznymi). Brak takiego zawężenia mógłby doprowadzić do absurdalnej sytuacji, w której dostawca tego rodzaju usług musiałby wprowadzić mechanizm pozyskiwania zgody przedstawiciela ustawowego[428].

Przez oferowanie usług bezpośrednio dziecku rozumie się usługi adresowane do niego. Uważa się, że nie są nimi takie usługi, których dostawca wyraźnie informuje, że są przeznaczone wyłącznie dla osób powyżej osiemnastego roku życia[429] i nie wskazują na to inne okoliczności[430], takie jak np. treść strony lub plany marketingowe[431]. Poza oczywistymi przykładami – gdy już w

[424] Zdaniem D. Lubasza, przepis ten ma zastosowanie także wtedy, jeśli zgoda na przetwarzanie danych osobowych wprawdzie nie dotyczy samego korzystania z usługi społeczeństwa informacyjnego – gdyż co do zasady znajdzie zastosowanie inna przesłanka legalizująca przetwarzanie (art. 6 ust.1 lit. b rozporządzenia 2016/679) – lecz obejmuje cel powiązany z korzystaniem z tej usługi, np. przetwarzanie danych osobowych do celów marketingowych - D. Lubasz, *Komentarz do art. 8 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 431.
[425] P. Fajgielski, *Zgoda na przetwarzanie danych osobowych w przepisach ogólnego rozporządzenia o ochronie danych*, „Informacja w administracji publicznej" 2016, nr 4, Legalis.
[426] EROD, *Wytyczne 05/2020…*, s. 29.
[427] E. Kosta, *Komentarz do art. 8 rozporządzenia 2016/679*, [w:] C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler (red.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oksford 2020, s. 361.
[428] Podobnie P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 8 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 7 – choć ci autorzy nie traktują sformułowania o oferowaniu usług bezpośrednio dziecku jako zawężenia pojęcia usług społeczeństwa informacyjnego wyłącznie na potrzeby art. 8 rozporządzenia 2016/679, lecz postulują zmianę dyrektywy 2015/1535, polegającą na poszerzeniu katalogu usług wyłączonych spod jego zakresu o usługi nieodpowiednie dla dzieci.
[429] R. Duminică, A. Drăghici, *The processing of personal data regarding children, according to Regulation (EU) 2016/679*, „Valahia University Law Study" Supplement 2018, s.122.
[430] D. Volosevici, *Child protection under GDPR*, „Jus et Civitas" 2019, nr 2, s. 21.
[431] EROD, *Wytyczne 05/2020…*, s. 29.

nazwie usługi pojawia się informacja, że jest ona skierowana do dzieci[432] – ocena, czy dana usługa jest skierowana bezpośrednio do dzieci, może nastręczać trudności – a od tej kwalifikacji zależy dopuszczalność powołania się przez administratora na art. 8 rozporządzenia 2016/679 i określone w nim zasady. Wydaje się, że obecnie powszechnie stosowaną praktyką jest ograniczenie się przez administratora do poinformowania w warunkach świadczenia usługi (regulaminie itp.), że usługa jest kierowana wyłącznie do osób, które ukończyły określony rok życia. Tak też funkcjonują portale społecznościowe informując, że z ich usług mogą korzystać wyłącznie osoby, które ukończyły trzynasty rok życia[433], choć powszechnie wiadomo, że korzystają z nich młodsze dzieci – co świadczy o tym, że to rozwiązanie tylko pozornie rozwiązuje problem. Częste wskazywanie trzynastego roku życia w regulaminach tego typu usług wynika z dostosowania się usługodawców do amerykańskich regulacji, a także z tego, że do czasu przyjęcia rozporządzenia 2016/679 brakowało jakichkolwiek europejskich regulacji w tym przedmiocie[434]. Słusznie zauważono, że samo stwierdzenie przez administratora, że usługa nie jest adresowana do dzieci, nie powinno być wystarczające – administrator będący dostawcą usługi społeczeństwa informacyjnego powinien mieć obowiązek ustalenia, do jakiej grupy wiekowej należą jej użytkownicy[435]. Poprzestanie na deklaracji administratora może skutkować obchodzeniem prawa, a tym samym obniżeniem poziomu ochrony danych osobowych dzieci.

Dla porównania, przepisy dotyczące ochrony prywatności dzieci w środowisku *online* obowiązujące w Stanach Zjednoczonych Ameryki obejmują swoim zakresem usługi skierowane bezpośrednio do dzieci, ale stanowią także o tym, że za usługę skierowaną do dzieci traktuje się również taką, której usługodawca wie, że gromadzi dane osobowe dzieci bezpośrednio od użytkowników innej witryny internetowej lub usługi *online* skierowanej do dzieci (*A Web site or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another Web site or online service directed to children*)[436]. Ponadto przepisy te określają kryteria, którymi należy się kierować przy kwalifikacji usługi jako skierowanej bezpośrednio do dzieci – zaliczono do nich m.in. zawartość wizualną witryny internetowej lub usługi online, występowanie postaci animowanych, muzykę,

[432] Przykładem może być YouTube Kids – „aplikacja stworzona z myślą o dzieciach" https://www.youtube.com/kids (dostęp: 07.02.2021).
[433] Takie postanowienie zawiera regulamin Facebooka (https://www.facebook.com/legal/terms/update, dostęp: 07.02.2021), Instagrama (https://help.instagram.com/581066165581870, dostęp: 07.02.2021) czy TikToka (https://www.tiktok.com/legal/terms-of-use?lang=pl-PL, dostęp: 07.02.2021).
[434] K. Mc Cullagh, *The general data protection regulation: a partial success for children on social network sites*?, [w:] T. Bräutigam, S. Miettinen (red.), *Data Protection, Privacy And European Regulation In The Digital Age*, Helsinki 2016, s. 116.
[435] I. Milkaite, V. Verdoodt, H. Martens, E. Lievens, *The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society. Roundtable Report*, Bruksela 2017, https://biblio.ugent.be/publication/8528975 (dostęp: 07.02.2021), s. 19.
[436] § 312.2 Children's Online Privacy Protection Act, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (dostęp: 07.02.2021), dalej jako: COPPA.

wiek przedstawianych osób – a także czy występują „dziecięcy celebryci" (*child celebrities*), wyświetlanie reklam produktów lub usług skierowanych do dzieci[437]. Choć ich wprowadzenie z pewnością nie rozwiązuje wszystkich problemów związanych ze stosowaniem i egzekwowaniem zasad dotyczących ochrony dzieci – co widać na przykładzie ww. portali społecznościowych o amerykańskiej proweniencji – zdefiniowanie w akcie normatywnym kryteriów, według których oceniana będzie działalność przedsiębiorcy, należy uznać za dobre rozwiązanie, sprzyjające podniesieniu poziomu ochrony dzieci z jednej strony, a z drugiej zwiększające ważną dla przedsiębiorców pewność prawa.

Dziecko, które ukończyło szesnasty rok życia, może zatem co do zasady samodzielnie i skutecznie udzielić zgody na przetwarzanie danych osobowych, jeśli zastosowanie ma art. 6 ust. 1 lit. a rozporządzenia 2016/679 – czyli jego zgoda może obejmować wyłącznie przetwarzanie tzw. danych osobowych zwykłych. Przesądza o tym odesłanie wprost do art. 6 rozporządzenia 2016/679 i jednocześnie brak odniesienia do wyraźnej zgody jako przesłanki przetwarzania szczególnych kategorii danych osobowych, czyli art. 9 ust. 2 lit. a rozporządzenia 2016/679[438]. Jeśli dziecko jest młodsze, zgodę powinien wyrazić lub zaaprobować przedstawiciel ustawowy. Przepis art. 8 ust. 2 rozporządzenia 2016/679 stanowi ponadto, że administrator, uwzględniając dostępną technologię, podejmuje rozsądne starania, by zweryfikować, czy przedstawiciel ustawowy wyraził zgodę lub ją zaaprobował. Mimo, że nie wynika to wprost z przepisów, oczywiste jest, że powyższe regulacje zobowiązują administratora nie tylko do weryfikacji, czy przedstawiciel ustawowy wyraził lub zaaprobował zgodę, lecz także do sprawdzenia, czy dziecko ukończyło szesnasty rok życia[439] – w innym przypadku administrator nie wiedziałby, czy może przetwarzać dane osobowe (czy zgoda została skutecznie udzielona), czy też powinien podjąć działania w celu zadośćuczynienia obowiązkowi, o którym mowa w art. 8 ust. 2 rozporządzenia 2016/679. Wynikają z tego dwa ważkie problemy: w jaki sposób administrator powinien zweryfikować wiek dziecka, a jeśli zachodzi taka konieczność – w jaki sposób administrator powinien sprawdzić, czy przedstawiciel ustawowy wyraził zgodę lub ją zaaprobował.

---

[437] § 312.2 COPPA.

[438] Przeciwne stanowisko prezentuje The Centre for Information Policy Leadership – amerykański *think tank*, którego członkami lub uczestnikami jego projektów jest 80 przedsiębiorstw, w tym Amazon, Apple Inc., Facebook Inc., Google, Microsoft Corporation, Twitter, Uber (https://www.informationpolicycentre.com/membership.html, dostęp: 07.02.2021) – co dowodzi, że te podmioty będą dążyć do promowania jak najbardziej korzystnych dla siebie interpretacji art. 8 ust. 1 rozporządzenia 2016/679, nawet w sytuacji, gdy jest on jasny w części, w jakiej determinuje kategorię danych osobowych, których dotyczy – *CIPL White Paper on GDPR Implementation In Respect of Children's Data and Consent* 2018, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf (dostęp: 07.02.2021), s. 7.

[439] E. Kosta, *Komentarz do art. 8 rozporządzenia 2016/679*, [w:] C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler (red.), *The EU General Data Protection Regulation…*, Oksford 2020, s. 362.

3.1.4 Weryfikacja wieku dziecka

Wobec braku jakichkolwiek wymogów przewidzianych w rozporządzeniu 2016/679 w zakresie weryfikacji wieku dziecka, ani nawet wskazówek interpretacyjnych w jego preambule, EROD podkreśla, że nie może ona prowadzić do „nadmiernego przetwarzania danych", lecz powinna być proporcjonalna do charakteru przetwarzania i związanego z nim ryzyka. Przy przetwarzaniu, które wiąże się z niskim ryzykiem, zdaniem EROD wystarczające może być zapytanie dziecka o datę urodzenia lub odebranie od niego odpowiedniego oświadczenia – co jednak nie przekreśla możliwości stosowania przez administratora dalszej weryfikacji[440]. Weryfikacja wieku poprzez datę urodzenia jest poddawana krytyce ze względu na łatwość obejścia tego zabezpieczenia. W literaturze zaprezentowano pogląd, że skoro podanie daty urodzenia jest niewystarczające, lepszą weryfikację zapewnia zapytanie o numer PESEL, choć prowadzi to do przetwarzania większej ilości danych niż jest to niezbędne do świadczenia usługi[441]. Nie zasługuje on na aprobatę, ponieważ podanie numeru PESEL nie umożliwia niezaprzeczalnej weryfikacji wieku (ani tożsamości) przez administratora-dostawcę usługi społeczeństwa informacyjnego, który nie ma prawnej ani faktycznej możliwości porównania podanego numeru z informacjami znajdującymi się w rejestrze PESEL. Inną metodę sprawdzenia wieku zaproponowała KE – jej zdaniem może polegać na zadaniu pytania, na które przeciętne dziecko nie zna odpowiedzi[442]. Biorąc pod uwagę, że weryfikacja wieku ma nastąpić w kontekście usług społeczeństwa informacyjnego – a zatem podczas korzystania przez dziecko z internetu, gdy ma dostęp do wyszukiwarek internetowych – skuteczność tej metody budzi wątpliwości.

Brytyjski organ nadzorczy proponuje pięć przykładowych metod weryfikacji wieku użytkownika, o różnym poziomie pewności i zakresie przetwarzanych informacji – wybór jednej z nich (lub zupełnie innej) należy do administratora, który powinien opierać się na wcześniej przeprowadzonej analizie ryzyka związanego z przetwarzaniem danych osobowych dziecka: 1) oświadczenie o wieku – środek ten może być dodatkowo wspierany przez techniczne środki „zniechęcające" użytkownika do podawania nieprawdziwej informacji o swoim wieku (np. blokada uruchomienia usługi po ponownym podaniu wieku, jeśli odmówiono jej świadczenia po pierwszym przyjęciu oświadczenia); 2) użycie rozwiązań opartych na tzw. sztucznej inteligencji (system automatycznie określa wiek użytkownika poprzez porównanie jego oświadczenia z

[440] EROD, *Wytyczne 05/2020…*, s. 30.
[441] M. Giermak, M. Sofronów, *Zgoda na przetwarzanie danych osobowych dzieci…,* s. 96. Pozyskiwanie numeru PESEL w celu weryfikacji wieku stanowiłoby naruszenie zasady minimalizacji danych – por. M. de Bazelaire de Ruppierre, *Komentarz do art. 8 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.
[442] KE, *Czy dozwolone jest gromadzenie danych dotyczących dzieci?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_pl (dostęp: 07.02.2021).

wnioskami z analizy sposobu interakcji z usługą – dochodzi zatem do profilowania); 3) korzystanie z usług weryfikacji wieku, dostarczanych przez podmiot trzeci (administrator otrzymuje od podmiotu trzeciego wyłącznie potwierdzenie lub zaprzeczenie, że dany użytkownik mieści się w określonej grupie wiekowej – sam nie przetwarza dodatkowych danych osobowych[443]); 4) potwierdzenie wieku przez innego użytkownika, którego pełnoletność została wcześniej sprawdzona (dotyczy to przykładowo usług opartych na subskrypcji, w którym przedstawiciel ustawowy, np. rodzic, zakłada tzw. konto główne, a następnie przydziela swoim dzieciom powiązane konta, których ustawienia może skonfigurować); 5) tzw. „twarde identyfikatory" – ICO podaje przykład paszportu (choć tego nie precyzuje – można podejrzewać, że chodzi o przesłanie skanu dokumentu), zwraca jednak uwagę na ryzyko pozyskania zbyt szerokiego zakresu danych osobowych[444]. Tego przykładu nie można uznać za trafny nie tylko ze względu na zasadę minimalizacji danych, ale przede wszystkim z powodu łatwości przerobienia skanu dokumentu z użyciem nawet najprostszego programu graficznego. Skan paszportu, dowodu osobistego czy innego dokumentu nie może być uznawany za „dowód" potwierdzający wiek czy tożsamość. Pozostałe propozycje ICO są warte uwagi, choć można wysnuć wniosek, że za wyjątkiem pierwszej z nich trudno uniknąć przy weryfikacji wieku dziecka przetwarzania dodatkowych danych osobowych lub dokonywania operacji przetwarzania, które nie są niezbędne do świadczenia samej usługi.

Problem weryfikacji wieku dziecka jest dodatkowo utrudniony przez to, że art. 8 ust. 1 rozporządzenia 2016/679 zawiera klauzulę kompetencyjną upoważniającą państwa członkowskie do obniżenia w swoim prawie granicy wiekowej, od której dziecko może wyrazić zgodę na przetwarzanie danych osobowych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku – z zastrzeżeniem, że musi ona wynosić co najmniej trzynaście lat. W literaturze poddano krytyce to, że określenie tych granic wiekowych nie było poprzedzone na etapie prac legislacyjnych nad rozporządzeniem 2016/679 przeprowadzeniem żadnych badań ani oceną skutków regulacji, a ustanowienie trzynastego roku życia jako minimalnej granicy stanowi po prostu przeniesienie na grunt prawa UE amerykańskich rozwiązań przyjętych w COPPA, korzystnych dla największych dostawców usług społeczeństwa informacyjnego[445].

[443] Działa to w ten sposób, że podmiot trzeci pozyskuje dane osobowe i według przyjętego przez siebie sposobu sprawdza wiek, a dostawcy usługi przekazuje jedynie informację o wyniku weryfikacji. ICO rekomenduje dokładne sprawdzenie wiarygodności takiego podmiotu, a także czy stosuje brytyjską normę PAS 1296:2018 – por. *Online age checking. Provision and use of online age check services. Code of Practice* (https://shop.bsigroup.com/ProductDetail?pid=000000000030328409, dostęp: 07.02.2021).
[444] ICO, *Age appropriate design…*, s. 34.
[445] K. Mc Cullagh, *The general…*, s.123-124.

W Polsce ostatecznie nie zdecydowano się na obniżenie granicy wieku, choć na etapie prac legislacyjnych nad uodo z 2018 r. taka propozycja znalazła się w dwóch pierwszych wersjach projektu[446]. Głównym argumentem za obniżeniem granicy wieku do ukończenia przez dziecko trzynastego roku życia było dążenie do przyjęcia rozwiązań spójnych z kc – a zatem kierowano się kryterium momentu osiągnięcia ograniczonej zdolności do czynności prawnych i art. 15 kc w związku z art. 19 kc jako „wzorcem regulacyjnym"[447].

Krytyczne uwagi przedstawił GIODO – opowiedział się za niekorzystaniem z możliwości obniżenia granicy wieku dziecka, ponieważ nie można, w jego ocenie, zrównać skutków wyrażenia zgody na przetwarzanie danych osobowych z zawieraniem umów powszechnie zawieranych w drobnych bieżących sprawach życia codziennego[448]. GIODO przeprowadził konsultacje z nauczycielami biorącymi udział w organizowanym przez niego programie edukacyjnym „Twoje dane – Twoja sprawa"[449] – wzięło w nich udział 79 placówek. 89% respondentów udzieliło negatywnej odpowiedzi na pytanie czy ich zdaniem „13 lat to prawidłowy wiek aby dziecko samodzielnie mogło wyrazić zgodę na przetwarzanie danych osobowych w przypadku usług społeczeństwa informacyjnego"[450]. Nauczyciele argumentowali przeważnie, że trzynastoletnie dzieci „nie mają dobrze rozwiniętej i pogłębionej autorefleksji oraz myślenia i wnioskowania dotyczącego ponoszenia konsekwencji swoich decyzji w przyszłości", a „trzy lata w rozwoju młodego człowieka to bardzo dużo"[451]. Z kolei zwolennicy obniżenia granicy wieku zauważyli, że faktycznie nawet dużo młodsze dzieci korzystają samodzielnie z portali społecznościowych czy innych usług społeczeństwa informacyjnego, co uczy je

[446] W projekcie nowej ustawy o ochronie danych osobowych z dnia 12.09.2017 r. (w art. 3) oraz z dnia 08.02.2018 r. (w art. 5) pojawił się przepis o następującym brzmieniu: „W przypadku usług świadczonych drogą elektroniczną oferowanych bezpośrednio osobie, która nie ukończyła lat trzynastu i która przebywa na terytorium Rzeczpospolitej Polskiej, gdy podstawą przetwarzania danych osobowych jest zgoda tej osoby, przetwarzanie danych osobowych możliwe jest wyłącznie po uzyskaniu uprzedniej zgody jej przedstawiciela ustawowego albo po niezwłocznym potwierdzeniu przez przedstawiciela ustawowego zgody wyrażonej przez taką osobę" (projekt ustawy o ochronie danych osobowych z dnia 12.09.2017 r. https://legislacja.rcl.gov.pl/docs//2/12302950/12457652/12457653/dokument308351.pdf; z dnia 08.02.2018 r. https://legislacja.rcl.gov.pl/docs//2/12302950/12457684/12457685/dokument334781.pdf, dostęp: 07.02.2021).

[447] Uzasadnienie do projektu nowej ustawy o ochronie danych osobowych z dnia 12.09.2017 r. (https://legislacja.rcl.gov.pl/docs//2/12302950/12457652/12457653/dokument308352.pdf, dostęp: 07.02.2021), s. 10-11.

[448] Uwagi GIODO do projektu nowej ustawy o ochronie danych osobowych z dnia 12.09.2017 r., zawarte w załączniku nr 2 do pisma GIODO z dnia 20.10.2017 r., DESiWM-070-20/77964/17 (https://legislacja.rcl.gov.pl/docs//2/12302950/12457664/12457667/dokument319357.pdf, dostęp: 07.02.2021), s. 2-3.

[449] Podstawowym celem programu „Twoje dane – Twoja sprawa" „jest poszerzenie oferty edukacyjnej placówek doskonalenia zawodowego nauczycieli, szkół podstawowych i szkół ponadpodstawowych o treści związane z ochroną danych osobowych i prawem do prywatności" – UODO, *Cele i Etapy Programu*, https://uodo.gov.pl/pl/21/30 (dostęp: 07.02.2021).

[450] GIODO, *Analiza opinii uczestników VII edycji Programu „Twoje dane – Twoja sprawa" na temat wieku dziecka w kwestii wyrażania przez nie zgody na przetwarzanie danych osobowych w świetle ogólnego rozporządzenia o ochronie danych*, https://archiwum.giodo.gov.pl/pl/1520281
https://archiwum.giodo.gov.pl/pl/file/12018 (dostęp: 07.02.2021), s. 1.

[451] Tamże, s. 2 i 4.

odpowiedzialności za własne wybory, lecz niezbędne jest zapewnienie dziecku odpowiedniej edukacji w zakresie jego praw i obowiązków[452].

Z projektu z dnia 16 marca 2018 r.[453], który przedłożono Radzie Ministrów, a który następnie (po drobnych autopoprawkach) został skierowany do Sejmu w dniu 11 kwietnia 2018 r.[454], usunięto przepis obniżający granicę wieku dziecka[455]. Pierwsze czytanie odbyło się w pierwszym dniu 62. posiedzenia Sejmu – 8 maja 2018 r., natomiast ustawa została uchwalona już dwa dni później[456]. Prezydent podpisał ją 22 maja 2018 r. i weszła w życie 25 maja 2018 r. Tempo prac było podyktowane datą rozpoczęcia stosowania rozporządzenia 2016/679, tj. 25 maja 2018 r., oraz harmonogramem posiedzeń Sejmu i Senatu (kolejne miało się odbyć dopiero w czerwcu 2018 r.). Podczas obrad w Senacie senator A. Pociej opowiedział się za obniżeniem granicy wieku dziecka do trzynastego roku życia – podnosząc takie same argumenty jakie podano w uzasadnieniu do pierwszej wersji projektu ustawy – i zgłosił poprawkę w tym przedmiocie[457], do której negatywnie ustosunkował się inny senator, a Minister Cyfryzacji M. Zagórski podkreślił, że kwestia wieku dziecka budziła kontrowersje przez cały czas prac nad ustawą, dodał też, że „Rzeczywiście jest tak, że jesteśmy troszeczkę pod ścianą, pod presją czasu (…)"[458]. Poprawka nie została przyjęta.

Powyższe świadczy o tym, że zarówno na etapie prac związanych z reformą ochrony danych osobowych na szczeblu unijnym – nad tekstem rozporządzenia 2016/679, jak i polskim – nad uodo z 2018 r., nie dokonano pogłębionej analizy w celu określenia odpowiedniego wieku dziecka, w szczególności zabrakło przeprowadzenia interdyscyplinarnych badań pozwalających

[452] GIODO, *Analiza opinii uczestników VII edycji Programu „Twoje dane – Twoja sprawa" na temat wieku dziecka w kwestii wyrażania przez nie zgody na przetwarzanie danych osobowych w świetle ogólnego rozporządzenia o ochronie danych*, https://archiwum.giodo.gov.pl/pl/1520281 https://archiwum.giodo.gov.pl/pl/file/12018 (dostęp: 07.02.2021), s. 5.

[453] Projekt ustawy o ochronie danych osobowych z dnia 16.03.2018, https://legislacja.rcl.gov.pl/docs//2/12302950/12457690/12457691/dokument334233.pdf (dostęp: 07.02.2021).

[454] Druk nr 2410.

[455] Rezygnacja z obniżenia granicy wieku dziecka na ostatnim pod koniec prac legislacyjnych została skrytykowana przez przedsiębiorców, którzy podnosili, że pozostawiono im zbyt mało czasu na dostosowanie się do wymogów wynikających z art. 8 rozporządzenia 2016/679 – por. S. Wikariak, *Dane dzieci pod ochroną aż do 16 lat*, „Dziennik Gazeta Prawna" 28.03.2018 r.

[456] Co spotkało się z krytyką parlamentarzystów – poseł A. Marchewka określił jako bulwersujące pozostawienie dwóch dni na uchwalenie ustawy, podczas gdy były dwa lata na dostosowanie przepisów: „Przez 2 lata coś się działo, ale na 2 dni przychodzi projekt do Sejmu (Dzwonek) i ekspresowo jest załatwiany. Tak być nie powinno. (Oklaski)" – Sprawozdanie Stenograficzne z 62. posiedzenia Sejmu Rzeczypospolitej Polskiej w dniu 10 maja 2018 r., https://orka2.sejm.gov.pl/StenoInter8.nsf/0/BD235D3C458A4419C1258289007B9B37/%24File/62_c_ksiazka_bis.pdf (dostęp: 07.02.2021), s. 374.

[457] Sprawozdanie Stenograficzne z 60. posiedzenia Senatu Rzeczypospolitej Polskiej w dniach 9, 10, 11, 15 i 16 maja 2018 r., https://www.senat.gov.pl/download/gfx/senat/pl/senat_przebieg_stenogramy_pdf/312/spr_60.pdf (dostęp: 07.02.2021), s. 255.

[458] Sprawozdanie Stenograficzne z 60. posiedzenia Senatu Rzeczypospolitej Polskiej w dniach 9, 10, 11, 15 i 16 maja 2018 r., https://www.senat.gov.pl/download/gfx/senat/pl/senat_przebieg_stenogramy_pdf/312/spr_60.pdf (dostęp: 07.02.2021), s. 256.

na podjęcie decyzji w tym przedmiocie w oparciu o obiektywne przesłanki. Dyskusja w polskim parlamencie również była ograniczona.

Zawarcie w art. 8 ust. 1 rozporządzenia 2016/679 klauzuli kompetencyjnej pozwalającej na obniżenie granicy wieku dziecka doprowadziło do powstania istotnych różnic w prawie poszczególnych państw członkowskich. Oprócz Polski, osiem państw członkowskich nie skorzystało z możliwości obniżenia granicy wieku dziecka (Niemcy, Chorwacja, Węgry, Irlandia, Luksemburg, Niderlandy, Rumunia, Słowacja); trzy państwa obniżyły ją do 15. roku życia (Czechy, Grecja, Francja); sześć państw – do 14. roku życia (Austria, Bułgaria, Cypr, Hiszpania, Włochy, Litwa); osiem państw – do 13. roku życia (Belgia, Dania, Estonia, Finlandia, Łotwa, Malta, Portugalia, Szwecja)[459]. W UE funkcjonują zatem aż cztery różne granice wieku dziecka, po ukończeniu którego może ono samodzielnie i skutecznie wyrazić zgodę na przetwarzanie danych osobowych w związku z oferowanymi mu bezpośrednio usługami społeczeństwa informacyjnego. Bez wątpienia oznacza to, że na tej płaszczyźnie nie udało się osiągnąć podstawowego celu reformy ochrony danych osobowych – zniwelowania różnic w poziomie ochrony w poszczególnych państwach członkowskich. W motywie 9 preambuły rozporządzenia 2016/679 wskazano, że „Różnice w stopniu ochrony praw i wolności osób fizycznych w państwach członkowskich - w szczególności prawa do ochrony danych osobowych - w związku z przetwarzaniem danych osobowych mogą utrudniać swobodny przepływ danych osobowych w Unii. Mogą zatem stanowić przeszkodę w prowadzeniu działalności gospodarczej na szczeblu Unii, zakłócać konkurencję oraz utrudniać organom wykonywanie obowiązków nałożonych na nie prawem Unii". Ustanowienie różnych granic wieku dziecka jest krytykowane nie tylko ze względu na brak spójnego podejścia do jego ochrony, ale także ze względu na sytuację, w jakiej znaleźli się administratorzy. Wątpliwości budzi to, prawo którego państwa powinni zastosować, chcąc świadczyć usługi, z których korzystać mogą obywatele kilku (lub wszystkich) państw członkowskich UE. Zdaniem EROD, „Administrator musi być świadomy różnic w przepisach krajowych, uwzględniając docelową grupę odbiorców jego usług" i „może być zobowiązany do przestrzegania odpowiednich przepisów krajowych każdego państwa członkowskiego, w którym oferuje usługę lub usługi społeczeństwa informacyjnego. Zależy to od tego, czy państwo członkowskie wybierze – jako punkt odniesienia w prawie krajowym – miejsce głównej jednostki organizacyjnej administratora czy też miejsce zamieszkania osoby, której dane dotyczą"[460]. Niestety, te informacje nie przyczyniają się do rozwiązania problemu. Jednoczesne przestrzeganie różnych przepisów wymagałoby dostosowania do nich sposobu świadczenia tej samej usługi – w

[459] KE, *Report on the implementation of specific provisions of Regulation (EU) 2016/679. Final report (Authors: TIPIK Legal)*, https://ec.europa.eu/info/sites/info/files/study_implementation_gdpr.pdf (dostęp: 07.02.2021), s. 5.
[460] EROD, *Wytyczne 05/2020…*, s. 30.

tym weryfikowanie, oprócz wieku dziecka, także miejsca jego zamieszkania. W skrajnym przypadku administrator, z którego usług może potencjalnie korzystać każde dziecko w UE, musiałby wdrożyć cztery różne procedury pozyskiwania zgody dziecka. Gdyby z kolei przyjął jedną, załóżmy najwyższą granicę wieku, wówczas naraziłby się na zarzut niezgodności z prawem państw, w którym jest ona niższa. Jednak jeszcze większe komplikacje powoduje to, że prawo państw członkowskich może wcale nie określać, czy punktem odniesienia jest miejsce głównej jednostki organizacyjnej administratora czy też miejsce zamieszkania osoby, której dane dotyczą – w Polsce nie wprowadzono takiego przepisu. W literaturze słusznie krytykuje się ten stan rzeczy, ponieważ wywołuje on stan niepewności prawnej[461], której negatywne skutki będą oddziaływać zarówno na dzieci jako osoby, których dane dotyczą, jak i administratorów.

3.1.5 Pozyskanie zgody lub aprobaty przedstawiciela ustawowego

Gdy w wyniku przeprowadzonej przez administratora weryfikacji okaże się, że z dostarczanej przez niego usługi społeczeństwa informacyjnego oferowanej bezpośrednio dziecku chce skorzystać dziecko, które zgodnie z art. 8 ust. 1 rozporządzenia 2016/679 nie ukończyło wieku pozwalającego mu na samodzielne wyrażenie zgody na przetwarzanie danych osobowych, stosownie do ust. 2 tego przepisu niezbędne jest podjęcie przez niego rozsądnych starań, by zweryfikować, czy przedstawiciel ustawowy wyraził zgodę lub ją zaaprobował. Administrator powinien przy tym uwzględnić dostępną technologię. Przepis wywołuje wątpliwości związane z tym, jakie działania powinien podjąć administrator w celu sprawdzenia, czy przedstawiciel ustawowy wyraził zgodę lub zaaprobował zgodę wyrażoną przez dziecko, jaki jest charakter „aprobaty" zgody i jaką powinna mieć formę, jak ustalić, że osoba, która wyraża lub aprobuje zgodę jest przedstawicielem ustawowym dziecka i wreszcie w jakim zakresie administrator może przetwarzać dane osobowe w celu przeprowadzenia weryfikacji.

Podobnie jak w przypadku weryfikacji wieku dziecka, rozporządzenie 2016/679 nie określa sposobu spełnienia powyższych obowiązków. EROD rekomenduje przyjęcie proporcjonalnego podejścia, które polega na dążeniu do pozyskania ograniczonej ilości danych osobowych przedstawiciela ustawowego, takich jak dane kontaktowe, a także zachowanie racjonalności, co oznacza, że dobór metod weryfikacji powinien być uzależniony od poziomu ryzyka związanego z przetwarzaniem danych osobowych[462]. W przypadku przetwarzania

[461] I. Milkaite, E. Lievens, *Children's Rights to Privacy and Data Protecton Around the World: Challenges in the Digital Realm*, „European Journal of Law and Technology" 2019, Vol 10, Issue 1, https://biblio.ugent.be/publication/8618586/file/8618590.pdf (dostęp: 07.02.2021).
[462] Choć EROD tego nie precyzuje, można jednak założyć – w świetle art. 32 i 35 rozporządzenia 2016/679 – że chodzi o ryzyko naruszenia praw lub wolności osób, których dane dotyczą.

powodującego niskie ryzyko, EROD wskazuje, że wystarczająca jest weryfikacja za pośrednictwem poczty elektronicznej, która może przebiegać następująco: 1) internetowa platforma gier pyta użytkownika, czy ukończył 16 rok życia – a użytkownik udziela negatywnej odpowiedzi; 2) platforma informuje dziecko, że rodzic lub opiekun musi wyrazić zgodę zanim nastąpi świadczenie usługi i prosi o podanie adresu e-mail tej osoby; 3) platforma nawiązuje kontakt za pośrednictwem uzyskanego adresu e-mail i pyta o zgodę na przetwarzanie danych osobowych dziecka oraz „podejmuje rozsądne kroki w celu upewnienia się, że dana osoba dorosła sprawuje władzę rodzicielską”[463]. Niestety, EROD nie podaje przykładów, jakie są rekomendowane sposoby pozwalające na sprawdzenie, czy osoba wyrażająca (aprobująca) zgodę jest przedstawicielem ustawowym. Wydaje się, że przy przetwarzaniu danych osobowych, z którym wiąże się niskie ryzyko, za wystarczające należy uznać odebranie oświadczenia o byciu przedstawicielem ustawowym dziecka – podobnie jak na wcześniejszym etapie uważa się za wystarczające oświadczenie samego użytkownika, że ukończył określony wiek. Gdy z przetwarzaniem danych osobowych wiąże się wysokie ryzyko, EROD sygnalizuje, że zasadne może być pozyskanie dodatkowych „dowodów” i podaje przykład poproszenia przez administratora o wpłatę na swoje konto symbolicznej kwoty za pomocą przelewu bankowego, w którego tytule zawarte będzie oświadczenie, że posiadacz rachunku sprawuje władzę rodzicielską lub opiekę nad użytkownikiem lub skorzystanie z usług weryfikacji, dostarczanych przez podmiot trzeci[464]. Wykorzystanie przelewu bankowego jest o tyle skuteczne, że – w przeciwieństwie do korespondencji elektronicznej – pozwala na poznanie tożsamości posiadacza rachunku nie tylko dzięki jego oświadczeniu, ale opierając się na wcześniejszej weryfikacji przez bank dokonanej na etapie zawierania umowy o prowadzenie rachunku bankowego. Wątpliwości natomiast może budzić to, w jakim zakresie można uznać, że została sprawdzona okoliczność istnienia przedstawicielstwa ustawowego lub chociażby, że posiadacz rachunku jest osobą pełnoletnią – mając na uwadze, że może nim być małoletni[465]. Innym problemem, który jak się wydaje może pojawiać się przy niemal każdej metodzie weryfikacji, jest to, w jaki sposób administrator może zweryfikować czy osoba podająca się za przedstawiciela ustawowego jest nim w rzeczywistości. Porównanie nazwisk czy adresów zamieszkania wydaje się niewłaściwym rozwiązaniem, gdyż nierzadko mogą się one różnić, co nie świadczy o braku uprawnień do reprezentacji dziecka. Natomiast żądanie przesłania skanów dokumentów zdaniem niektórych komentatorów byłoby działaniem nadmiarowym i godzącym w zasadę minimalizacji[466], a ponadto, co już wcześniej

[463] EROD, *Wytyczne 05/2020*…, s. 31.
[464] Tamże.
[465] Por. art. 58 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz.U. z 2020 r. poz. 1896 z późn zm.).
[466] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 8 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 13.

sygnalizowano, trudno uznać skan dokumentu za dowód tego, co zostało w nim urzędowo zaświadczone.

W amerykańskiej ustawie COPPA, która zawiera podobny do art. 8 ust. 2 rozporządzenia 2016/679 przepis nakładający obowiązek podjęcia rozsądnych działań w celu uzyskania zgody rodzica (przedstawiciela ustawowego) na przetwarzanie danych osobowych dziecka[467], jako przykładowe sposoby weryfikacji wskazano: 1) podpisanie przez rodzica oświadczenia i przesłanie go za pośrednictwem poczty, faksu, lub elektronicznie w formie skanu; 2) wymaganie od rodzica, w przypadku transakcji pieniężnej, by posłużył się kartą kredytową, kartą debetową lub inną metodą płatności *online*, która posiada funkcję informowania głównego posiadacza o każdej transakcji; 3) wymaganie, by rodzic zadzwonił pod bezpłatny numer telefonu i odbył rozmowę z przeszkolonym personelem; 4) połączenie rodzica z przeszkolonym personelem za pośrednictwem wideokonferencji; 5) weryfikację tożsamości rodzica poprzez sprawdzenie formularza tożsamości wydanego przez rząd w bazach danych zawierających takie informacje[468].

Przepisy COPPA przewidują także wyjątki, w którym uzyskanie zgody rodzica nie jest konieczne – zaliczono do nich m.in.: 1) zbieranie danych osobowych wyłącznie w celu uzyskania zgody rodzica – w przypadku jej braku, istnieje obowiązek ich usunięcia w rozsądnym czasie; 2) udzielenie bezpośredniej, jednorazowej odpowiedzi na konkretną prośbę dziecka, jeśli informacje nie są wykorzystywane do ponownego skontaktowania się z dzieckiem lub w jakimkolwiek innym celu, ani nie są one ujawniane, a po udzieleniu odpowiedzi są niezwłocznie usuwane; 3) gdy celem gromadzenia imienia i nazwiska oraz danych kontaktowych jest ochrona bezpieczeństwa dziecka i gdy takie informacje nie są wykorzystywane ani ujawniane w jakimkolwiek celu niezwiązanym z bezpieczeństwem dziecka; 4) gdy celem gromadzenia imienia i nazwiska oraz danych kontaktowych jest zapewnienie bezpieczeństwa witryny internetowej lub usługi *online*, podjęcie działań w celu dochodzenia lub obrony przed roszczeniami, udzielania informacji organom ścigania w sprawie związanej z bezpieczeństwem publicznym[469].

Porównanie regulacji zawartych w rozporządzenie 2016/679 i COPPA w zakresie uzyskania zgody przedstawiciela ustawowego na przetwarzanie danych osobowych dziecka pozwala na wyciągnięcie wniosku, że przepisy COPPA – mimo, że nie zdecydowano się w nich na taksatywne wskazanie możliwych sposobów uzyskania zgody rodzica (przedstawiciela

[467] Przepis § 312.5 b (1) COPPA stanowi, że *An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.* Analogiczne zasady wprowadzono w kalifornijskiej ustawie w dziedzinie ochrony praw konsumenta – por. D. Kuźnicka-Błaszkowska, *Protecting Children's Personal Data under General Data Protection Regulation and California Consumer Privacy Act in Relation to Information Society Services – European Perspective*, „Przegląd Prawa Konstytucyjnego" 2022, nr 2, s. 495.
[468] Por. § 312.5 b (2) i-v COPPA.
[469] Por. § 312.5 b (5) i (6) COPPA.

ustawowego) – określają przykładowe, najbardziej typowe sposoby, podczas gdy rozporządzenie 2016/679 ogranicza się jedynie do nałożenia na administratora takiego obowiązku, pozostawiając go nawet bez jakichkolwiek wskazówek interpretacyjnych w motywach preambuły. Na praktykę stosowania rozporządzenia 2016/679 mają wpływ wytyczne EROD, w których jednak w bardzo lakoniczny sposób odniesiono się do tego problemu – poprzez zasugerowanie dwóch sposobów, z których jeden – weryfikacja z wykorzystaniem usług podmiotu trzeciego – jest obecnie trudny do zastosowania w praktyce, gdyż tego rodzaju usługi są w fazie rozwoju. Brytyjski organ nadzorczy wydał wprawdzie dość szczegółowe wytyczne, są one jednak wiążące tylko dla podmiotów działających w Wielkiej Brytanii[470], która ponadto nie jest już członkiem UE – mogą więc być brane pod uwagę wyłącznie pomocniczo. Ten stan niepewności prawnej należy ocenić negatywnie, ponieważ naruszenie art. 8 rozporządzenia 2016/679 jest zagrożone odpowiedzialnością administracyjną, cywilną i karną, a ciężar oceny, jakie działania się odpowiednie, spoczywa na administratorze. Dokonanie tej oceny może rodzić trudności w obliczu braku orzecznictwa oraz rozstrzygnięć Prezesa UODO w tej materii. Zastosowanie niewłaściwych środków nie tylko powoduje ryzyko dla administratora, ale przede wszystkim może ujemnie wpływać na poziom ochrony danych osobowych dzieci. Przepis art. 8 rozporządzenia 2016/679 w sposób niedostateczny reguluje kwestię sposobów uzyskania zgody przedstawiciela ustawowego lub jego aprobaty dla zgody udzielonej przez dziecko. Wydaje się, że przepisy COPPA mogą stanowić źródło inspiracji dla organów nadzorczych ds. ochrony danych osobowych, które byłoby pomocne w wydawaniu przez nie zaleceń, opinii, materiałów informacyjnych itp.

W rozważaniach na temat sposobu uzyskiwania zgody lub aprobaty przedstawiciela ustawowego należy zwrócić uwagę na to, że unijny prawodawca nie nakłada jednak na administratorów wymogu niezaprzeczalnej weryfikacji, lecz obowiązek podjęcia rozsądnych starań w tym celu (*reasonable efforts*). Okoliczność wyrażenia lub zaaprobowania zgody przez przedstawiciela ustawowego powinna być więc uprawdopodobniona, a nie udowodniona[471]. Podobne stanowisko prezentują m.in. P. Litwiński, P. Barta i M. Kawecki, którzy uważają, że pojęcie „rozsądne starania" należy rozumieć porównywalnie jak pojęcie „należyta staranność" – czyli staranność ogólnie wymagana w stosunkach danego rodzaju[472]. Administratorzy nie mają więc obowiązku weryfikacji, jednak powinni dążyć do przyjęcia możliwie jak najbardziej

[470] Strona internetowa rządu Wielkiej Brytanii, *Explanatory memorandum to the Age Appropriate Design Code 2020*, https://www.gov.uk/government/publications/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020#extent-and-territorial-application (dostęp: 07.02.2021).
[471] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie…*, Legalis, *Komentarz do art. 8 rozporządzenia 2016/679,* teza 16.
[472] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 8 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 12.

efektywnych rozwiązań[473]. Pożądane jest wypracowanie standardów w tym zakresie zgodnych z aktualnym stanem wiedzy technicznej.

Jak zasygnalizowano, przepis art. 8 ust. 1 i ust. 2 rozporządzenia 2016/679 dotyczy dwóch sytuacji: wyrażenia przez przedstawiciela ustawowego zgody na przetwarzanie danych osobowych dziecka zamiast niego oraz potwierdzenia przez przedstawiciela ustawowego zgody wyrażonej przez dziecko[474]. Prawodawca nie przewidział jednak żadnych szczególnych zasad pozyskania aprobaty (potwierdzenia) przez przedstawiciela ustawowego zgody wcześniej wyrażonej przez dziecko. Wydaje się, że należy ją traktować tak jak zgodę na przetwarzanie danych osobowych w rozumieniu art. 4 pkt 11 rozporządzenia 2016/679 i przy jej pozyskaniu zasadne jest analogiczne stosowanie warunków określonych w art. 7 rozporządzenia 2016/679. Wydaje się, że przedstawiciel ustawowy, który aprobuje zgodę wyrażoną wcześniej przez dziecko, nie powinien co do zasady modyfikować jej zakresu w sposób rozszerzający, tj. przykładowo zgodzić się na przetwarzanie szerszego zakresu danych osobowych lub wykonywanie dodatkowych operacji przetwarzania niż te, na które zgodziło się dziecko – chyba, że biorąc pod uwagę okoliczności, przedstawiciel ustawowy uzna, że leży to w interesie dziecka.

Przedstawiciel ustawowy przed podjęciem decyzji powinien skrupulatnie zapoznać się z informacjami o przetwarzaniu danych osobowych podawanymi przez administratora. W literaturze zwraca się uwagę na problem nieznajomości warunków korzystania z platform internetowych. Badania pokazują, że aż 56% dorosłych użytkowników ich nie czyta, a 18% czyta, ale nie bierze ich pod uwagę – przez co poddawana jest w wątpliwość zdolność takich osób do wyjaśnienia swoim dzieciom, jak działają takie platformy – choć za główną przyczynę tego zjawiska uważa się nieprzystępność tych informacji[475]. Wydaje się, że nieznajomość zasad działania usług społeczeństwa informacyjnego może prowadzić do zbyt pochopnego aprobowania korzystania z nich. Nierzadko zdarza się, że dzieci sprawniej poruszają się w internecie i przez to lepiej rozumieją specyfikę świadczonych za jego pośrednictwem usług niż osoby dorosłe[476]. Ponadto dzieci niechętnie informują dorosłych o swoich aktywnościach podejmowanych w środowisku *online* i jak zauważa A. Blecher-Prigat, nadzorowanie ich zachowań może mieć negatywny wpływ na ich rozwój oraz relacje z rodzicami. Z tych względów autorka ta wypowiada się krytyczne na temat rozwiązania przyjętego w art. 8 rozporządzenia 2016/679, tj. pozostawienia decyzji co do aprobaty zgody wyrażonej przez dziecko przedstawicielom ustawowym, najczęściej rodzicom[477]. Pomocne w rozwiązaniu tego problemu byłyby kampanie edukacyjno-informacyjne

[473] P. Fajgielski, *Ogólne rozporządzenie…*, s. 192-193.
[474] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 8 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 9.
[475] K. Mc Cullagh, *The general…*, s.115-116 i tam powołane wyniki badań przeprowadzonych przez KE w 2016 r.
[476] D. Tapscott, *Gospodarka cyfrowa…*, s. 7.
[477] A. Blecher-Prigat, *Children's Right to Privacy*…, s. 379.

skierowane do przedstawicieli ustawowych, uławiające im zrozumienie znaczenia art. 8 rozporządzenia 2016/679.

3.1.6 Wyrażenie zgody na przetwarzanie danych osobowych w przypadku dziecka w wieku 16-18 lat

O ile w przypadku dzieci, które nie ukończyły szesnastego roku życia[478] oczywiste jest, że zgodę może wyrazić lub potwierdzić przedstawiciel ustawowy, o tyle nie jest jasne, czy może ją wyrazić również w odniesieniu do danych osobowych dziecka między szesnastym a osiemnastym rokiem życia, które jest już prawnie zdolne do samodzielnego i skutecznego jej udzielenia. Wydaje się, że należy rozważyć trzy możliwe podejścia: 1) zgodę może wyrazić przedstawiciel ustawowy oraz dziecko; 2) zgodę może wyrazić dziecko lub jego przedstawiciel ustawowy; 3) zgodę może wyrazić wyłącznie dziecko.

Warto jednocześnie zasygnalizować, że w opinii Grupy Roboczej Art. 29 dziecku w każdym wieku powinno przysługiwać tzw. prawo do uczestnictwa – którego zakres powinien być dostosowany do jego dojrzałości, ponieważ „Dzieci stopniowo pozyskują coraz większe możliwości udziału w podejmowaniu decyzji, które ich dotyczą. W miarę jak rosną, powinny coraz bardziej regularnie uczestniczyć w wykonywaniu swoich praw, w tym również praw związanych z ochroną osobowych”[479]. Jak wyjaśnia Grupa Robocza Art. 29, podstawowym poziomem tego prawa jest prawo dziecka do wyrażenia opinii, „Kiedy jednak dzieci osiągną zdolność do odpowiednich czynności, ich uczestnictwo można zwiększyć nawet do podejmowania wspólnej lub autonomicznej decyzji”[480].

Jeśli chodzi o podejście pierwsze, to wymaganie zarówno zgody przedstawiciela ustawowego, jak i dziecka, które ukończyło szesnasty rok życia, wydaje się nieuprawnione w świetle art. 8 ust. 1 rozporządzenia 2016/679 i mogłoby prowadzić do nieuzasadnionego utrudnienia korzystania z usług społeczeństwa informacyjnego i ich świadczenia – dlatego należy je odrzucić.

Argumentów przemawiających za drugim podejściem można poszukiwać w charakterze instytucji przedstawicielstwa ustawowego, którego częścią składową jest reprezentacja dziecka, pozwalająca m.in. na dokonywaniu w imieniu dziecka czynności prawnych. Przedstawicielstwo ustawowe trwa do momentu osiągnięcia pełnej zdolności do czynności prawnych. Co do zasady, uzyskanie przez dziecko ograniczonej zdolności do czynności prawnych nie wyklucza możliwości

[478] Lub w przypadku państw, które zdecydowały się na obniżenie tej granicy – wieku określonego w ich prawie. Ze względu na to, że w Polsce obowiązuje granica ukończenia 16. roku życia, w dalszej części rozprawy będę operować tą wartością.
[479] Grupa Robocza Art. 29, *Opinia w sprawie ochrony danych osobowych dzieci…*, s. 6.
[480] Tamże, s. 7.

zastępowania go przez przedstawiciela ustawowego, nawet w odniesieniu do czynności, których może dokonywać samodzielnie – jednak zdaniem J. Strzebinczyka w przypadku tego rodzaju czynności taki generalny wniosek budzi wątpliwości, nawet gdy przepisy nie wyłączają *expressis verbis* reprezentowania dziecka przez przedstawiciela ustawowego[481]. Zgodnie z art. 95 §1 kc, czynności prawnej można dokonać przez przedstawiciela z zastrzeżeniem wyjątków przewidzianych w ustawie[482] albo wynikających z właściwości czynności prawnej – do tej grupy zalicza się „przejawy woli bądź przejawy uczuć, których właściwość wyklucza możliwość ich dokonania przez przedstawiciela"[483] – a zatem czynności o charakterze czynności osobistej[484], za którą nie można uznać wyrażenia zgody na przetwarzanie danych osobowych dziecka. Powstaje więc wątpliwość czy przepis art. 8 ust. 1 rozporządzenia 2016/679 – w zakresie, w jakim stanowi, że przetwarzanie danych osobowych dziecka, które ukończyło 16 lat, na podstawie samodzielnie wyrażonej przez niego zgody – należy traktować jako wyjątek od ogólnej zasady, że czynności tej można dokonać przez przedstawiciela ustawowego. Nie zostało to rozstrzygnięte przez unijnego prawodawcę i może być dyskusyjne. Biorąc pod uwagę kontekst przetwarzania danych osobowych, w jakim ma zastosowanie art. 8 rozporządzenia 2016/679 – czyli wyłącznie świadczenie usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, a także wiek dziecka (16-18 lat), będącego właściwie u progu dorosłości – najwłaściwsze wydaje się skłonienie się ku uznaniu, że w takiej sytuacji wyrażenie zgody powinno należeć wyłącznie do dziecka – a zatem opowiedzenie się za trzecim podejściem. Korzystanie z usług społeczeństwa informacyjnego jest dobrowolne – nie jest powiązane z aktywnościami, w których dziecko musi lub powinno uczestniczyć. Wobec tego brak zgody dziecka na przetwarzanie jego danych osobowych nie będzie niósł żadnych poważnych i negatywnych konsekwencji – trudno za takie byłoby uznać np. nieotrzymywanie biuletynu informacyjnego od księgarni internetowej lub nieopublikowanie zdjęcia na portalu społecznościowym. Natomiast możliwość wyrażenia zgody na przetwarzanie danych osobowych dziecka przez przedstawiciela ustawowego w sytuacji, gdy zgodnie z prawem może ono już samodzielnie dokonać tej czynności, rodzi ryzyko, że jego postępowanie nie będzie w pełni pokrywało się z wolą dziecka, co potencjalnie może powodować konflikty, na tyle poważne, by musiał rozstrzygać je sąd. Przykładowo, sąd we Włoszech nakazał

[481] J. Strzebinczyk, [w:] T. Smyczyński (red.), *Prawo rodzinne i opiekuńcze. System Prawa Prywatnego. Tom 12*, wyd. II, Warszawa 2011, s. 290.
[482] Jako wyjątek przewidziany w ustawie wskazać można tytułem przykładu art. 98 §2 krio, zgodnie z którym „żadne z rodziców nie może reprezentować dziecka: 1) przy czynnościach prawnych między dziećmi pozostającymi pod ich władzą rodzicielską; 2) przy czynnościach prawnych między dzieckiem a jednym z rodziców lub jego małżonkiem, chyba że czynność prawna polega na bezpłatnym przysporzeniu na rzecz dziecka albo że dotyczy należnych dziecku od drugiego z rodziców środków utrzymania i wychowania".
[483] K. Kopaczyńska-Pieczniak, *Komentarz do art. 95 kc*, [w:] A. Kidyba (red.), *Kodeks cywilny…*, s. 599.
[484] P. Sobolewski, *Komentarz do art. 95 kc*, [w:] K. Osajda (red.), *Kodeks cywilny. Komentarz*, Warszawa 2020, Legalis, teza 5.

matce usunięcie z portalu Facebook zdjęć jej szesnastoletniego syna, opublikowanych przez nią bez jego zgody[485]. Ponadto na aprobatę zasługuje przytoczone wcześniej stanowisko Grupy Roboczej Art. 29 mówiące o tym, że dziecko powinno uczestniczyć w wykonywaniu swoich praw związanych z ochroną osobowych. Skoro prawodawca unijny przewidział jego zdolność do samodzielnego wyrażenia zgody, zdaje się to wykluczać jednoczesne zastępowanie go w tym zakresie przez przedstawiciela ustawowego. Na poparcie tej tezy można dodatkowo przytoczyć stanowisko EROD, zgodnie z którym dziecko po osiągnięciu wieku pozwalającego na samodzielne wyrażenie zgody na przetwarzanie danych osobowych, może zgodę wcześniej wyrażoną (lub zaaprobowaną) przez swojego przedstawiciela ustawowego potwierdzić, zmienić lub wycofać – dlatego administrator powinien je o tym poinformować[486].

3.1.7 Wycofanie zgody

Przepis art. 7 ust. 3 rozporządzenia 2016/679 traktuje o istotnym uprawnieniu związanym ze zgodą na przetwarzanie danych osobowych – o możliwości jej wycofania, co jest przejawem koncepcji autonomii informacyjnej. Zgodnie z tym przepisem osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę, co nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Co ważne, osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Ponadto wycofanie zgody musi być równie łatwe jak jej wyrażenie – wszelkie zbyt skomplikowane procedury mogą być odczytane jako utrudnianie wykonania tego uprawnienia. Choć EROD podkreśla, że przepisy rozporządzenia 2016/679 nie precyzują, że wyrażenie zgody i jej wycofanie musi odbywać się w identyczny sposób, w przypadku wyrażenia zgody w środowisku *online*, poprzez przeznaczony do tego interfejs, rekomenduje zapewnienie użytkownikowi możliwości jej odwołania w ten sam sposób[487]. Wycofanie zgody nie musi być w żaden sposób umotywowane – osoba, której dane dotyczą, nie jest zobligowana do wyjaśnienia przyczyn zmiany swojej decyzji. Wymaganie przez administratora ich podania jako warunku skutecznego cofnięcia zgody stanowi w ocenie Prezesa UODO naruszenie art. 7 ust. 3 rozporządzenia 2016/679[488]. W rezultacie wycofania zgody, który wywołuje skutek *ex nunc*, konieczne jest zaprzestanie przetwarzania danych osobowych[489], o ile

[485] L. Smith, *Woman faces £9,000 fine if she posts pictures of her son on Facebook*, „Independent" 12.01.2018, https://www.independent.co.uk/news/world/europe/facebook-fines-woman-son-photos-post-social-media-court-italy-rome-a8155361.html (dostęp: 07.02.2021). Mimo, że orzeczenie nie zapadło na gruncie przepisów o ochronie danych osobowych, lecz prawa autorskiego, ilustruje problem.
[486] EROD, *Wytyczne 05/2020*…, s. 32.
[487] EROD, *Wytyczne 05/2020*…, s. 25-26.
[488] Decyzja Prezesa UODO z dnia 16 października 2019 r., ZSPR.421.7.2019, https://uodo.gov.pl/decyzje/ZSPR.421.7.2019 (dostęp: 07.02.2021).
[489] A. Nerka, M. Sakowska-Baryła, *Komentarz do art. 7 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie*…, Legalis.

nie istnieje inna podstawa prawna. Brak faktycznej możliwości wycofania zgody bez negatywnych konsekwencji podważałoby jedną z cech, jaką powinna się charakteryzować – mianowicie dobrowolność[490].

Wskazanie w art. 7 ust. 3 rozporządzenia 2016/679 *expressis verbis* istnienia uprawnienia do wycofania zgody na przetwarzanie danych osobowych oraz nałożenie na administratora obowiązku informowania o nim należy ocenić pozytywnie. Przed wprowadzeniem w 2010 r. do art. 7 pkt 5 uodo z 1997 r. frazy „zgoda może być odwołana w każdym czasie" kwestia ta przez kilkanaście lat budziła wątpliwości[491]. Dlatego słusznie postąpił prawodawca unijny wyraźnie akcentując tak ważne uprawnienie osoby, której dane dotyczą, jednocześnie zmniejszając poczucie niepewności administratorów i podnosząc ich świadomość w tym zakresie, a dzięki wprowadzeniu obowiązku informowania o tym uprawnieniu – także świadomość osób, których dane dotyczą.

Odwołanie zgody na przetwarzanie danych osobowych dziecka w związku ze świadczeniem usług społeczeństwa informacyjnego jest więc możliwe w każdym momencie, powinno być równie łatwe jak jej udzielenie i nie powinno nieść dla niego żadnych negatywnych konsekwencji. Należy rozważyć, czy i kiedy dziecko może samodzielnie wycofać zgodę, a w jakich okolicznościach niezbędne jest działanie jego przedstawiciela ustawowego. Za punkt wyjścia należy przyjąć założenie, że charakter prawny wycofania zgody na przetwarzanie danych osobowych jest analogiczny jak jej wyrażenia[492]. Wzięcie pod uwagę dwóch czynników – wieku dziecka oraz okoliczności, w jakich przetwarzane są jego dane osobowe – w świetle wcześniejszych rozważań na tle przepisów kc i rozporządzenia 2016/679 prowadzi do wniosku, że możliwych jest pięć sytuacji: 1) zgodę może odwołać wyłącznie przedstawiciel ustawowy – gdy chodzi o dziecko, które nie ukończyło trzynastego roku życia – dotyczy wszystkich okoliczności przetwarzania za wyjątkiem usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku (patrz pkt 5); 2) zgodę może odwołać przedstawiciel ustawowy lub dziecko – gdy chodzi o dziecko, które nie ukończyło szesnastego roku życia i gdy dane osobowe są przetwarzane w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku; 3) zgodę może odwołać przedstawiciel ustawowy lub dziecko – gdy chodzi o dziecko w wieku między trzynastym a osiemnastym rokiem życia – gdy chodzi o inne okoliczności przetwarzania niż świadczenie usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (a zatem także pozostałe usługi społeczeństwa informacyjnego); 4) zgodę

[490] Por. motyw 42 preambuły rozporządzenia 2016/679.
[491] P. Fajgielski, *Odwoływalność zgody na przetwarzanie danych osobowych – znaczenie dla praktyki gospodarczej*, [w:] A. Mednis (red.), *Prywatność a ekonomia…,* s. 65.
[492] J. Byrski, *Odwołanie zgody na przetwarzanie danych osobowych. Wybrane zagadnienia*, „Monitor Prawniczy" dodatek: *Nowelizacja ustawy o ochronie danych osobowych 2010*, G. Sibiga (red.), 2011, nr 3, s. 1014-1015.

może odwołać wyłącznie dziecko – gdy chodzi o dziecko, które ukończyło szesnasty rok życia i gdy dane osobowe są przetwarzane w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku. W przypadku dziecka, które ukończyło szesnasty rok życia, a zatem może samodzielnie wyrazić zgodę na przetwarzanie danych osobowych w sytuacji określonej w art. 8 rozporządzenia 2016/679, nie ulega wątpliwości, że powinno mieć ono również możliwość skutecznego jej wycofania; 5) zgodę może odwołać wyłącznie dziecko – bez względu na wiek dziecka, gdy dane osobowe są przetwarzane w związku ze świadczeniem usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku. Mając na względzie, że korzystanie z nich może niekiedy odbywać się bez wiedzy przedstawiciela ustawowego, a w świetle motywu 38 preambuły rozporządzenia 2016/679 bez jego zgody, dziecko powinno mieć możliwość wycofania zgody, którą wcześniej wyraziło. Ingerencja przedstawiciela ustawowego polegająca na wycofaniu zgody nie powinna być dopuszczalna. Jeśli dziecko poszukuje pomocy, wycofanie przez jego przedstawiciela ustawowego zgody na przetwarzanie danych osobowych mogłoby zniweczyć możliwość jej otrzymania, jeśli nie kieruje nim troska o dobro dziecka.

3.1.8 Ważność oświadczeń o wyrażeniu zgody złożonych przez rozpoczęciem stosowania rozporządzenia 2016/679

Rozporządzenie 2016/679 nie zawiera przepisów przejściowych, które odnosiłyby się do oceny ważności zgody, która została wyrażona pod rządami wcześniej obowiązujących przepisów o ochronie danych osobowych, co może wywoływać stan niepewności prawnej[493]. Motyw 171 preambuły rozporządzenia 2016/679 dostarcza pewnych wskazówek interpretacyjnych – stanowi, że jeśli przetwarzanie danych osobowych opiera się na zgodzie osoby, której dane dotyczą, wyrażonej na podstawie dyrektywy 95/46, nie musi ona ponownie wyrażać zgody, jeżeli pierwotny sposób jej wyrażenia odpowiada warunkom przewidzianym w rozporządzeniu 2016/679 i w takim przypadku administrator może kontynuować przetwarzanie po rozpoczęciu jego stosowania[494]. Administrator powinien zatem ocenić, czy sposób pozyskania przez niego zgód przed 25 maja 2018 r. odpowiada tym warunkom. Jednak wobec braku odesłania w motywie 171 do konkretnych jednostek redakcyjnych rozporządzenia 2016/679 powstaje wątpliwość, które

[493] Por. A. Nerka, M. Sakowska-Baryła, *Komentarz do art. 6 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 9.

[494] Ponadto zgodnie z motywem 171 preambuły rozporządzenia 2016/679 „Przetwarzanie, które w dniu rozpoczęcia stosowania niniejszego rozporządzenia już się toczy, powinno w terminie dwóch lat od wejścia niniejszego rozporządzenia w życie zostać dostosowane do jego przepisów", a także „Decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia". Wydaje się, że takie postanowienia powinny znaleźć się w części normatywnej – np. w rozdziale XI. Przepisy końcowe.

warunki (wymogi) należy wziąć pod uwagę – czy wystarczające jest poprzestanie na ocenie, czy zgoda spełnia wszystkie cechy wynikające z art. 4 pkt 11 rozporządzenia 2016/679 – tzn. czy jest dobrowolnym, konkretnym, świadomym i jednoznacznym okazaniem woli w przedmiocie przyzwolenia na przetwarzanie danych osobowych – czy konieczne jest spełnienie także warunków określonych w art. 7 rozporządzenia 2016/679. Legalna definicja zgody na przetwarzanie danych osobowych nie uległa znaczącym zmianom w wyniku reformy – w obydwu stanach prawnych można wskazać na te same cechy: konkretność, świadomość, dobrowolność[495]. Jednak art. 7 rozporządzenia 2016/679 istotnie rozszerzył zakres warunków ważności zgody m.in. poprzez nałożenie na administratora obowiązku poinformowania osoby, której dane dotyczą – zanim wyrazi zgodę – o tym, że ma prawo w dowolnym momencie ją wycofać, co nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Należy podkreślić, że na gruncie dyrektywy 95/46 nie istniał analogiczny obowiązek. Wobec powyższego przyjęcie, że zgoda pozyskana przed 25 maja 2018 r. musi spełniać warunki określone zarówno w art. 4 pkt 11, jak i art. 7 rozporządzenia 2016/679 i przy założeniu, że administratorzy nie będąc do tego zobowiązani co do zasady nie informowali o możliwości wycofania zgody przed jej wyrażeniem, prowadziłoby do sytuacji, w której jedynie w nielicznych przypadkach możliwe byłoby kontynuowanie przetwarzania danych osobowych – co czyniłoby motyw 171 pozbawionym sensu[496]. Dlatego na aprobatę zasługuje pogląd, że wystarczające jest, jeśli zgoda posiada cechy, o których mowa w art. 4 pkt 11 rozporządzenia 2016/679[497]. Ponadto wypada skłonić się ku przyjęciu, że powinny zostać także spełnione warunki wskazane w art. 7 ust. 1, 2 i 4 rozporządzenia 2016/679[498]. EROD zdaje się prezentować bardziej restrykcyjne podejście[499], jednak nie można moim zdaniem przekreślać trudu i kosztów, jakie ponieśli przedsiębiorcy-administratorzy w celu pozyskania zgód na przetwarzanie danych osobowych, jeśli czynili to zgodnie z wymogami dyrektywy 95/46. Wydaje się zatem, że praktykę informowania osób, których dane były przetwarzane na podstawie zgody udzielonej przed reformą ochrony danych osobowych, m.in. o prawie do wycofania zgody – będąca swoistym uzupełnieniem wcześniej

[495] Zgodnie z art. 2 lit. h dyrektywy 95/46, zgoda „oznacza konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych".
[496] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 206. Odmiennie D. Lubasz, *Komentarz do art. 6 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 357.
[497] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 206.
[498] Przepis art. 7 rozporządzenia 2016/679 w ust. 1, 2 i 4 określa również inne warunki ważności zgody, które nie były wprawdzie wskazane w przepisach dyrektywy 95/46, jednak wynikały z orzecznictwa i doktryny powstałych na jej kanwie – nie można więc uznać, że te wymogi są nowością – por. P. Litwiński, *Nowe rozporządzenie ogólne w sprawie ochrony danych osobowych i jego wpływ na społeczeństwo informacyjne. Wybrane zagadnienia*, [w:] K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Media elektroniczne…*, s. 145 i tam powołane orzecznictwo. Z tego względu administrator powinien wziąć je pod uwagę oceniając ważność zgód pozyskanych przed 25 maja 2018 r.
[499] EROD, *Wytyczne 05/2020*…, s. 36.

spełnionego obowiązku informacyjnego – a także wprowadzenie możliwości wycofania zgody w równie łatwy sposób, jak jej wyrażenie, można uznać za prawidłową[500].

O wiele trudniejsza jest ocena ważności zgód pozyskanych pod rządami dyrektywy 95/46 w przypadku przetwarzania danych osobowych dzieci. W tym akcie prawnym brakowało szczególnych regulacji odnoszących się do pozyskiwania zgód na przetwarzanie danych osobowych dzieci. Przepis art. 8 rozporządzenia 2016/679 stanowi *novum*. Należy pamiętać, że jednym z celów reformy jest zwiększenie poziomu ochrony danych osobowych dziecka, a wszelkie działania związane z przetwarzaniem danych osobowych powinno się oceniać przez pryzmat jego dobra. Z tych wydaje się najwłaściwsze zajęcie stanowiska, że w świetle motywu 171 preambuły rozporządzenia 2016/679 administrator świadczący usługę społeczeństwa informacyjnego oferowaną bezpośrednio dziecku, jeśli przetwarza jego dane na podstawie zgody pozyskanej przed 25 maja 2018 r. i która nie spełnia warunków określonych w art. 8 rozporządzenia 2016/679, nie powinien kontynuować przetwarzania bez dostosowania go do tych wymogów, tj. winien pozyskać zgodę (lub aprobatę) przedstawiciela ustawowego, jeśli przetwarzał dane dziecka poniżej 16 roku życia na podstawie wyrażonej przez niego zgody. Administrator nie powinien też zasłaniać się niewiedzą na temat wieku użytkowników swojej usługi, ponieważ jak już wcześniej zasygnalizowano, powinien dołożyć należytej staranności w sprawdzeniu tej okoliczności. W procesie oceny ważności zgód na przetwarzanie danych osobowych przed 25 maja 2018 r. każdy administrator świadczący usługę społeczeństwa informacyjnego powinien przeprowadzić rzetelną ocenę, czy jego usługa mieści się w zakresie pojęcia usługi społeczeństwa informacyjnego oferowanej bezpośrednio dziecku i w zależności od wyniku tej analizy, podjąć działania w celu dostosowania przetwarzania do nowych wymogów związanych z ochroną danych osobowych dzieci.

3.2 Przetwarzanie w celu zawarcia i wykonania umowy

Zgodnie z art. 6 ust. 1 lit. b rozporządzenia 2016/679 jedną z przesłanek legalizujących przetwarzanie danych osobowych jest okoliczność, że jest ono niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. W przypadku usług społeczeństwa informacyjnego, umowy zawierane przez internet w większości stanowią umowy adhezyjne, które zawiera się przez przystąpienie – akceptację określonych warunków, bez możliwości ich negocjacji – co więcej, czasem nawet bez świadomości ze strony usługobiorcy, że dokonuje on czynności prawnej[501], co może być spowodowane tym, że rozpoczęcie korzystania z usługi jest szybkie i łatwe. Akceptacja

[500] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 206.
[501] J. Janowski, *Kontrakty elektroniczne w obrocie prawnym*, rozdział III pkt 1.2, Warszawa 2008, LEX.

regulaminu czy warunków korzystania z usługi często nie jest postrzegana przez użytkowników jako zawarcie umowy. Przesłanka z art. 6 ust. 1 lit. b rozporządzenia 2016/679 dotyczy wszystkich umów i ma zastosowanie w dwóch przypadkach: gdy podejmowane są działania zainicjowane przez osobę, której dane dotyczą, w celu zawarcia umowy, oraz gdy umowa została już zawarta i powinna być wykonana. Należy podkreślić, że zawarcie umowy nie musi dojść do skutku, by art. 6 ust. 1 lit. b rozporządzenia 2016/679 legitymizował przetwarzanie przed zawarciem umowy – jednak w takim przypadku administrator powinien usunąć dane osobowe, które pozyskał, zgodnie z zasadą ograniczenia celu, jeśli nie istnieje inny uzasadniony cel przechowywania i podstawa prawna uprawniająca do dalszego przetwarzania.

Powołanie się na art. 6 ust. 1 lit. b rozporządzenia 2016/679 jest więc dopuszczalne, gdy spełniony jest warunek niezbędności przetwarzania do zawarcia lub wykonania umowy. Oceniając, czy został on spełniony, należy ustalić, czy istnieje obiektywny i bezpośredni związek między przetwarzaniem danych osobowych a dążeniem do zawarcia lub wykonaniem konkretnej umowy[502]. Zakres danych osobowych jest uzależniony od przedmiotu świadczenia, niekiedy przepisów prawa regulujących dany stosunek umowny, okoliczności zawarcia i wykonania umowy[503]. Przykładowo, niezbędne do wykonania umowy jest przetwarzanie danych osobowych i innych informacji związanych z płatnością za usługę, czy pozyskanie adresu poczty elektronicznej, na który ma być wysłany produkt (np. książka w wersji elektronicznej). W pojęciu wykonania umowy mieszczą się także działania związane z wymianą, zwrotem towaru czy wysyłanie wezwań do zapłaty[504]. Niezbędność przetwarzania wpływa także na ocenę tego, jakie operacje przetwarzania są dopuszczalne w celu wykonania umowy – mogą one obejmować, w uzasadnionych przypadkach, także przekazywanie danych osobowych innemu podmiotowi[505]. Zdaniem EROD także udzielenie odpowiedzi na pytanie potencjalnego klienta o ofertę mieści się w pojęciu przetwarzania w celu podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy – natomiast nie uprawnia to administratora do przesyłania mu ofert w przyszłości, z własnej inicjatywy[506].

W kontekście świadczenia usług społeczeństwa informacyjnego szereg problemów interpretacyjnych wynika z przepisów uśude, które nie zostały dostosowane do rozporządzenia 2016/679 w sposób właściwy. W art. 18 uśude ustawodawca dokonał swoistej kategoryzacji danych, dzieląc je na trzy typy: 1) dane, które określił jako niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między usługodawcą a

[502] EROD, *Wytyczne 2/2019…,* s. 9.
[503] A. Nerka, M. Sakowska-Baryła, *Komentarz do art. 6 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.
[504] EROD, *Wytyczne 2/2019*…, s. 12.
[505] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, s. 425.
[506] EROD, *Wytyczne 2/2019*…, s. 14.

usługobiorcą, a także do realizacji umów lub dokonania innej czynności prawnej (ust. 1 i 2); 2) dane, których przetwarzanie w określonych celach może się odbywać za zgodą usługobiorcy (ust. 4 uśude); 3) dane eksploatacyjne.

Jeśli chodzi o pierwszą kategorię, ustawodawca w art. 18 ust. 1 uśude określił katalog danych osobowych niezbędnych do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego, zaliczając do nich: nazwisko i imiona usługobiorcy; numer ewidencyjny PESEL lub, gdy ten numer nie został nadany, numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość; adres zameldowania na pobyt stały; adres do korespondencji, jeżeli jest inny niż adres zameldowania na pobyt stały; dane służące do weryfikacji podpisu elektronicznego usługobiorcy; adresy elektroniczne usługobiorcy. Z kolei art.18 ust. 2 uśude stanowi, że w celu realizacji umów lub dokonania innej czynności prawnej z usługobiorcą, usługodawca może przetwarzać inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia. Już przed reformą ochrony danych osobowych podnoszono, że art. 18 ust. 1 uśude i przyjęta w nim konstrukcja – oderwana od oceny konkretnego stanu faktycznego, tj. jakie dane osobowe rzeczywiście są potrzebne do rozpoczęcia korzystania z danej usługi – rodzi wątpliwości, czy administrator ma obowiązek badania adekwatności zakresu danych osobowych do celu ich przetwarzania, czy powinien (lub może) po prostu pozyskiwać wszystkie dane wskazane w tym przepisie[507]. W świetle zasady minimalizacji danych wątpliwości budzi zwłaszcza przetwarzanie numeru PESEL lub numeru dokumentu potwierdzającego tożsamość oraz adresu zameldowania lub do korespondencji – tym bardziej, jeśli chodzi o nieodpłatną usługę i zaistnienie przesłanek do dochodzenia lub obrony przed roszczeniami, co mogłoby częściowo uzasadniać pozyskiwanie takich danych, wydaje się mało prawdopodobne. Należy zgodzić się ze stanowiskiem, że jeśli w danym przypadku przetwarzanie tych danych nie będzie niezbędne do celu dość wyraźnie określonego w art. 18 ust. 1 uśude, a zatem nie będzie zachodzić bezpośredni związek między celem przetwarzania a zakresem danych, omawiany przepis nie będzie legalizował takiego przetwarzania[508]. Zdaniem X. Konarskiego, po 25 maja 2018 r. należy stosować zasady określone w rozporządzeniu 2016/679, ponieważ art. 18 ust. 1 uśude – jako przepis niezgodny z art. 5 ust. 1 lit. c rozporządzenia 2016/679, zawężający zastosowanie przesłanek legalizujących przetwarzanie i wprowadzony przez ustawodawcę w oderwaniu od prawa unijnego – narusza zasadę pierwszeństwa prawa UE[509]. Choć X. Konarski,

[507] K. Klafkowska-Waśniowska, *Komentarz do art. 18 uśude*, [w:] D. Lubasz, M. Namysłowska (red.), *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, Warszawa 2011, LEX, i tam powołana literatura.

[508] J. Gołaczyński, *Komentarz do art. 18 uśude*, [w:] J. Gołaczyński (red.), *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Warszawa 2009, s. 146.

[509] X. Konarski, *Dostosowanie przepisów sektorowych dotyczących usług łączności elektronicznej do wymogów RODO*, [w:] G. Sibiga (red.), *Polskie przepisy o ochronie danych osobowych. Aktualne problemy prawnej ochrony danych osobowych 2019* (dodatek do „Monitora Prawniczego" 2019, nr 22), Warszawa 2019, s. 11-12.

powołując się na orzecznictwo TSUE, słusznie zauważa, że w takiej sytuacji sąd krajowy powinien odmówić zastosowania normy prawa krajowego, nawet jeśli nie została ona uchylona, wydaje się, że nie rozwiązuje to wszystkich problemów ze stosowaniem art. 18 ust. 1 uśude. Brak jego uchylenia przez ustawodawcę może powodować praktyczne problemy, zwłaszcza dla przedsiębiorców, którzy nieświadomi zawiłości stanu prawnego mogą stosować ten przepis ufając, że skoro znajduje się w obowiązującej ustawie, to działanie zgodne z nim jest uprawnione i nie wymaga dodatkowych analiz dotyczących zakresu pozyskiwanych danych osobowych usługobiorców. Przepis art. 18 ust. 1 uśude powinien być zatem niezwłocznie uchylony lub zmieniony i dostosowany do rozporządzenia 2016/679.

Dane eksploatacyjne, które zgodnie z art. 18 ust. 5 uśude może przetwarzać usługodawca, to dane charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną. Ustawodawca zaliczył do nich: oznaczenia identyfikujące usługobiorcę; oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca; informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną; informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną. Oznaczeniami identyfikującymi usługobiorcę może być przykładowo nadany mu przez usługodawcę numer klienta, zaś do informacji identyfikujących zakończenie sieci telekomunikacyjnej oraz system teleinformatyczny zaliczyć można m.in. numery telefonów oraz numery IMEI telefonów jako urządzeń, nr karty sieciowej, nr IP[510]. Natomiast informacjami o rozpoczęciu, zakończeniu i zakresie świadczonej usługi mogą być tzw. dane o ruchu w sieci, logi systemowe, informacje pozyskane poprzez pliki *cookie*[511]. Przepisy rozporządzenia 2016/679 będą miały zastosowanie do tych informacji w takim zakresie, w jakim będą stanowiły dane osobowe. Jak słusznie zauważa K. Klafkowska-Waśniowska, art. 18 ust. 5 uśude nie określa, w jakim celu mogą być wykorzystane te informacje, a zatem – jeśli stanowią dane osobowe – nie determinuje podstawy prawnej ich przetwarzania na gruncie przepisów o ochronie danych osobowych[512]. Najlepiej ilustruje to przykład plików *cookies*, które mogą służyć rozmaitym celom – począwszy od zapewnienia właściwego działania strony internetowej, przez ułatwienie korzystanie z niej (np. pliki zapamiętujące ustawienia języka), aż po śledzenie zachowań w celach marketingowych – w tym poprzez pliki dostarczane przez inne podmioty niż usługodawca[513]. Analogicznie na różne potrzeby mogą być wykorzystywane informacje o korzystaniu z usługi pozyskane w inny sposób. O ile w przypadku

[510] K. Klafkowska-Waśniowska, *Komentarz do art. 18 uśude*, [w:] D. Lubasz, M. Namysłowska (red.), *Świadczenie usług drogą elektroniczną…*, LEX.
[511] Tamże.
[512] Tamże.
[513] S. Piątek, *Prawne warunki stosowania cookies*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2015, nr 6, s. 50-53.

plików *cookies*, które są instalowane w urządzeniu[514], bez względu na zakwalifikowanie pozyskanych poprzez nie informacji jako danych osobowych, potrzebna jest na podstawie art. 173 ust. 1 lit. b upt[515] zgoda użytkownika końcowego[516] – a zatem podstawę prawną przesądził ustawodawca[517] – o tyle w pozostałych przypadkach usługodawca jako administrator zobowiązany jest do oceny charakteru innych informacji, celu, w jakich zamierza je wykorzystywać, a jeśli okaże się, że będzie przetwarzał dane osobowe, powinien oprzeć je na odpowiedniej przesłance z art. 6 ust. 1 rozporządzenia 2016/679. Prowadzi to do wniosku, że często może wystąpić sytuacja, że nawet jeśli głównym celem przetwarzania danych osobowych jest zawarcie i wykonanie umowy, realizowanym na podstawie art. 6 ust. 1 lit. b rozporządzenia 2016/679, dodatkowe cele przetwarzania będą wymagały zastosowania innej przesłanki.

Powyższy wniosek potwierdza to, że w zakres stosowania przesłanki z art. 6 ust. 1 lit. b rozporządzenia 2016/679 nie wchodzi przetwarzanie do celów marketingowych, reklamy behawioralnej i co do zasady przetwarzanie w celu personalizacji treści[518]. Takie działania najczęściej są możliwe dzięki przetwarzaniu danych osobowych, które polega na profilowaniu. Wymaga to istnienia innej niż wskazana w art. 6 ust. 1 lit. b rozporządzenia 2016/679 podstawy prawnej. Zgodnie z art. 18 ust. 4 uśude, usługodawca może przetwarzać, za zgodą usługobiorcy i dla celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę, inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną. Ustawodawca dopuszcza więc przetwarzanie danych do tych celów wyłącznie, jeśli usługobiorca wyrazi na to zgodę. Należy podkreślić, że jest to oryginalne rozwiązanie polskiego ustawodawcy, ponieważ rozporządzenie 2016/679 nie zawiera aż tak rygorystycznych wymogów i co do zasady możliwe jest przetwarzanie danych osobowych do celów marketingu

[514] S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2019, Legalis, *Komentarz do art. 172 upt*.
[515] Jego adresatami są także usługodawcy w rozumieniu uśude – M. Olszewska, *Prawne zasady dotyczące plików cookies a ochrona danych osobowych użytkowników Internetu*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2017, nr 7, s. 47.
[516] Użytkownikiem końcowym jest podmiot korzystający z publicznie dostępnej usługi telekomunikacyjnej lub żądający świadczenia takiej usługi, dla zaspokojenia własnych potrzeb (art. 2 pkt 50 upt). Przepis art. 172 upt dotyczy także abonenta, czyli podmiotu, który jest stroną umowy o świadczenie usług telekomunikacyjnych zawartej z dostawcą publicznie dostępnych usług telekomunikacyjnych (art. 2 pkt 1 upt).
[517] Ustawodawca również w tym przypadku zawęził w sposób nieuzasadniony możliwość instalowania plików *cookie* (lub innego oprogramowania) wyłącznie do sytuacji, gdy użytkownik końcowy (lub abonent) wyraził na to zgodę. Grupa Robocza Art. 29 zinterpretowała art. 5 ust. 3 dyrektywy 2002/58 w ten sposób, że w określonych w nich przypadkach, możliwe jest instalowanie plików *cookies* bez zgody. Zgodnie z tym przepisem, wymóg pozyskania zgody nie stanowi „przeszkody dla technicznego przechowywania danych lub dostępu do danych jedynie w celu wykonania lub ułatwiania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej lub gdy jest to szczególnie niezbędne w celu dostarczania usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika". Por. Grupa Robocza Art. 29, *Opinia nr 04/2012 w sprawie wyłączenia zapisywania plików cookie spod zasady pozyskiwania zgody*, przyjęta dnia 7 czerwca 2012 r., https://archiwum.giodo.gov.pl/pl/1520111/4722 (dostęp: 07.02.2021).
[518] EROD, *Wytyczne 2/2019*…, s. 15-16.

bezpośredniego oraz profilowania[519] na innej podstawie prawnej – art. 6 ust. 1 lit. f rozporządzenia 2016/679, o ile zostaną spełnione określone w nim warunki. Podkreślić należy, że art. 28 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)[520], którego rozpoczęcie stosowania przypada na 17 lutego 2024 r., stanowi że dostawcy platform internetowych nie mogą prezentować na swoim interfejsie reklam opartych na profilowaniu w rozumieniu zgodnie z art. 4 pkt 4 rozporządzenia 2016/679 z wykorzystaniem danych osobowych odbiorcy usługi, jeżeli wiedzą z wystarczającą pewnością, że odbiorca usługi jest małoletni. Innymi słowy przepis ten wyłącza możliwość profilowania danych osobowych dzieci w celu wyświetlania reklam.

EROD sygnalizuje również, że umowy muszą być zawierane i wykonywane z poszanowaniem właściwych przepisów z zakresu prawa umów, ochrony konsumentów, aby można było uznać, że przetwarzanie danych osobowych w tych celach było rzetelne i zgodne z prawem[521]. Rada podkreśla obowiązek administratora zapewnienia zgodności zawierania i wykonywania umów z prawem krajowym, w tym regulującym tę materię w odniesieniu do dzieci[522]. Stosownie do art. 8 ust. 3 rozporządzenia 2016/679, przepis określający wiek dziecka w kontekście wyrażenia zgody na przetwarzanie danych osobowych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, nie wpływa na ogólne przepisy prawa umów państw członkowskich, takie jak przepisy o ważności, zawieraniu lub skutkach umowy wobec dziecka.

Ważność zawarcia umowy jest uzależniona od posiadania zdolności do czynności prawnych. Jak już wspomniano wcześniej, czynność prawna dokonana przez osobę, która nie ukończyła lat trzynastu, jest nieważna. Istotny wyjątek wprowadza art. 14 §2 kc, który stanowi, że jeśli doszło do zawarcia umowy należącej do umów powszechnie zawieranych w drobnych bieżących sprawach życia codziennego, umowa taka staje się ważna z chwilą jej wykonania, o ile nie pociąga za sobą rażącego pokrzywdzenia osoby niezdolnej do czynności prawnych. Jest to pewien wyjątek od reguły, że czynność prawna dokonana przez dziecko, które nie ukończyło 13 roku życia, jest nieważna i nie może być potwierdzona przez przedstawicieli ustawowych[523]. Jeśli natomiast umowa została zawarta bez zgody przedstawiciela ustawowego, jej ważność zależy od tego, czy zostanie przez nią potwierdzona (art. 18 §1 kc) – do momentu potwierdzenia stanowi

[519] Za wyjątkiem profilowania będącego operacją wchodzącą w skład przetwarzania polegającego na podejmowaniu decyzji w sposób zautomatyzowany w rozumieniu art. 22 rozporządzenia 2016/679.
[520] Dz. Urz. UE L 277 z 27.10.2022, s. 1, dalej jako: „rozporządzenie 2022/2065". Na temat genezy i założeń rozporządzenia 2022/2065 por. X. Konarski, *Unijny Akt o Usługach Cyfrowych – cele uchwalenia, zakres stosowania oraz najważniejsze obowiązki dostawców usług pośrednich*, „Prawo Nowych Technologii" 2022, nr 3.
[521] EROD, *Wytyczne 2/2019*…, s. 5.
[522] Tamże, s. 6.
[523] S. Grobel, *Treść władzy…*, s. 193.

czynność prawną niezupełną (*negotium claudicans*)[524]. Osoba ograniczona w zdolności do czynności prawnych może jednak bez zgody przedstawiciela ustawowego zawierać umowy należące do umów powszechnie zawieranych w drobnych bieżących sprawach życia codziennego (art. 20 kc).

W kontekście zawierania umów o świadczenie usług społeczeństwa informacyjnego, podobnie jak w przypadku zgody na przetwarzanie danych osobowych, problematyczna jest kwestia weryfikacji wieku osoby, która ma dokonać czynności prawnej, a także sposobu uzyskania zgody lub potwierdzenia przedstawiciela ustawowego. Rozważania w tej materii poczynione na gruncie art. 8 rozporządzenia 2016/679 można zastosować odpowiednio w przypadku zawierania umów. Dodatkowej analizy wymaga pojęcie umów powszechnie zawieranych w drobnych bieżących sprawach życia codziennego, które ma fundamentalne znaczenie dla oceny ważności umów zawieranych przez dzieci w związku z korzystaniem z usług społeczeństwa informacyjnego, a także możliwości przetwarzania ich danych osobowych na podstawie art. 6 ust. 1 lit. b rozporządzenia 2016/679. Możliwość powołania się na tę przesłankę w zakresie, w jakim przetwarzanie danych osobowych jest niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, wydaje się dopuszczalne w każdym przypadku – nawet gdy tą osobą jest dziecko nieposiadające zdolności do czynności prawnych – ponieważ przetwarzanie np. w celu weryfikacji wieku i sprawdzenia, czy osoba podająca dane może zawrzeć umowę, zmierza do zawarcia umowy, co nie zmienia faktu, że może to nie dojść do skutku. Jednak w przypadku, gdy administrator wie, że czynność prawna jest nieważna, bo przykładowo dokonało jej 10-letnie dziecko, a nie zachodzi okoliczność wskazana w art. 14 §2 kc, przetwarzanie jego danych osobowych nie powinno być dopuszczalne na podstawie art. 6 ust. 1 lit. b rozporządzenia 2016/679 w celu wykonania umowy, skoro ta umowa jest nieważna. Odpadła bowiem podstawowa okoliczność upoważniająca do przetwarzania danych osobowych, a dane osobowe, które zostały pozyskane w celu zawarcia umowy, powinny być usunięte.

Pojęcie umów powszechnie zawieranych w drobnych bieżących sprawach życia codziennego zostało wprowadzone jako odpowiedź na potrzeby życia codziennego i współczesnego obrotu[525]. Jako sformułowanie niedookreślone może rodzić trudności interpretacyjne. Uważa się, że kluczowym czynnikiem w kwalifikacji umowy jako zawieranej w drobnych bieżących sprawach życia codziennego jest jej przedmiot oraz jego wartość – „Czynności tego rodzaju służą zaspokojeniu potrzeb konsumpcyjnych, niepowodujących znacznych wydatków, są one typowe w obecnych stosunkach prawnych, nie wymagają

[524] M. Pazdan, Glosa do postanowienia SN z dnia 15 grudnia 1999 r., I CKN 299/98, LEX.
[525] S. Kalus, *Komentarz do art. 14 kc*, [w:] M. Fras, M. Habdas (red.), *Kodeks cywilny...*, s. 83.

szczególnej wiedzy ani rozeznania”[526]. R. Mianowana-Kubiak zwraca także uwagę, że istotna jest „typowość umowy w stosunkach społecznych charakterystycznych dla grupy, do której przynależy osoba niezdolna do czynności prawnych (małoletni), nieskomplikowanie procedury zawierania umowy”[527]. W literaturze jako przykłady umów zawieranych przez dzieci w drobnych bieżących sprawach życia codziennego podaje się umowy nabycia przyborów szkolnych, książek, prasy, żywności, biletów autobusowych, biletów na wydarzenia kulturalne lub sportowe, a także umowy przewozu, umowy zamiany[528]. Ocena, czy dana umowa jest zawierana w drobnych bieżących sprawach życia codziennego powinna być także uzależniona od wieku dziecka. T. Sokołowski słusznie zauważa, że „drobne sprawy odnoszące się do osoby w wieku powyżej 13 lat mają z natury rzeczy szerszy zakres niż w odniesieniu do młodszego dziecka. Zakres ten ulega coraz bardziej dynamicznemu wzrostowi w miarę dorastania dziecka lub podopiecznego”[529]. Za zróżnicowaniem podejścia do tej kwestii ze względu na wiek dziecka opowiada się także S. Kalus podnosząc, że starsze dziecko „dysponuje większą dozą rozeznania”[530]. W literaturze wyrażono pogląd, że interpretacja umów powszechnie zawieranych w drobnych bieżących sprawach życia codziennego powinna dążyć do obiektywizacji – ocena powinna być dokonywana przez pryzmat bieżących potrzeb konsumpcyjnych przeciętnej rodziny[531]. Sytuacja materialna dziecka i jego rodziców czy miejsce zamieszkania (np. miasto lub wieś) nie powinny być decydującymi kryteriami[532]. Z drugiej strony niektórzy autorzy opowiadają się za badaniem indywidualnej sytuacji danego dziecka i otoczenia, w którym się wychowuje – P. Nazaruk, rozważając zakres pojęcia umów powszechnie zawieranych w drobnych bieżących sprawach życia codziennego, podaje przykład dwunastoletniego dziecka, które ma zamożnych rodziców i kupuje luksusowe zabawki[533]. Najbardziej trafne wydaje się pierwsze podejście, zakładające odwołanie do wzorca tzw. przeciętnej rodziny, jej potrzeb konsumpcyjnych, sytuacji materialnej, z uwzględnieniem wieku dziecka. Identyczne traktowanie dziesięcio- i siedemnastolatka jest z oczywistych powodów nieuzasadnione. Nawet poruszając się w granicach wiekowych, które wyznaczają początek i koniec posiadania ograniczonej zdolności do czynności prawnych, z pewnością należy przyjąć inną ocenę umów zawieranych przez dzieci, które dopiero ją osiągnęły, niż nastolatków, które zbliżają się do pełnoletności.

[526] M. Serwach, *Komentarz do art. 14 kc*, [w:] P. Księżak, M. Pyziak-Szafnicka (red.), *Kodeks cywilny. Komentarz. Część ogólna*, wyd. II, Warszawa 2014, s. 217.
[527] R. Mianowana-Kubiak, *Małoletni jako strona w umowie rachunku wspólnego – rozważania na tle ustaw: Kodeks cywilny, Kodeks rodzinny i opiekuńczy oraz Prawo bankowe*, „Monitor Prawa Bankowego” 2014, nr 5, s. 73-81.
[528] S. Kalus, *Komentarz do art. 14 kc*, [w:] M. Fras, M. Habdas (red.), *Kodeks cywilny...*, s. 83.
[529] T. Sokołowski, *Komentarz do art. 20 kc*, [w:] A. Kidyba (red.), *Kodeks cywilny…*, s. 105.
[530] S. Kalus, *Komentarz do art. 14 kc*, [w:] M. Fras, M. Habdas (red.), *Kodeks cywilny...*, s. 83.
[531] M. Serwach, *Komentarz do art. 14 kc*, [w:] P. Księżak, M. Pyziak-Szafnicka (red.), *Kodeks cywilny…*, s. 216.
[532] Tamże.
[533] P. Nazaruk, *Komentarz do art. 14 kc*, [w:] J. Ciszewski (red.), *Kodeks cywilny. Komentarz*, Warszawa 2019, s. 86.

W kontekście świadczenia usług społeczeństwa informacyjnego, nawet przy przyjęciu powyższych założeń, kwestia kwalifikacji umów jako powszechnie zawieranych w drobnych bieżących sprawach życia codziennego jest bardziej skomplikowana niż w przypadku umów, które nie są zawierane drogą elektroniczną. Wynika to m.in. ze sposobu zawierania umowy. O ile w przypadku umów zawieranych w lokalu przedsiębiorstwa – zakupów przedmiotów, np. książki, co do zasady można dokonać tego anonimowo, o tyle przy zakupie przez internet książki w postaci elektronicznej (ebooka) sposób dokonania tej czynności powoduje, że kupujący musi podać swoje dane osobowe – przynajmniej adres poczty elektronicznej by otrzymać produkt. Ponadto korzystanie z niektórych rodzajów usług społeczeństwa informacyjnego, takich jak portale społecznościowe, ze swej istoty wiąże się z przetwarzaniem dużej ilości danych osobowych – związanych nie tylko z rejestracją konta w tym serwisie, ale przede wszystkim pozyskiwanych w toku korzystania z jego funkcji. Nie można jednak nie zauważyć, że prowadzenie konta w serwisie internetowym i korzystanie z jego podstawowych funkcji może być oparte na podstawie art. 6 ust. 1 lit. b rozporządzenia 2016/679, zaś dodatkowe cele, które nie są niezbędne, mogą być realizowane na innej przesłance, np. zgodzie użytkownika. W pierwszym przypadku trudno uznać, że taka czynność wykracza poza ramy pojęcia umów zawieranych w drobnych bieżących sprawach życia codziennego. Wydaje się, że podobnie podejść można do korzystania z usług społeczeństwa informacyjnego polegających na udostępnianiu muzyki, filmów, z których korzysta się na co dzień. Różnorodność usług społeczeństwa informacyjnego jest tak duża, że nieodzowne jest indywidualne badanie stanu faktycznego pod kątem możliwości uznania danej umowy za zawieranej w drobnych bieżących sprawach życia codziennego.

3.3 Przetwarzanie w celach wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią

Zgodnie z art. 6 ust. 1 lit. f rozporządzenia 2016/679, przetwarzanie danych osobowych jest zgodne z prawem, jeśli jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem. Mając zamiar przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679, administrator powinien ocenić, czy zostaną spełnione kumulatywnie dwie przesłanki: czy występują prawnie uzasadniony interes i czy przetwarzanie danych osobowych jest niezbędne do realizacji wynikających z niego celów, a

także czy nie zachodzi okoliczność wyłączająca dopuszczalność powołania się na tę podstawę[534]. Kluczowe jest więc ustalenie, na czym polega prawnie uzasadniony interes, którego nie można osiągnąć bez przetwarzania danych osobowych, a następnie ocena, czy interesy lub podstawowe prawa i wolności osób, których dane dotyczą, nie mają nad nim prymatu, biorąc pod uwagę konkretny stan faktyczny – przeprowadzenie tzw. testu równowagi. Nadrzędność interesów i praw osób, których dane dotyczą, może wystąpić zwłaszcza wtedy, gdy nie spodziewają się one przetwarzania – należy zatem uwzględnić przede wszystkim to, czy istnieje już relacja między nimi a administratorem, np. czy planowane przetwarzanie dotyczy danych osobowych klientów administratora[535]. Cel wynikający z prawnie uzasadnionego interesu, który jest odpowiednikiem występującego na gruncie uodo z 1997 r. pojęcia prawnie usprawiedliwionego celu[536], należy oceniać przez pryzmat prowadzonej działalności i czy nie narusza ona prawa, zasad współżycia społecznego i dobrych obyczajów – nie jest jednak wymagane, by ten cel był uprzednio skonkretyzowany w przepisie prawa[537]. Stanowisko to pozostaje aktualne również pod rządami rozporządzenia 2016/679. Potwierdza to art. 13 ust. 1 lit. d rozporządzenia 2016/679, który nakazuje informować osoby, których dane dotyczą, na czym polega prawnie uzasadniony interes, na który powołuje się administrator – jest to zatem okoliczność, którą on definiuje, z poszanowaniem wyżej wskazanych kryteriów. W opinii Grupy Roboczej Art. 29 wydanej na kanwie dyrektywy 95/46, uznanie interesu za uzasadniony wymaga sprawdzenia, czy jest on legalny (zgodny z prawem UE i państwa członkowskiego), wystarczająco jasno sformułowany (konkretny) oraz czy jest rzeczywisty i aktualny[538]. W motywach 47-49 preambuły rozporządzenia 2016/679 prawodawca unijny wskazał przykładowe działania, które można uznać za wynikające z prawnie uzasadnionego interesu: przetwarzanie danych osobowych do celów marketingu bezpośredniego; przesyłanie danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych; przetwarzanie danych osobowych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji, np. w związku z zapobieganiem nieuprawnionemu dostępowi do sieci łączności elektronicznej.

Przepis art. 6 ust. 1 lit. f rozporządzenia 2016/679 ma na celu uelastycznienie przetwarzania danych osobowych w środowisku *online*, w tym usług społeczeństwa

---

[534] W. Chomiczewski, *Komentarz do art. 6 ust. 1 lit. f rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 390.
[535] Motyw 47 preambuły rozporządzenia 2016/679.
[536] W art. 7 lit. f dyrektywy 95/46 mowa była o uzasadnionych interesach administratora lub osoby trzeciej.
[537] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, s. 430-431. O zgodności interesu z dobrymi obyczajami mowa także w artykule C. O. Mihăilă, M. Mihăilă, *The legal interest, legal basis for the processing of personal data and the right to private life*, „Fiat Iustitia" 2020, nr 1, s. 132.
[538] Grupa Robocza Art. 29, *Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE*, przyjęta w dniu 9 kwietnia 2014 r., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_pl.pdf (dostęp: 07.02.2021), s. 63.

informacyjnego, uwzględniając jego szczególną specyfikę – wynikającą m.in. z wykorzystania nowoczesnych technik i sposobów przetwarzania danych osobowych, niewymagających udziału człowieka, czy zaangażowania wielu podmiotów w tym samym procesie przetwarzania, dokonujących w jego ramach wybranych operacji[539]. Z perspektywy administratorów, za zastosowaniem przesłanki prawnie uzasadnionego interesu w tym kontekście przemawia to, że nie wymaga ona żadnych działań ze strony osoby, której dane dotyczą – w przeciwieństwie do przetwarzania w oparciu o zgodę, gdzie konieczne jest spełnienie rygorystycznych warunków jej pozyskania – jednak, patrząc z kolei przez pryzmat praw osób, których dane dotyczą, „Nie wolno zapominać, iż podstawa ta stanowi odejście od zasady samostanowienia przez osobę, której dane dotyczą, o tym, co dzieje się z jej danymi, a przez to potencjalnie wiąże się z większym ryzykiem naruszenia jej praw czy wolności”[540]. Ponadto już przed reformą ochrony danych osobowych dostrzeżono ryzyko nadużywania przesłanki uzasadnionego interesu w sytuacji, gdy nie można powołać się na żadną inną – traktowanie jej jako „otwartej furtki”[541]. Najprawdopodobniej z tego powodu prawodawca unijny uznał, że konieczne jest zaakcentowanie w art. 6 ust. 1 lit. f rozporządzenia 2016/679, że dopuszczalne jest przetwarzanie danych osobowych w ramach prawnie uzasadnionych interesów „z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem”. Brak jakichkolwiek regulacji w zakresie przetwarzania danych osobowych dzieci w celach marketingu bezpośredniego w dyrektywie 95/46 był słusznie krytykowany[542], a jest to typowy przykład zastosowania klauzuli prawnie uzasadnionego interesu. W literaturze prezentowane są skrajnie różne podejścia do problemu, czy obecnie przetwarzanie danych osobowych dzieci na tej podstawie jest dopuszczalne.

Podejście rygorystyczne przejawia się w uznaniu niedopuszczalności przetwarzania danych osobowych dziecka na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679. Zdaniem P. Litwińskiego, M. Kaweckiego i P. Barty jest to wykluczone, ponieważ wykładnia językowa prowadzi do wniosku, że jeśli osoba, której dane dotyczą, jest dzieckiem, zawsze występuje nadrzędność jej interesów lub podstawowych prawa i wolności, wymagających ochrony danych osobowych, w stosunku do interesów realizowanych przez administratora lub przez stronę trzecią[543].

---

[539] M. Czerniawski, *Prawnie uzasadnione interesy jako podstawa przetwarzania danych online*, „Prawo Mediów Elektronicznych” 2018, nr 3, Legalis.
[540] Tamże.
[541] Grupa Robocza Art. 29, *Opinia 06/2014…,* s. 6.
[542] E. Bartoli, *Children's data protection vs marketing companies*, „International Review of Law, Computers & Technology” 2009, nr 23, s. 41.
[543] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 6 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis.

Podejście umiarkowane polega na uznaniu za dopuszczalne przetwarzanie danych osobowych dziecka na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679 pod warunkiem dołożenia należytej staranności w rzetelnym przeprowadzeniu testu równowagi i wdrożenia odpowiednich środków ochrony praw dziecka. Takie stanowisko prezentuje M. Czerniawski podnosząc, że decyzję o przetwarzaniu danych osobowych na podstawie ww. przepisu zawsze, także w przypadku dzieci, należy oprzeć na rezultacie wyniku testu równowagi, a także wskazując, że „co do zasady prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią nie będą mieć nadrzędnego charakteru wobec interesów bądź podstawowych praw i wolności dziecka, a ewentualne przetwarzanie takich danych na podstawie tej przesłanki będzie wymagać podjęcia przez administratora danych szczególnych środków ochrony”[544]. Z kolei W. Chomiczewski uważa, w ślad za przedstawicielami niemieckiej doktryny, że możliwość zastosowania tej przesłanki powinna być uzależniona od kryterium wieku dziecka – ukończenia przez niego 13 lub 16 roku życia – wyznaczonego w art. 8 rozporządzenia 2016/679, ponieważ te progi wiekowe determinują poziom ochrony danych osobowych dziecka na gruncie całego rozporządzenia 2016/679. W. Chomiczewski stoi na stanowisku, że na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679 „należy dopuszczać przetwarzanie danych osobowych dzieci poniżej 13. roku życia jedynie w wyjątkowych i szczególnie uzasadnionych sytuacjach. W przedziale wiekowym od 13. do 16. roku życia rygor ten można zmniejszyć, ale nadal należy zakładać, że interesy, podstawowe prawa i wolności dziecka, które wymagają ochrony jego danych osobowych, będą miały prymat nad prawnie uzasadnionymi interesami administratora lub strony trzeciej”[545].

Podejście liberalne nie tylko zakłada dopuszczalność przetwarzania danych osobowych dziecka na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679, ale wręcz promuje tę przesłankę jako przyczyniającą się do podniesienia poziomu ochrony – zwłaszcza w porównaniu do przetwarzania na podstawie zgody. Jak argumentują M. Macenaite i E. Kosta, prawidłowe zastosowanie klauzuli prawnie uzasadnionego interesu w przypadku przetwarzania danych osobowych dzieci stanowi dodatkową gwarancję, ponieważ doznaje wielu ograniczeń ze względu na ich szczególny status, a wykazanie nadrzędności interesu administratora nad ich prawami jest o wiele trudniejsze, niż w przypadku przetwarzania danych osobowych dotyczących osób dorosłych, a także bardziej skomplikowane, niż uzyskanie zgody na przetwarzanie danych osobowych[546].

[544] M. Czerniawski, *Prawnie uzasadnione interesy…*, Legalis.
[545] W. Chomiczewski, *Komentarz do art. 6 ust. 1 lit. f rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 398-399, i tam powołana literatura.
[546] M. Macenaite, E. Kosta, *Consent for processing…*, s. 172.

Przechodząc do oceny wyżej przedstawionych stanowisk należy zauważyć, że całkowite, bezwarunkowe wykluczenie zastosowania art. 6 ust. 1 lit. f rozporządzenia 2016/679 w przypadku danych osobowych dzieci nie wynika z treści tego przepisu, ani żadnego motywu. Grupa Robocza Art. 29 wprost dopuszczała stosowanie klauzuli uzasadnionego interesu przy przetwarzaniu danych osobowych dzieci, podając jako przykład stronę internetową dla nastolatków, poświęconą ich problemom, która zbiera dane o odwiedzających ją osobach w celu sporządzania, docelowo anonimowych, statystyk na temat zainteresowania stroną[547]. Co więcej, stosowanie podejścia rygorystycznego mogłoby prowadzić do negatywnych konsekwencji. Dla przykładu, wykluczenie tej przesłanki uniemożliwiłoby, w świetle braku innej adekwatnej podstawy prawnej przetwarzania, realizację w pełni zrozumiałych interesów administratora (a w zależności od okoliczności – także osób, których dane dotyczą), polegających na zapewnieniu bezpieczeństwa sieci i informacji, o czym mowa w motywie 49 preambuły rozporządzenia 2016/679. Uzależnienie przetwarzania danych osobowych np. od wyrażenia zgody przez użytkownika portalu internetowego – który może odmówić jej udzielenia, lub w dowolnym momencie ją wycofać – mogłoby doprowadzić do powstania zagrożeń w obszarze bezpieczeństwa informatycznego, w tym ograniczeń w ich wykrywaniu i dokumentowaniu, a ponadto stosowanie związanych z tym rozwiązań wybiórczo byłoby, jak się wydaje, bardzo trudne lub wręcz niemożliwe do wdrożenia z powodów technicznych. Z kolei argumenty przytoczone przez W. Chomiczewskiego zasługują tylko na częściowe poparcie, ponieważ, po pierwsze, art. 8 rozporządzenia 2016/679 i wyznaczone w nim kryterium wieku odnosi się wyłącznie do kwestii wyrażenia zgody na przetwarzanie danych osobowych w przypadku usług społeczeństwa informacyjnego skierowanych bezpośrednio do dziecka, co jest wskazane w tym przepisie poprzez odesłanie wprost do art. 6 ust. 1 lit. a rozporządzenia 2016/679, a zatem nie jest uprawnione przenoszenie tych rozwiązań *per analogiam* na grunt innych przesłanek legalizujących przetwarzanie, ani tym bardziej uznanie, że stanowią one determinantę poziomu ochrony danych osobowych dziecka w ogólności. Po drugie, ryzyko naruszenia interesów lub podstawowych praw i wolności dziecka, wymagających ochrony danych osobowych, będzie, jak się wydaje, wynikać raczej z celu konkretnego przetwarzania, rodzajów operacji przetwarzania, niż tylko z jego wieku. Słabością podejścia liberalnego, zwłaszcza jego aprobaty dla stosowania klauzuli prawnie uzasadnionego interesu w przypadku dzieci, jest oparcie go na idealistycznym założeniu, że każdy administrator wyważy interesy obiektywnie, rzetelnie i uczciwie, co może budzić wątpliwości. Zresztą nawet jeśli działa on w

[547] Grupa Robocza Art. 28, *Opinia 06/2014*…, s. 77. Wydaje się, że jej stanowisko nie utraciło aktualności, ponieważ zostało wypracowane przy założeniu, że dziecko wymaga szczególnej ochrony i konieczne jest przeprowadzenie testu równowagi, a zatem z uwzględnieniem wymogów niekwestionowanych ani przed, ani po wejściu w życie rozporządzenia 2016/679. EROD stwierdziła, że ww. wytyczne zachowały aktualność „w ujęciu ogólnym" – EROD, *Wytyczne 2/2019*…, s. 5.

dobrej wierze, zauważyć należy, że nie istnieje jeden, obowiązujący standard przeprowadzania testu równowagi, co rodzi obawy o subiektywność dokonywanych ocen. Natomiast na aprobatę zasługuje podejście umiarkowane, prezentowane przez M. Czerniawskiego. Przetwarzanie danych osobowych dziecka na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679 powinno być dopuszczone w szczególnych przypadkach, po przeprowadzeniu testu równowagi i wdrożeniu dodatkowych gwarancji[548]. Warto zatem skłonić się ku wąskiej interpretacji, lecz niewykluczającej stosowania ww. przepisu w przypadku dzieci, zwłaszcza gdy prawnie uzasadniony interes polega na zapewnieniu bezpieczeństwa informatycznego.

3.4 Przetwarzanie oparte na innych przesłankach

Przepis art. 6 rozporządzenia 2016/679 przewiduje także inne przesłanki legalizujące przetwarzanie. Zgodnie z art. 6 ust. 1 lit. c rozporządzenia 2016/679, przetwarzanie danych osobowych jest zgodne z prawem, jeśli jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Z kolei stosownie do art. 6 ust. 1 lit. e rozporządzenia 2016/679, przetwarzanie danych osobowych jest zgodne z prawem, jeśli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi[549]. W przypadku przetwarzania danych osobowych przez podmioty świadczące usługi społeczeństwa znaczenie przesłanki z art. 6 ust. 1 lit. e rozporządzenia 2016/679 informacyjnego ma jednak marginalne znaczenie ze względu na charakter i cele ich działalności. Zdecydowanie większe znaczenie ma podstawa przetwarzania określona w art. 6 ust. 1 lit. c rozporządzenia 2016/679, ponieważ te podmioty mogą być adresatami rozmaitych obowiązków wynikających z przepisów prawa – chociażby w związku z prowadzeniem działalności gospodarczej.

Charakterystycznym dla podmiotów świadczących usługi społeczeństwa informacyjnego (i usługi świadczonej drogą elektroniczną) jest obowiązek nieodpłatnego udostępniania danych określonych w art. 18 ust. 1-5 uśude organom państwa uprawnionym na podstawie odrębnych przepisów na potrzeby prowadzonych przez nie postępowań (art. 18 ust. 6 uśude). Ponieważ w wyżej wskazanych ustępach, za wyjątkiem pierwszego, ustawodawca nie określił zamkniętego

[548] Przy wspomnianym wcześniej przykładzie strony internetowej dla nastolatków Grupa Robocza Art. 29 wyjaśniła, że „przetwarzanie leży w interesie publicznym i wprowadzone są surowe gwarancje (dane są natychmiast anonimizowane i wykorzystywane wyłącznie do tworzenia statystyk), co pomaga przechylić szalę na korzyść administratora danych" – Grupa Robocza Art. 28, *Opinia 06/2014*…, s. 77.

[549] Na temat pojęcia zadania publicznego por. G. Sibiga, *Kryterium „zadania publicznego" w ustawie z 10.5.2018 r. o ochronie danych osobowych oraz jego konsekwencje dla wykonywania obowiązków administratora oraz realizacji praw osoby, której dane dotyczą*, [w:] G. Sibiga (red.), *Przepisy prawa uzupełniające RODO. Aktualne problemy prawnej ochrony danych osobowych 2018* (dodatek do „Monitora Prawniczego" 2018, nr 22), Warszawa 2018, s. 11-12; A. Nerka, M. Sakowska-Baryła, *Komentarz do art. 6 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis; M. Czerniawski, *Interes publiczny w ogólnym rozporządzeniu o ochronie danych. Wybrane zagadnienia*, „Informacja w administracji publicznej" 2019, nr 1, s. 17.

katalogu informacji, udostępnieniu podlegają wszelkie dane przetwarzane w związku ze świadczeniem usługi[550]. Wśród nich niewątpliwie znajdują się dane osobowe. Podstawą prawną przetwarzania danych osobowych polegającego na ich udostępnieniu organowi państwa jest zatem art. 6 ust. 1 lit. c rozporządzenia 2016/679, uśude oraz właściwe przepisy ustawy, na podstawie której prowadzone jest dane postępowanie[551] – ponieważ udostępnienie danych osobowych jest obowiązkiem wynikającym z tych przepisów. Za ochronę danych osobowych pozyskanych w ten sposób odpowiada organ, który zażądał ich udostępnienia, jako odrębny administrator. Nie zwalnia to jednak „pierwotnego" administratora (usługodawcy) z analizy, czy żądanie udostępnienia danych osobowych jest uzasadnione, zanim nastąpi jego spełnienie[552]. Zgodnie z motywem 31 preambuły rozporządzenia 2016/679, żądanie ujawnienia danych osobowych, z którym występują organy publiczne w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych, a przetwarzając otrzymane dane osobowe, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

Obowiązki usługodawców związane z udostępnianiem informacji, w tym danych osobowych, określają także przepisy innych ustaw. W szczególności należy zwrócić uwagę na ustawę z dnia 6 kwietnia 1990 r. o Policji[553], w której w wyniku nowelizacji z 2016 r.[554] nałożono na usługodawców obowiązek zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej (art. 19 ust. 12 i 12a). Analogiczny obowiązek dotyczy działań prowadzonych przez inne podmioty, w tym Straż Graniczną, tzw. wywiad skarbowy czy służby specjalne[555]. Z perspektywy usługodawcy,

[550] K. Chałubińska-Jentkiewicz, J. Taczkowska-Olszewska, *Komentarz do art. 18 uśude*, *Świadczenie usług…*, Legalis.
[551] Np. kpk, kpc.
[552] Największe przedsiębiorstwa – jak np. dostawca Facebook, LinkedIn czy usług Google – publikują informacje na temat otrzymanych żądań (ich liczby i rodzaju), a także o tym, ile spośród nich zostało zrealizowanych – raporty dotyczące ww., nazywane *Transparency Report,* dostępne są pod adresami https://transparency.facebook.com/government-data-requests, https://about.linkedin.com/transparency/government-requests-report, https://transparencyreport.google.com/user-data/overview?hl=pl (dostęp: 07.02.2021). Podmioty te nie uwzględniają wszystkich żądań.
[553] T.j. Dz.U. z 2023 r. poz. 171 z późn zm.
[554] Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw, Dz. U. z 2016 r. poz. 147.
[555] Wprowadzone rozwiązania są krytykowane przez Rzecznika Praw Obywatelskich (Biuro RPO, *Inwigilacja i uprawnienia polskich służb specjalnych w ETPC. Rzecznik przedstawia swą opinię*, 30.07.2020, https://www.rpo.gov.pl/pl/content/etpc-zbada-uprawnienia-polskich-sluzb-specjalnych-opinia-rpo, dostęp: 07.02.2021) oraz organizacje pozarządowe zajmujące się ochroną praw człowieka, w tym prawa do prywatności. Przetwarzanie przez właściwe organy danych osobowych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar powinno odbywać się zgodnie z dyrektywą 2016/680 – choć poza jej zakresem pozostaje działalność nieobjęta zakresem prawa UE, co ogranicza jej zastosowanie w przypadku służb specjalnych (Fundacja Panoptykon, *Pogrzebana szansa na ochronę danych w służbach*, 10.05.2018, https://panoptykon.org/wiadomosc/pogrzebana-szansa-na-ochrone-danych-w-sluzbach, dostęp: 07.02.2021). Warto zwrócić uwagę, że szeroki dostęp służb specjalnych Stanów Zjednoczonych

udostępnienie tym podmiotom danych osobowych również jest przykładem zastosowania przesłanki przetwarzania, o której mowa w art. 6 ust. 1 lit. c rozporządzenia 2016/679 i nie istnieją odmienności w sposobie stosowania tych przepisów w odniesieniu do danych osobowych dzieci.

Zgodnie z art. 6 ust. 1 lit. d rozporządzenia 2016/679, przetwarzanie danych osobowych jest zgodne z prawem, jeśli jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej. Wskazówek interpretacyjnych dotyczących pojęcia „żywotnych interesów" dostarcza motyw 46 preambuły rozporządzenia 2016/679. Prawodawca unijny wyjaśnił w nim, że chodzi o interes, który ma istotne znaczenie dla życia osoby, której dane dotyczą, lub innej osoby fizycznej. Podano w nim następujące przykłady żywotnych interesów osób fizycznych: gdy przetwarzanie niezbędne do celów humanitarnych, w tym monitorowania epidemii i ich rozprzestrzeniania się lub w nadzwyczajnych sytuacjach humanitarnych, w szczególności w przypadku klęsk żywiołowych i katastrof spowodowanych przez człowieka. Należy zgodzić się z poglądem, że żywotny interes może być związany z ochroną zdrowia, życia lub majątku[556]. Jednocześnie prawodawca zaznaczył, że „Żywotny interes innej osoby fizycznej powinien zasadniczo być podstawą przetwarzania danych osobowych wyłącznie w przypadkach, gdy ewidentnie przetwarzania tego nie da się oprzeć na innej podstawie prawnej". Powołanie się na art. 6 ust. 1 lit. d rozporządzenia 2016/679 będzie zatem szczególnie uzasadnione w nagłych przypadkach, wymagających przetwarzania danych osobowych, gdzie kluczowe dla ochrony żywotnych interesów jest szybkie reagowanie, a przykładowo pozyskiwanie zgód na przetwarzanie danych osobowych z zachowaniem wszystkich wymogów mogłoby ten cel zniweczyć lub znacznie utrudnić. Ocena, czy ww. przesłanka może być zastosowana, zależy więc od analizy konkretnego stanu faktycznego[557].

W przypadku usług społeczeństwa informacyjnego nie wydaje się, by art. 6 ust. 1 lit. d rozporządzenia 2016/679 znajdował szerokie zastosowanie. W razie powzięcia niepokojących informacji o dziecku, np. o jego zaginięciu, z żądaniem udostępnienia danych potrzebnych do ustalenia sytuacji dziecka może wystąpić np. policja, po otrzymaniu zawiadomienia od opiekuna prawnego, a zatem przetwarzanie danych osobowych odbywałoby się na podstawie omawianej wcześniej przesłanki, o której mowa w art. 6 ust. 1 lit. c rozporządzenia 2016/679. W przypadku

Ameryki do danych osobowych użytkowników usług społeczeństwa informacyjnego był jednym z powodów unieważnienia przez TSUE wyrokiem z dnia 16.07.2020 w sprawie C-311/18 decyzji Komisji Europejskiej ustanawiającej tzw. Tarczę Prywatności – program pozwalający na przekazywanie danych osobowych podmiotom ze Stanów Zjednoczonych Ameryki, które spełniły określone w nim wymogi – co było istotnym czynnikiem ułatwiającym współpracę gospodarczą między państwami UE a Stanami i narzędziem pozwalającym na legalizację transferu danych osobowych zgodnie z art. 45 rozporządzenia 2016/679.

[556] W. Chomiczewski, *Komentarz do art. 6 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 378

[557] P. Fajgielski, *Ogólne rozporządzenie…*, s. 172.

przetwarzania na podstawie art. 6 ust. 1 lit. d rozporządzenia 2016/679 nie ma żadnych odmienności w sposobie jego stosowania w odniesieniu do danych osobowych dzieci.

3.5 Dopuszczalność przetwarzania szczególnych kategorii danych osobowych dziecka w kontekście świadczenia usług społeczeństwa informacyjnego

Dane osobowe, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, mogą być potencjalnie przetwarzane zwłaszcza w przypadku takich usług społeczeństwa informacyjnego, w których ich użytkownicy tworzą i publikują treści, zazwyczaj na temat własnego życia. Ten problem będzie więc dotyczył przede wszystkim portali społecznościowych. Ponadto administratorzy (dostawcy tego rodzaju usług), którzy stosują techniki pozwalające np. na rozpoznawanie twarzy utrwalonej na zamieszczonej fotografii w celu oznaczenia danej osoby na wszystkich innych zdjęciach znajdujących się w portalu, a także niekiedy w innych zasobach – przetwarzają dane biometryczne, co może rodzić niekorzystne skutki dla osoby, której dane dotyczą, zwłaszcza, gdy nie ma ona takiej świadomości i nie może w pełni kontrolować tego, co dzieje się z jej danymi przetwarzanymi z użyciem kontrowersyjnych technik[558]. Takie ryzyko niewątpliwe występuje w przypadku dzieci.

Stosownie do art. 9 ust. 2 rozporządzenia 2016/679, ogólny zakaz przetwarzania danych osobowych należących do szczególnych kategorii, o którym mowa w ust. wcześniejszym, jest uchylony, jeśli spełniony jest jeden z warunków określonych w tym przepisie. Z tego względu konstrukcje przepisów określających przesłanki legalności przetwarzania tzw. zwykłych danych osobowych (art. 6 ust. 1 rozporządzenia 2016/679) oraz danych osobowych należących do szczególnych kategorii uważane są za odmienne[559], jednak różnica ta zaciera się w praktyce ich stosowania, gdyż interpretuje się je tak samo: zgodne z prawem jest przetwarzanie wyłącznie wtedy, gdy spełniona jest przynajmniej jedna spośród wymienionych przesłanek.

W przypadku danych osobowych należących do szczególnych kategorii prawodawca unijny zaliczył do nich okoliczność: 1) wyrażenia przez osobę, której dane dotyczą, wyraźnej zgody na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, o ile prawo UE lub państwa członkowskiego nie przewidują, że osoba, której dane dotyczą, nie może uchylić tego zakazu (art. 9 ust. 1 lit. a rozporządzenia 2016/679); 2) niezbędności przetwarzania do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o

[558] Szerzej na ten temat por. M. Amarikwa, *Social Media Platforms' Reckoning: The Harmful Impact of TikTok's Algorithm on People of Color*, „Richmond Journal of Law & Technology" 2023, nr 3, s. 69-144.
[559] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 9 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 1.

ile jest to dozwolone prawem UE lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. b rozporządzenia 2016/679); 3) niezbędności przetwarzania do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, gdy osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody (art. 9 ust. 2 lit. c rozporządzenia 2016/679); 4) przetwarzania w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych – pod warunkiem, że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą (art. 9 ust. 2 lit. d rozporządzenia 2016/679); 5) przetwarzania danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą (art. 9 ust. 2 lit. e rozporządzenia 2016/679); 6) niezbędności przetwarzania do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy (art. 9 ust. 2 lit. f rozporządzenia 2016/679); 7) niezbędności przetwarzania ze względów związanych z ważnym interesem publicznym, na podstawie prawa UE lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. g rozporządzenia 2016/679); 8) niezbędności przetwarzania do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa UE lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia[560] (art. 9 ust. 2 lit. h rozporządzenia 2016/679); 9) niezbędności przetwarzania ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa UE lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę

[560] Ponadto, zgodnie z art. 9 ust. 3 rozporządzenia 2016/679, dane osobowe muszą być przetwarzane w tym celu „przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe".

zawodową (art. 9 ust. 2 lit. i rozporządzenia 2016/679); 10) niezbędności przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 rozporządzenia 2016/679, na podstawie prawa UE lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. j rozporządzenia 2016/679).

Mając na względzie świadczenie usług społeczeństwa informacyjnego jako kontekst przetwarzania danych osobowych, zastosowanie mogą znaleźć w szczególności przesłanki wymienione w art. 9 ust. 2 lit. a i e rozporządzenia 2016/679 (odpowiednio: wyraźna zgoda na przetwarzanie danych osobowych i upublicznienie w sposób oczywisty danych osobowych przez osobę, której dane dotyczą)[561].

Dopuszczalność przetwarzania danych osobowych dziecka, które należą do szczególnych kategorii danych osobowych, w związku ze świadczeniem usług społeczeństwa informacyjnego na podstawie zgody wydaje się wątpliwe. Prawodawca nie odniósł się do problematyki takiego przetwarzania w motywach preambuły ani w normatywnej części rozporządzenia 2016/679. Biorąc pod uwagę szczególne wymogi w zakresie pozyskania zgody na przetwarzanie tzw. danych zwykłych, określone w art. 8 rozporządzenia 2016/679, *a minori ad maius* nie mogą być one łagodniejsze w przypadku danych objętych szczególną ochroną. Jednocześnie trudno doszukać się uzasadnienia do stosowania przez analogię art. 8 rozporządzenia 2016/679. W obecnym stanie prawnym dopuszczalność przetwarzania danych osobowych dziecka, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, na podstawie zgody jest dyskusyjna, chyba, że wyraził ją przedstawiciel ustawowy.

Przesłanka dopuszczalności przetwarzania danych osobowych należących do szczególnych kategorii, o której mowa w art. 9 ust. 2 lit. e rozporządzenia 2016/679, spełniona jest wówczas, gdy upublicznienie tych danych przez osobę, której dotyczą, nie budzi żadnych wątpliwości – prawodawca unijny chciał to zaakcentować dodając zwrot „w sposób oczywisty", którego brakowało w analogicznym przepisie zawartym w dyrektywie 95/46[562]. Upublicznienie danych osobowych powinno nastąpić przez osobę, której dotyczą, choć uznaje się, że można tak traktować również upublicznienie za jej wyraźną zgodą[563]. Sposób upublicznienia może mieć dowolną formę, choć nie ulega wątpliwości, że ww. przepis będzie miał zastosowanie przede wszystkim w odniesieniu do publikacji w środkach masowego przekazu, takich jak internet,

[561] Na gruncie dyrektywy 95/46 istniały analogiczne przesłanki i zdaniem Grupy Roboczej Art. 29 były to dwie możliwe, dopuszczalne podstawy prawne przetwarzania szczególnych kategorii danych osobowych polegającego na ich publikowaniu w internecie – por. Grupa Robocza Art. 29, *Opinia nr 5/2009*…, s. 8-9.
[562] Por. M. Kuba, *Komentarz do art. 9 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO*…, s. 451.
[563] P. Fajgielski, *Ogólne rozporządzenie*…, s. 227.

telewizja, prasa lub radio[564]. Przepis art. 9 ust. 2 lit. e rozporządzenia 2016/679 ma zastosowanie w przypadku opublikowania przez osobę, której dane dotyczą, swoich danych osobowych np. na ogólnie dostępnych forach internetowych i to nawet wówczas, jeśli dostęp do tych treści wymaga zalogowania[565] (po uprzednim utworzeniu konta w serwisie). Ten pogląd zasługuje na aprobatę, ponieważ takie ograniczenie dostępu do treści znajdujących się w serwisie jest iluzoryczne, jeśli każdy może w łatwy i szybki sposób zapoznać się z nimi. Wydaje się, że odmiennie należy traktować sytuację, w której osoba publikująca informacje o sobie korzysta z ustawień w serwisie, takim jak portal społecznościowy, polegających na ograniczeniu dostępu do tych treści tylko dla określonego przez nią kręgu osób – np. jej „znajomych". Wówczas trudno uznać, że dane osobowe zostały upublicznione – gdyż upublicznienie należy rozumieć jako „możliwość zapoznania się z danymi przez niezamknięty, bliżej nieokreślony krąg osób"[566].

Do możliwości oparcia przetwarzania szczególnych kategorii danych osobowych dotyczących dziecka na podstawie art. 9 ust. 2 lit. e rozporządzenia 2016/679 należy podejść z dużą ostrożnością. Z uwagi na jego brzmienie i dobro dziecka właściwe wydaje się zajęcie stanowiska, że nie powinien mieć zastosowania w przypadku upublicznienia danych osobowych przez inną osobę, w tym przedstawiciela ustawowego. W literaturze słusznie zauważono, że bazowanie administratora na tym przepisie jest dla niego bardzo dogodne, ponieważ pozwala mu na przetwarzanie bez konieczności uzyskania wyraźnej zgody, o której mowa w art. 9 ust. 2 lit. a rozporządzenia 2016/679 i spełniającej wszystkie warunki ważności w myśl art. 7 rozporządzenia 2016/679[567]. Innymi słowy, istnieje zagrożenie, że okoliczność nieprzemyślanego opublikowania przez dziecko swoich danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, zostanie wykorzystana przez administratora do argumentowania, że przetwarzanie jest zgodne z prawem i nie jest konieczne podejmowanie wysiłków w celu pozyskania wyraźnej zgody przedstawiciela ustawowego. Uzasadnione jest uznanie, że stanowiłoby to poważne ryzyko, zatem warta rozważenia byłaby rewizja art. 9 ust. 2 lit. e rozporządzenia 2016/679 pod kątem przetwarzania danych osobowych dzieci-użytkowników społeczeństwa informacyjnego.

[564] A. Nerka, *Komentarz do art. 9 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 16.
[565] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 9 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 19.
[566] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, s. 499.
[567] Por. E. S. Dove, J. Chens, *What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e)*, „International Data Privacy Law" 2021, nr 2, s. 108.

4. Zasada ograniczenia celu

Stosownie do art. 5 ust. 1 lit. b rozporządzenia 2016/679, zasada ograniczenia celu oznacza, że dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Określenie celu leży u podstaw prawa ochrony danych osobowych, ponieważ jest punktem wyjścia do oceny legalności planowanych operacji przetwarzania i określenia, jakie zabezpieczenia powinny być zastosowane[568]. Cel przetwarzania powinien być określony możliwie jak najbardziej precyzyjnie – nie powinien być zbyt ogólnikowy, np. sformułowanie „cele marketingowe" jest na tyle pojemne, że nie wyjaśnia w dostateczny sposób, do jakich działań dane osobowe będą wykorzystywane[569]. To, że cel powinien być prawnie uzasadniony, nie należy interpretować w ten sposób, że musi istnieć konkretny przepis prawa, wskazujący na niego – chodzi o to, czy została spełniona przynajmniej jedna z określonych w rozporządzeniu 2016/679 przesłanek, pozwalających na przetwarzanie[570]. W świetle zasady ograniczenia celu nie jest dopuszczalne zbieranie danych osobowych „na zapas", na podstawie przypuszczenia, że mogą być przydatne w przyszłości do innych, bliżej nieokreślonych celów[571]. W motywie 39 preambuły do rozporządzenia 2016/679 wskazano, że cele przetwarzania powinny być określone w momencie ich zbierania. Wydaje się, że jest to sformułowanie nieprecyzyjne. W praktyce określenie celów następuje przed rozpoczęciem zbierania, a więc przetwarzania danych osobowych, zaś w momencie zbierania danych osobowych podmiot danych powinien być o celach poinformowany.

Przepis art. 5 ust. 1 lit. b rozporządzenia 2016/679 ustanawia generalny zakaz przetwarzania danych osobowych w sposób niezgodny z celami pierwotnie ustalonymi i przedstawionymi osobie, której dane dotyczą. Istnieją jednak wyjątki od tej reguły. Pierwszy dotyczy przetwarzania do celów archiwalnych w interesie publicznym, badań naukowych lub historycznych, statystycznych[572]. Drugi dotyczy przetwarzania wprawdzie w innych celach, niż pierwotne, ale zgodnych z nimi – o czym traktuje motyw 50 preambuły rozporządzenia 2016/679. Zawiera on wskazówki, co powinien wziąć pod uwagę administrator badając, czy inny cel przetwarzania jest zgodny z pierwotnym – mianowicie wszelkie powiązania pomiędzy celami pierwotnymi a celami

[568] Grupa Robocza Art. 29, Opinion 03/2013 on purpose limitation adpoted on 2 April 2013, https://archiwum.giodo.gov.pl/pl/1520167/6565 (dostęp: 07.02.2021), s. 15. Opinia zachowuje aktualność także po reformie ochrony danych osobowych ze względu na to, że zasady przetwarzania nie uległy zasadniczym zmianom w porównaniu do poprzedniego stanu prawnego.
[569] Tamże, s. 16.
[570] P. Fajgielski, *Ogólne rozporządzenie…*, s. 147.
[571] P. Drobek, *Zasada celowości w dobie wielkich zbiorów danych (big data)*, [w:] G. Sibiga (red.), *Aktualne problemy prawnej ochrony danych osobowych 2014*, Warszawa 2014, Legalis.
[572] Dalsze przetwarzanie danych osobowych w tych celach nie jest uważane za niezgodne z pierwotnymi celami (art. 5 ust. 1 lit. b rozporządzenia 2016/679). Jak wyjaśniono w motywie 33 preambuły rozporządzenia 2016/679, w momencie zbierania danych często nie da się w pełni zidentyfikować celu przetwarzania danych osobowych na potrzeby badań naukowych.

zamierzonego dalszego przetwarzania; kontekst, w którym dane osobowe zostały zebrane, w szczególności rozsądne przesłanki pozwalające osobom, których dane dotyczą, oczekiwać dalszego wykorzystania danych oparte na rodzaju ich powiązania z administratorem; charakter danych osobowych; konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą; oraz istnienie odpowiednich zabezpieczeń zarówno podczas pierwotnej, jak i zamierzonej operacji dalszego przetwarzania. Kryterium uzasadnionych oczekiwań osoby, której dane dotyczą, co do dalszego przetwarzania jej danych osobowych, odwołuje się do koncepcji racjonalnej osoby i oceny m.in. tego, czy z jej perspektywy nowy cel przetwarzania może być nieoczekiwany lub zaskakujący[573]. Zastosowanie tej koncepcji w przypadku przetwarzania danych osobowych dzieci wymaga zachowania szczególnej ostrożności i rozwagi. Administrator powinien wziąć pod uwagę nie tylko sam fakt przetwarzania danych osobowych dzieci, ale także – zwłaszcza jeśli zachodzi prawdopodobieństwo, że będą one korzystały z usługi bez udziału opiekunów prawnych – zastanowić się nad tym, w jakim są wieku i dopiero wówczas poddać ocenie, czy mogą spodziewać się przetwarzania ich danych w innym celu. W praktyce, zwłaszcza w przypadku młodszych dzieci, byłoby to bardzo trudne, dlatego dopuszczalność zmiany celu przetwarzania jest wątpliwa. Inne, mniej rygorystyczne podejście można przyjąć w przypadku nastolatków, np. będących tuż przed osiągnięciem pełnoletności. Są to aspekty, które trzeba rozważyć w odniesieniu do każdego przetwarzania biorąc pod uwagę jego uwarunkowania i wszystkie istotne czynniki, co ciąży na administratorze. Jeżeli jednak w wyniku ich analizy okaże się, że zamierzone cele dalszego przetwarzania są zgodne z pierwotnymi, administrator może rozpocząć przetwarzanie. Trzeci wyjątek od zakazu dotyczy sytuacji, w której osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie w innym celu niż pierwotny – co oznacza, że niezbędne jest zapytanie jej o zgodę przed rozpoczęciem przetwarzania, lub jeżeli istnieje podstawa prawna w prawie UE lub krajowym uprawniająca do takiego przetwarzania, w szczególności do realizacji ważnych celów leżących w ogólnym interesie publicznym. W przypadku zapytania o zgodę, administrator musi przestrzegać wszystkich zasad odnoszących się do tej przesłanki przetwarzania i warunków ważności oświadczeń o wyrażeniu zgody.

5. Zasada minimalizacji danych

Zgodnie z art. 5 ust. 2 lit. c rozporządzenia 2016/679, dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Zasadę minimalizacji należy rozumieć w ten sposób, że dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi

[573] P. Drobek, *Zasada celowości…*, Legalis.

sposobami[574]. Ocena spełnienia tego kryterium powinna dotyczyć dwóch aspektów – czy przetwarzanie danych osobowych jest w ogóle niezbędne, tj. czy celu nie uda się osiągnąć bez informacji identyfikujących osobę fizyczną, a w razie odpowiedzi twierdzącej – w jakim zakresie mogą być przetwarzane. Niektórzy komentatorzy interpretują kryterium niezbędności jako dopuszczalność przetwarzania wyłącznie tych danych osobowych, bez których nie da się zrealizować zamierzonego celu[575] i podnoszą, że przetwarzanie danych osobowych, które nie są niezbędne do osiągnięcia zamierzonych celów, będzie stanowiło naruszenie rozporządzenia 2016/679[576]. Słusznie jednak zauważa P. Fajgielski, że skupienie się wyłącznie na kryterium niezbędności i pominięcie pozostałych składowych zasady minimalizacji, tj. adekwatności i stosowności danych w odniesieniu do celu przetwarzania, wydaje się przesadnie zawężać możliwość przetwarzania danych osobowych, które choć nie są absolutnie niezbędne, to w znaczący sposób przyczyniają się do realizacji celów przetwarzania – dlatego wszystkie te elementy powinny być rozpatrywane łącznie[577].

6. Zasada prawidłowości

Przepis art. 5 ust. 2 lit. d rozporządzenia 2016/679 stanowi, że dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane i należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Istotą tej zasady jest więc zapewnienie merytorycznej poprawności danych osobowych, ich zgodności ze stanem faktycznym, kompletności oraz aktualności[578], bez względu na przyczynę wystąpienia ewentualnych błędów – a zatem nie tylko wtedy, gdy ich wystąpienie spowodował administrator, lecz także, gdy nieprawidłowa (czy niepełna) informacja pochodzi bezpośrednio od osoby, której dane dotyczą[579]. Przepisy rozporządzenia 2016/679 nie precyzują, co oznacza podjęcie „wszelkich rozsądnych działań". Bez wątpienia można jednak zgodzić się z poglądem, że administrator powinien pozyskiwać dane osobowe z wiarygodnego źródła[580], a w razie dowiedzenia się o błędzie lub nieprawidłowości innego rodzaju, usunąć je lub sprostować. Podobnie na aprobatę zasługuje stanowisko, że zasada prawidłowości danych nie

[574] Patrz motyw 39 preambuły rozporządzenia 2016/679.
[575] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis.
[576] A. Nerka, *Komentarz do art. 5 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.
[577] P. Fajgielski, *Ogólne rozporządzenie…*, s. 160.
[578] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016, Legalis.
[579] A. Nerka, *Komentarz do art. 5 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.
[580] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis

powoduje obowiązku systematycznego poszukiwania danych nieprawidłowych[581], tym bardziej, jeśli przy okazji nadgorliwie przeprowadzanej weryfikacji doszłoby do pozyskania przez administratora z jego własnej inicjatywy dodatkowych, „nadmiarowych" danych osobowych (a zatem z naruszeniem zasady minimalizacji).

7. Zasada ograniczenia przechowywania

Zasada ograniczenia przechowywania ściśle wiąże się z zasadą ograniczenia celu i minimalizacji danych. Ograniczenie przechowywania, zgodnie z art. 5 ust. 1 lit. e rozporządzenia 2016/679, polega na tym, że dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których są przetwarzane[582]. Jednym z przejawów przestrzegania zasad minimalizacji i ograniczenia przechowywania jest zapewnienie ograniczenia okresu przechowywania danych do ścisłego minimum, o czym mowa w motywie 39 preambuły rozporządzenia 2016/679. Wskazano w nim również, że administrator, dążąc do zadośćuczynienia zasadzie ograniczenia przechowywania, powinien ustalić termin ich usuwania lub okresowego przeglądu. Innymi słowy, zadaniem administratora jest, biorąc pod uwagę cel przetwarzania, określenie odpowiedniego czasu jego trwania opierając się na regulujących tę materię przepisach prawa, jeśli takie istnieją[583], „a w przypadkach, w których prawo nie reguluje okresu retencji danych, po przeprowadzeniu analiz, określić ten okres tak, aby przetwarzanie danych było zgodne z celami, z którymi je pozyskano"[584]. Obowiązek usunięcia danych osobowych może zaistnieć także w przypadku skorzystania przez osobę, której dane dotyczą, z niektórych uprawnień przewidzianych w rozporządzeniu 2016/679, np. wycofania zgody na przetwarzanie danych osobowych w sytuacji, gdy nie istniała inna przesłanka pozwalająca na dalsze przechowywanie[585]. Po upływie dopuszczalnego czasu przetwarzania, dane osobowe powinny być usunięte, przez co należy rozumieć całkowite pozbycie się ich ze wszystkich nośników. Tożsamy skutek z usunięciem danych osobowych – tj. zaprzestanie ich przetwarzania – ma ich zanonimizowanie[586], pod warunkiem, że nie ma możliwości ponownego powiązania informacji z osobą, której dotyczyła.

---

[581] P. Fajgielski, *Ogólne rozporządzenie…*, s. 152.

[582] Przepis art. 5 ust. 1 lit. e rozporządzenia 2016/679 w dalszej części stanowi, że dane osobowe można przechowywać przez okres dłuższy, z zachowaniem odpowiednich środków technicznych i organizacyjnych w celu ochrony praw i wolności osób, których dane dotyczą, jeśli będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

[583] Dotyczy to przeważnie podmiotów publicznych, por. decyzja Prezesa UODO z dnia 03.04.2019 r., sygn. ZSPU.421.8.2018, https://uodo.gov.pl/decyzje/ZSPU.421.8.2018 (dostęp: 07.02.2021).

[584] Decyzja Prezesa UODO z dnia 18.10.2019 r., sygn. ZSPU.421.3.2019, https://uodo.gov.pl/decyzje/ZSPU.421.3.2019 (dostęp: 07.02.2021).

[585] M. Bienias, *Zasada czasowego ograniczenia przechowywania danych osobowych na gruncie RODO*, „Prawo Mediów Elektronicznych" 2017, nr 4, Legalis.

[586] Tamże.

8. Zasada zachowania integralności i poufności

Zasada zachowania integralności i poufności oznacza, zgodnie z art. 5 ust. 1 lit. f rozporządzenia 2016/679, że dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. W motywie 39 preambuły rozporządzenia 2016/679 wskazano, że dotyczy to także ograniczenia dostępu i korzystania ze sprzętu służącego do przetwarzania danych osobowych, choć należy to potraktować jako przykład zabezpieczenia. Atrybuty integralności i poufności – a także dostępności informacji, którą z niewiadomych przyczyn unijny prawodawca pominął w art. 5 ust. 1 lit. f rozporządzenia 2016/679 – wywodzą się z norm ISO/IEC serii 27000, które mogą być pomocniczo stosowane w celu zabezpieczenia danych osobowych[587]. Wymieniona w tym przepisie „przypadkowa utrata, zniszczenie lub uszkodzenie" będzie bowiem skutkowała właśnie naruszeniem dostępności danych osobowych. Zapewnienie integralności danych polega na ich ochronie przez nieautoryzowaną zmianą lub usunięciem, zaś poufność oznacza nieudostępnianie danych nieuprawnionym osobom[588].

[587] M. Byczkowski, *Znaczenie norm ISO we wdrażaniu bezpieczeństwa technicznego i organizacyjnego wymaganego w RODO*, [w:] G. Sibiga (red.), *Wdrażanie ogólnego rozporządzenia o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2017*, Warszawa 2017. Wg normy ISO 27001 za bezpieczeństwo informacji uznaje się zachowanie poufności, integralności i dostępności informacji – L. Kępa, *Bezpieczeństwo danych…*, Warszawa 2019, Legalis.

[588] P. Drobek, *Komentarz do art. 5 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 340. O obowiązkach związanych z zapewnieniem bezpieczeństwa traktuje rozdział IV niniejszej rozprawy.

ROZDZIAŁ III
UPRAWNIENIA PRZYSŁUGUJĄCE DZIECKU W ZWIĄZKU Z PRZETWARZANIEM DANYCH OSOBOWYCH W KONTEKŚCIE ŚWIADCZENIA USŁUG SPOŁECZEŃSTWA INFORMACYJNEGO

1. Uprawnienia informacyjne

1.1 Uzyskanie informacji o przetwarzaniu danych osobowych

Przepisy o ochronie danych osobowych, które obowiązywały przed reformą, przewidywały obowiązek informowania osób, których dane dotyczą, o przetwarzaniu ich danych osobowych[589], a TSUE wskazywał na jego szczególne znaczenie – podkreślając, że wiedza o przetwarzaniu danych osobowych warunkuje możliwość korzystania przez podmiot danych z innych uprawnień pozwalających na ochronę jego praw[590]. Wzmocnienie poziomu ochrony danych osobowych, które było jednym z celów reformy, ma się urzeczywistnić m.in. dzięki posiadaniu przez osoby fizyczne kontroli nad własnymi danymi osobowymi[591]. Z tego względu w rozporządzeniu 2016/679 tzw. uprawnienia informacyjne podmiotów danych i skorelowane z nimi obowiązki administratorów zostały znacznie rozbudowane[592], a ich szczególne znaczenie akcentuje także organ nadzorczy i EROD. Zdaniem Prezesa UODO, informowanie przez administratora o przetwarzaniu danych osobowych ma fundamentalne znaczenie dla ochrony podmiotów danych, ponieważ brak świadomości w tym zakresie pozbawia je faktycznej możliwości skorzystania z uprawnień wynikających z rozporządzenia 2016/679[593]. Uprawnienia informacyjne są emanacją zasady przejrzystości, o której mowa w art. 5 ust. 1 lit. a rozporządzenia 2016/679[594] i uważa się je za „jeden z filarów ochrony danych osobowych" – ze względu na ich znaczenie z perspektywy realizacji koncepcji autonomii informacyjnej[595].

[589] Por. art. 24 i 25 uodo z 1997 r. oraz art. 10 i 11 dyrektywy 95/46.
[590] Por. wyrok TSUE z dnia 1 października 2015 r. w sprawie C-201/14, Smaranda Bara i in. przeciwko Președintele Casei Naționale de Asigurări de Sănătate i inni.
[591] Por. motyw 7 preambuły do rozporządzenia 2016/679.
[592] Nakładanie na przedsiębiorców tzw. obowiązków informacyjnych występuje także w innych dziedzinach prawa – przede wszystkim na gruncie prawa konsumenckiego, gdzie „informacja staje się głównym instrumentem przedsięwzięć o ochronnym charakterze", a „Założeniem są tu działania (także regulatywne) na rzecz zrekompensowania braków jego (konsumenta – przyp. autorki) wiedzy i orientacji, wywołanych masowością produkcji i obrotu. Nie przywilej, lecz zrównoważenie utraconych szans; powrót do idei spoczywającej u założeń swobody umów, przywrócenie warunków do oceny sytuacji rynkowej, przywrócenie równości szans traconych wraz z rozwojem nowoczesnej produkcji, handlu czy marketingu" – E. Łętowska, K. Osajda, *Wprowadzenie do części ogólnej zobowiązań* [w:] K. Osajda (red.), *Prawo zobowiązań – część ogólna. System Prawa Prywatnego tom 5*, wyd. 3, Warszawa 2020, s. 49.
[593] Por. UODO, *Prezes UODO nałożyła pierwszą karę pieniężną*, https://uodo.gov.pl/pl/138/786 (dostęp: 04.05.2021).
[594] P. Fajgielski, *Ogólne rozporządzenie…*, s. 251.
[595] T. Będźmirowski, A. Zalewska, *Modalność obowiązku informacyjnego* [w:] W. R. Wiewiórowski, H. Wolska (red.), *Rok RODO*…, Legalis.

Uprawnienie polegające na uzyskaniu informacji o przetwarzaniu danych osobowych realizowane jest na dwa sposoby. Po pierwsze, osoba, której dane dotyczą, ma prawo uzyskania od administratora informacji o przetwarzaniu, o których mowa w art. 13 i 14 rozporządzenia 2016/679 i które są przekazywane są z inicjatywy administratora[596], o ile nie zaistnieją przesłanki zwalniające go z tego obowiązku. Po drugie, w myśl art. 15 ust. 1 i 2 rozporządzenia 2016/679, podmiot danych ma prawo uzyskania informacji od administratora informacji o przetwarzaniu na swój wniosek (żądanie).

Przepis art. 13 rozporządzenia 2016/679 ma zastosowanie w przypadku zbierania przez administratora danych osobowych bezpośrednio od podmiotu danych – a zatem wtedy, gdy przykładowo dziecko podaje mu swoje dane w formularzu na stronie internetowej. W takiej sytuacji, stosownie do art. 13 ust. 1 lit. a-f rozporządzenia 2016/679, administrator ma obowiązek podać: swoją tożsamość i dane kontaktowe (oraz – gdy ma to zastosowanie – tożsamość i dane kontaktowe swojego przedstawiciela[597]); dane kontaktowe wyznaczonego przez siebie inspektora ochrony danych; cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania; jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679 – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią; informacje o odbiorcach danych osobowych lub o kategoriach odbiorców (jeżeli istnieją); informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez KE odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46 rozporządzenia 2016/679, art. 47 rozporządzenia 2016/679 lub art. 49 ust. 1 rozporządzenia 2016/679, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia. Ponadto art. 13 ust. 2 lit. a-f rozporządzenia 2016/679 nakłada obowiązek podania innych informacji, które są „niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania". Katalog informacji podlegających udostępnieniu został więc podzielony na dwa ustępy, choć wszystkie są tak samo istotne i powinny być podane osobie, której dane dotyczą[598]. Do innych niezbędnych informacji prawodawca zaliczył: okres, przez który dane osobowe będą przechowywane, a jeśli nie jest to możliwe, kryteria ustalania tego okresu; informacje o prawie do

[596] Por. M. Sakowska-Baryła, *Komentarz do art. 13 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 1.

[597] Przez przedstawiciela należy rozumieć, zgodnie z art. 4 pkt 17 rozporządzenia 2016/679, osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w UE, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający do reprezentowania go w zakresie obowiązków wynikających z rozporządzenia 2016/679.

[598] Por. Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości*…, s. 15. Ten podział wydaje się mieć znaczenie wyłącznie w kontekście art. 13 ust. 3 rozporządzenia 2016/679 i można przypuszczać, że służy uniknięciu ponownego przekazywania tych samych informacji w razie zmiany celu przetwarzania przez tego samego administratora – por. J. Łuczak, *Komentarz do art. 13 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 480.

żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych; jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a rozporządzenia 2016/679 – czyli zgody na przetwarzanie danych osobowych – informacje o prawie do jej cofnięcia w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; informacje o prawie wniesienia skargi do organu nadzorczego; informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych; informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 rozporządzenia 2016/679, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania.

Administrator podaje informacje wskazane w art. 13 ust. 1 i 2 rozporządzenia 2016/679 podczas pozyskiwania danych osobowych. Pozyskiwanie (zbieranie) danych osobowych można rozumieć jako „wejście w posiadanie danych osobowych (zapoznanie się z danymi osobowymi) z zamiarem (celem) ich dalszego przetwarzania”[599]. Ze względu na cele zasady przejrzystości i uprawnień informacyjnych, na aprobatę zasługuje stanowisko M. Sakowskiej-Baryły, której zdaniem „zasadne jest, aby informowanie odbywało się na najwcześniejszym możliwym etapie, aby osoba, której dane dotyczą, możliwie szybko mogła się zorientować w okolicznościach przetwarzania danych i przysługujących jej uprawnieniach, a gdy podawanie danych jest dobrowolne lub czynności wymagające przetwarzania danych osobowych są uzależnione wyłącznie od jej woli, mogła na możliwie wczesnym etapie zdecydować, czy w istocie akceptuje warunki przetwarzania jej danych osobowych i znając je, chce uczestniczyć w danej aktywności”[600]. Uprawnienie otrzymania informacji, o których mowa w art. 13 ust. 1 i 2 rozporządzenia 2016/679, jest jednym ze środków umożliwiających podmiotowi danych sprawowanie kontroli nad nimi, dlatego powinno nastąpić przed rozpoczęciem przetwarzania[601].

Przepisy rozporządzenia 2016/679 nie determinują sposobu przekazania informacji. Jak wyjaśnia Grupa Robocza Art. 29, administrator ma obowiązek podjąć „odpowiednie środki” w celu przekazania informacji zgodnie z zasadą przejrzystości, co oznacza, że powinien mieć na

[599] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 13 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021, Legalis, teza 2.
[600] M. Sakowska-Baryła, *Komentarz do art. 13 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 7.
[601] Por. M. M. Bârsan, *A partial overview of the data subjects' control over their personal data under the General Data Protection Regulation*, „Bulletin of the Transilvania University of Brasov. Series VII: Social Sciences. Law” 2018, nr 2, s.130.

uwadze okoliczności zbierania i przetwarzania danych osobowych, w tym doświadczenie potencjalnego użytkownika i na tej podstawie dobrać właściwe rozwiązanie[602]. W kontekście świadczenia usług społeczeństwa informacyjnego, określone w art. 13 ust. 1 i 2 rozporządzenia 2016/679 informacje o przetwarzaniu mogą być przykładowo podane w elektronicznym formularzu służącym do pozyskania danych osobowych, wyświetlane na ekranie komputera, smartfona lub innego urządzenia[603]. Zwłaszcza w środowisku cyfrowym zasadne jest stosowanie tzw. warstwowego informowania w celu uniknięcia przeładowania informacyjnego[604] – do czego powinien dążyć administrator. Warstwowe informowanie polega na podaniu podstawowych informacji o przetwarzaniu w pierwszej warstwie, z jednoczesnym wskazaniem, gdzie znajdują się bardziej szczegółowe (druga, ewentualnie kolejna warstwa), zamiast prezentowania ich w formie ciągłego tekstu[605] – przy czym istotne jest, by dostęp do wszystkich był łatwy, co można osiągnąć poprzez zamieszczenie bezpośredniego linku, kodu QR czy zastosowaniu powiadomień typu *just-in-time* – czyli komunikatów wyświetlanych w danym momencie korzystania z usługi, zawierających krótkie, adekwatne do niego wyjaśnienia na temat przetwarzania[606]. Doniosłe znaczenie ma określenie, jakie informacje powinny być podane przez administratora w tzw. pierwszej warstwie informacyjnej. W ocenie Grupy Roboczej Art. 29 powinny to być „szczegółowe informacje na temat celów przetwarzania, tożsamości administratora i opisu praw osoby, której dane dotyczą", co wywiodła z treści motywu 39 preambuły rozporządzenia 2016/679[607]. Wydaje się, że są to odpowiedniki informacji wymienionych w art. 13 ust. 1 lit. a, c oraz ust. 2 lit. b, d rozporządzenia 2016/679, choć Grupa Robocza Art. 29 pominęła wskazanie podstawy prawnej przetwarzania, zaś w kontekście praw podmiotu danych zamiast „informacji o prawach" posłużyła się frazą „opis praw". Pominięcie w pierwszej warstwie informacji o podstawie prawnej przetwarzania, lecz z zachowaniem wskazania jego celów, należy ocenić pozytywnie. Informacja o podstawie prawnej jest trudna do zrozumienia dla przeciętnego odbiorcy – zwłaszcza dziecka – jeśli jej treść sprowadza się do podania numeru przepisu i nazwy aktu prawnego. Wątpliwości może natomiast wzbudzać zalecenie zamieszczania „opisu praw". Celem tzw. warstwowego informowania jest przekazanie kluczowych informacji w zwięzłej i przystępnej formie. Zawarcie w pierwszej warstwie opisu wszystkich praw, jakie przysługują osobie fizycznej

[602] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości*…, s. 16.
[603] Por. M. Sakowska-Baryła, *Komentarz do art. 13 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 8.
[604] P. Fajgielski, *Obowiązek informacyjny z perspektywy dwóch lat stosowania nowych przepisów o ochronie danych osobowych*, „Monitor Prawniczy" dodatek: *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020*, G. Sibiga (red.), 2020, nr 23, s. 49.
[605] Por. L. Słocka, *Obowiązki informacyjne przedsiębiorcy charakterystyczne dla świadczenia usług drogą elektroniczną na rzecz konsumenta a plain language i warstwowe obowiązki informacyjne jako próba rozwiązania problemu tzw. information overkill*, „Prawo Mediów Elektronicznych" 2022, nr 4, s. 31.
[606] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości*…, s. 21-24.
[607] Tamże, s. 22.

w związku z przetwarzaniem jej danych osobowych – jeśli miałoby mu towarzyszyć podanie okoliczności, które wyłączają możliwość ich realizacji – niweczyłoby ten cel. Z tego powodu bardziej zasadne jest wymienienie praw, jakie przysługują osobie, której dane dotyczą, i opisanie, na czym one polegają, w kolejnej warstwie.

Ustawodawca zdecydował się na wprowadzenie szczególnych regulacji dotyczących sposobu realizacji obowiązku wynikającego z art. 13 rozporządzenia 2016/679 w przypadku administratora będącego mikroprzedsiębiorcą[608] i w zakresie niektórych umów zawieranych z konsumentem, w tym – co istotne w świetle tematu niniejszej rozprawy – umów zawieranych na odległość. Zgodnie z art. 4a ust. 1 ustawy z dnia 30 maja 2014 r. o prawach konsumenta[609], ten obowiązek jest realizowany „przez wywieszenie w widocznym miejscu w lokalu przedsiębiorstwa lub udostępnienie na swojej stronie internetowej stosownych informacji". Jednocześnie ustawodawca przewidział wyjątki od tego sposobu informowania – jest nią niemożność zapoznania się przez osobę, której dane dotyczą, z informacjami wskazanymi w art. 13 rozporządzenia 2016/679 (art. 4a ust. 2 upk); okoliczność, że administrator przetwarza dane osobowe, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679 (art. 4a ust. 3 pkt 1 upk), czyli dane należące do szczególnych kategorii; okoliczność, że administrator udostępnia dane osobowe, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, innym administratorom – za wyjątkiem sytuacji, gdy osoba, której dane dotyczą, wyraziła zgodę na udostępnienie swoich danych albo udostępnienie jest niezbędne do wypełnienia obowiązku ciążącego na administratorze (art. 4a ust. 3 pkt 2 upk). W praktyce oznacza to, że zamierzone uproszczenie realizacji obowiązku wynikającego z 13 rozporządzenia 2016/679 doznaje wielu ograniczeń. W literaturze podnosi się, że pierwszy spośród ww. wyjątków rodzi znaczne trudności interpretacyjne, ponieważ nie jest jasne, jak przedsiębiorca ma sprawdzić, czy osoba, której dane dotyczą, ma możliwość zapoznania się z informacją wywieszoną w lokalu przedsiębiorstwa lub udostępnioną na stronie internetowej, a także w jaki sposób ma wykazać, że swój obowiązek wypełnił prawidłowo[610]. W przypadku usługi społeczeństwa informacyjnego – biorąc pod uwagę jej konstytutywne cechy – nie ulega wątpliwości, że osoba, której dane dotyczą, nie ma możliwości zapoznania się z informacją wywieszoną w lokalu przedsiębiorstwa – co eliminuje ten sposób informowania. Analizując zatem

[608] W myśl art. 7 ust. 1 pkt 1 ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców (t.j. Dz. U. z 2023 r. poz. 221 z późn. zm.), mikroprzedsiębiorcą jest przedsiębiorca, „który w co najmniej jednym roku z dwóch ostatnich lat obrotowych spełniał łącznie następujące warunki: a) zatrudniał średniorocznie mniej niż 10 pracowników oraz b) osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych nieprzekraczający równowartości w złotych 2 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 2 milionów euro".

[609] T.j. Dz.U. z 2020 r. poz. 287 z późn. zm., dalej jako: upk.

[610] M. Topyła, *Zmiana ustawy o prawach konsumenta w związku z wejściem w życie tzw. ustawy dostosowującej RODO a obowiązek informacyjny w wykonaniu mikroprzedsiębiorcy*, „Monitor Prawniczy" dodatek: *Polskie przepisy o ochronie danych osobowych*. *Aktualne problemy prawnej ochrony danych osobowych 2019*, G. Sibiga (red.), 2019, nr 22, s. 27.

drugą z możliwości – udostępnienie na stronie internetowej – zastosowanie tego środka również wydaje się wyłączone, gdy do zawarcia umowy dochodzi np. poprzez aplikację mobilną, która nie została pobrana bezpośrednio z tej strony, lecz z tzw. sklepu z aplikacjami, prowadzonego przez inny podmiot. Możliwe jest wskazanie także innych niedoskonałości tego przepisu. Zastosowanie art. 4a upk ograniczone jest do wykonywania obowiązku informacyjnego „w zakresie umów" – powstaje zatem pytanie, czy przedsiębiorca może powołać się na ten przepis także wtedy, gdy zamierza przetwarzać dane osobowe nie tylko w celu zawarcia i wykonania umowy, ale także pozyskać zgodę na przesyłanie informacji handlowych w przyszłości. W literaturze trafnie wskazuje się na niejasność art. 4a upk i trudności w jego stosowaniu w praktyce[611], co sprawia, że uproszczenie informowania osób, których dane dotyczą, o przetwarzaniu, jest iluzoryczne. W razie braku możliwości zastosowania tego przepisu, obowiązek ten należy wypełnić zgodnie z zasadami ogólnymi, określonymi w rozporządzeniu 2016/679.

W trakcie trwania przetwarzania, jeśli administrator planuje zmienić jego cel i jest to dopuszczalne w świetle zasady ograniczenia celu, w myśl art. 13 ust. 3 rozporządzenia 2016/679 przed rozpoczęciem tego „nowego" przetwarzania[612] jest zobowiązany do poinformowania osoby, której dane dotyczą, o nowym celu. Ponadto powinien udzielić innych stosownych informacji, o których mowa w art. 13 ust. 2 rozporządzenia 2016/679 – co można odczytywać jako konieczność podania tych informacji, które są relewantne ze względu na uwarunkowania realizacji nowego celu przetwarzania – np. gdy występuje inny czas przechowywania danych osobowych, inna podstawa prawna przetwarzania, która może implikować konieczność przekazania dodatkowych informacji o prawach. Nie wydaje się jednak błędną praktyka powtórzenia wszystkich informacji – nawet jeśli zostały już wcześniej przekazane – zwłaszcza, jeśli od tego momentu upłynęło dużo czasu. Wówczas może przyczynić się to do zwiększenia przejrzystości działań administratora.

W przypadku pozyskiwania danych osobowych bezpośrednio od osoby, której dotyczą, unijny prawodawca przewidział jeden wyjątek od obowiązku realizacji tego uprawnienia. Mianowicie, zgodnie z art. 13 ust. 4 rozporządzenia 2016/679, ust. 1 i 2 nie mają zastosowania, „gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami". Wynika z niego, że osoba, której dane dotyczą, jest uprawniona do otrzymania informacji przekazywanej z inicjatywy administratora raz – podczas pozyskiwania jej danych. Uprawnienie to będzie się odnawiało w przypadku zaistnienia okoliczności, które sprawią, że dotychczas przekazane informacje są niepełne lub nieaktualne[613].

[611] T. Czech, *Prawa konsumenta. Komentarz, wyd. II*, Warszawa 2020, s. 170-176.
[612] Por. J. Łuczak, *Komentarz do art. 13 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO*..., s. 485.
[613] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości*…, s. 32.

Przepis art. 14 rozporządzenia 2016/679 dotyczy z kolei zbierania przez administratora danych osobowych nie od osoby, której dotyczą – czyli pozyskania ich z innych źródeł, np. od innych osób, z dokumentów, ogólnie dostępnych zbiorów[614] czy w wyniku uzyskania bazy danych w drodze umowy cywilnoprawnej[615]. Zakres informacji, do uzyskania których w takim przypadku uprawniona jest osoba, której dane dotyczą, w większości pokrywa się z wymienionym w art. 13 rozporządzenia 2016/679, choć istnieją pewne wyjątki. Po pierwsze, obowiązek nie obejmuje tych informacji, których podanie byłoby bezprzedmiotowe ze względu na sposób pozyskania danych – czyli informacji o tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym i jakie są ewentualne konsekwencje niepodania danych (art. 13 ust. 2 lit. e rozporządzenia 2016/679). Po drugie, pozyskanie danych z innego źródła niż osoba, której dane dotyczą, powoduje konieczność przekazania jej informacji o kategoriach odnośnych danych osobowych (art. 14 ust. 1 lit. d rozporządzenia 2016/679) – co można rozumieć jako informację o rodzaju danych, które odnoszą się do osoby, której dotyczą[616] i która jest uprawniona do uzyskania informacji o przetwarzaniu; źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych (art. 14 ust. 2 lit. f rozporządzenia 2016/679). Zdaniem J. Łuczak, nie należy traktować podania danych osobowych dziecka przez jego przedstawiciela ustawowego jak uzyskania danych z innych źródeł niż osoba, której dane dotyczą, ponieważ działa on w imieniu i na jego rzecz[617].

W przypadku pozyskania danych z innych źródeł niż osoba, której dane dotyczą, przepisy rozporządzenia 2016/679 określają trzy terminy, w których administrator ma obowiązek przekazać informacje wymienione w art. 14 rozporządzenia 2016/679. Zgodnie z art. 14 ust. 3 lit. a rozporządzenia 2016/679, administrator powinien uczynić to w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych. Administrator powinien więc dokonać oceny, kiedy najbardziej właściwe jest przekazanie informacji, choć nie może przekroczyć miesiąca licząc od momentu zebrania danych. Kolejne dwa terminy również są uzależnione od okoliczności przetwarzania. Stosownie do art. 14 ust. 3 lit. b rozporządzenia 2016/679, jeśli dane osobowe mają być wykorzystane do komunikacji z osobą, której dane dotyczą, administrator powinien przekazać

[614] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 14 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Ogólne rozporządzenie…,* teza 1.
[615] NSA orzekł, że „nabycie w drodze umowy jest więc także sposobem uzyskiwania, czy wydostawania /danych/, co prowadzi do konkluzji, iż zakup bazy danych jest tożsamy z procesem ich zbierania i pozyskiwania", a zatem powoduje powstanie obowiązku poinformowania osób, których dane dotyczą, o pozyskaniu ich danych z innych źródeł stosownie do art. 25 ust. 1 pkt 3 uodo z 1997 r. (który kreował analogiczny obowiązek do przewidzianego obecnie w art. 14 rozporządzenia 2016/679) – por. wyrok NSA z dnia 13 lipca 2004 r., sygn. akt OSK 507/04, http://orzeczenia.nsa.gov.pl/doc/0730920DD9 (dostęp: 04.05.2021).
[616] P. Fajgielski, *Ogólne rozporządzenie…*, s. 270.
[617] J. Łuczak, *Komentarz do art. 15 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), RODO…, s. 495.

informacje najpóźniej przy pierwszym kontakcie. Natomiast jeśli administrator planuje ujawnić dane osobowe innemu odbiorcy, to w myśl art. 14 ust. 3 lit. c rozporządzenia 2016/679 jest zobowiązany do przekazania informacji najpóźniej przy ich pierwszym ujawnieniu. Analogicznie jak w przypadku przetwarzania danych osobowych, które zostały pozyskane bezpośrednio od osoby, której dotyczą, w razie planowanej zmiany cel przetwarzania konieczne jest uprzednie poinformowanie o tym zamiarze (art. 14 ust. 4 rozporządzenia 2016/679). M. Mostowik zaprezentował pogląd, że art. 14 ust. 3 lit. a rozporządzenia 2016/679 ustanawia ogólny, podstawowy termin na spełnienie obowiązku informacyjnego, natomiast pozostałe należy traktować jak przepisy szczegółowe, które nakazują w określonych w nich przypadkach udzielić informacji wcześniej, niż w ciągu miesiąca od pozyskania danych. Stanowisko to zasługuje na aprobatę pod warunkiem uznania pierwszorzędności wykładni celowościowej, gdyż jak wskazuje autor odmienna interpretacja – należy odnotować, że taka również wystąpiła w literaturze przedmiotu i autor ją przywołuje – prowadziłaby do „znacznego opóźniania udzielenia informacji poprzez odsuwanie w czasie momentu komunikacji lub udostępnienia danych", co stałoby w sprzeczności z celami omawianego przepisu[618].

W przypadku pozyskiwania danych osobowych z innych źródeł niż od osoby, której dotyczą, rozporządzenie 2016/679 przewiduje cztery wyjątki od obowiązku realizacji uprawnienia wynikającego z jego art. 14 – przy czym pierwszy z nich jest identyczny jak w przypadku wyłączenia spod obowiązku realizacji uprawnienia określonego w art. 13, tzn. jeżeli osoba, której dane dotyczą, dysponuje już tymi informacjami (art. 14 ust. 5 lit. a rozporządzenia 2016/679). Trzy kolejne dotyczą sytuacji, gdy: „udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie" (art. 14 ust. 5 lit. b rozporządzenia 2016/679); pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem UE lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą (art. 14 ust. 5 lit. c rozporządzenia 2016/679); dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie UE lub w prawie

[618] M. Mostowik, *Ochrona danych osobowych w Internecie rzeczy w prawie UE*, Warszawa 2022, Legalis.

państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy (art. 14 ust. 5 lit. d rozporządzenia 2016/679). W odniesieniu do usług społeczeństwa informacyjnego wydaje się, że zastosowanie mogą mieć przede wszystkim wyłączenia, o których mowa w art. art. 14 ust. 5 lit. a i b rozporządzenia 2016/679, choć drugie z nich wzbudza kontrowersje z powodu problemów, jakie wiążą się z dokonaniem oceny, kiedy zachodzi niemożność podania informacji o przetwarzaniu ze względu na niewspółmiernie duży wysiłek.

Forma przekazania i treść informacji o przetwarzaniu danych osobowych powinna być dostosowana do możliwości poznawczych dziecka korzystającego z usług społeczeństwa informacyjnego, zgodnie z omówioną w rozdziale II zasadą przejrzystości i wskazanymi tam dobrymi praktykami w zakresie komunikacji z dzieckiem w sprawach dotyczących ochrony danych osobowych. W motywie 39 preambuły do rozporządzenia 2016/679 prawodawca położył szczególny nacisk na przekazywanie dziecku informacji w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Sugeruje to, że naruszenie zasady przejrzystości wobec dzieci będzie oceniane surowiej, niż gdyby dotyczyło innych osób, a ponadto, że administrator musi zróżnicować sposób porozumiewania się z dorosłymi i dziećmi[619]. Niewątpliwie wdrożenie komunikatów dotyczących przetwarzania danych osobowych dostosowanych do wieku, możliwości poznawczych i potrzeb dzieci jest obowiązkiem administratora świadczącego usługi społeczeństwa informacyjnego oferowane bezpośrednio dzieciom.

1.2 Uzyskanie dostępu do danych osobowych

O doniosłości prawa dostępu do swoich danych osobowych świadczy to, że gwarantuje je każdemu art. 8 ust. 2 KPP. Wiedza, jakie dane osobowe są przetwarzane, ułatwia osobie, której dane dotyczą, świadome korzystanie z innych uprawnień takich jak usunięcie lub sprostowanie danych[620]. Przepis art. 15 rozporządzenia 2016/679 reguluje zakres i sposób realizacji prawa dostępu do danych osobowych. W istocie składają się na nie trzy różne uprawnienia – uzyskanie przez podmiot danych: 1) potwierdzenia, czy administrator przetwarza jego dane osobowe; 2) dostępu do swoich danych osobowych *sensu stricto*; 3) informacji o przetwarzaniu[621]. W ramach realizacji ostatniego z nich osoba, której dane dotyczą, jest uprawniona do zaznajomienia się z informacjami wskazanymi w art. 15 ust. 1 rozporządzenia 2016/679, tzn. ma prawo poznać: 1)

[619] R. Polčák, *Komentarz do art. 12 rozporządzenia 2016/679*, [w:] C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler (red.), *The EU General Data Protection Regulation…*, s. 408.
[620] EROD, *Guidelines 01/2022 on data subject rights - Right of access*, Version 2.0. adopted on 28 March 2023, https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf (dostęp 21.06.2023), s. 3.
[621] EROD, *Guidelines 01/2022…*, s. 12.

cele przetwarzania; 2) kategorie danych osobowych; 3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych; 4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu; 5) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, prawie do wniesienia sprzeciwu wobec przetwarzania; 6) informacje o prawie wniesienia skargi do organu nadzorczego; 7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle; 8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 rozporządzenia 2016/679 oraz, jeśli takie przetwarzanie ma miejsce – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Ponadto art. 15 ust. 2 rozporządzenia 2016/679 stanowi, że w razie dokonywania operacji przetwarzania polegającej na przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo otrzymać informacje o zastosowanych zabezpieczeniach, o których mowa w art. 46 rozporządzenia 2016/679, związanych z przekazaniem. Zakres informacji, których podania może żądać podmiot danych w ramach realizacji swojego prawa dostępu, pokrywa się więc z katalogiem określonym w art. 13 i 14 rozporządzenia 2016/679. Okoliczność, że administrator spełnił swój obowiązek wynikający z tych przepisów i przekazał w przeszłości osobie, której dane dotyczą, klauzulę informacyjną zawierającą wszystkie wymagane informacje, w żaden sposób nie ogranicza możliwości wykonywania uprawnienia wynikającego z art. 15 ust. 1 i 2 rozporządzenia 2016/679[622]. Ponadto, w przeciwieństwie do art. 32 uodo z 1997 r., art. 15 rozporządzenia 2016/679 nie przewiduje ograniczeń odnoszących się do częstotliwości możliwości korzystania z prawa do uzyskania na informacji o przetwarzaniu danych osobowych[623]. Istotą uprawnienia, o którym mowa w art. 15 ust. 1 rozporządzenia 2016/679, jest umożliwienie podmiotowi danych dostępu do samych danych – jak wyjaśnia EROD, nie chodzi o wskazanie kategorii danych. Nie ma znaczenia także źródło pozyskania danych – administrator ma obowiązek umożliwić dostęp także do danych, które zostały podane bezpośrednio przez osobę, której dotyczą, ponieważ celem realizacji omawianego uprawnienia jest pozyskanie aktualnej wiedzy o tym, jakie dane faktycznie przetwarzania administrator[624]. Najpełniej urzeczywistniłoby

[622] Por. J. Łuczak, *Komentarz do art. 15 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 513.
[623] Por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 15 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Ogólne rozporządzenie…,* teza 3. Mimo, że art. 15 rozporządzenia 2016/679 nie przewiduje takich ograniczeń, administrator może w określonych przypadkach odmówić podjęcia działań w związku z żądaniem – por. art. 12 ust. 5 rozporządzenia 2016/679.
[624] EROD, *Guidelines 01/2022*…, s. 12.

się to dzięki zapewnieniu wglądu w dane, umożliwienie kontaktu z nośnikiem, na którym zostały utrwalone, co jednak nie zawsze jest możliwe[625]. W motywie 63 prawodawca podkreślił, że „w miarę możliwości administrator powinien mieć możliwość udzielania zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych". Byłoby to odpowiednim rozwiązaniem w przypadku przetwarzania danych osobowych w sposób zautomatyzowany lub częściowo zautomatyzowany.

Prawo dostępu do danych osobowych uzupełnia ponadto uprawnienie do uzyskania ich kopii, które w przeciwieństwie do wyżej wymienionych doznaje pewnych ograniczeń[626]. W myśl art. 15 ust. 3 rozporządzenia 2016/679, administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Celem tego uprawnienia jest zagwarantowanie osobie, której dane dotyczą, sposobności weryfikacji zgodności przetwarzania z prawem (por. motyw 63 preambuły do rozporządzenia 2016/679). Realizacja prawa do uzyskania kopii danych osobowych może polegać na przekazaniu osobie, której dane dotyczą, treści danych lub – jeśli są one utrwalone w dokumentach – kopii tych dokumentów. Zdaniem Prezesa UODO, „w przypadku zwrócenia się do administratora o kopię przetwarzanych danych osobowych, administrator każdorazowo podejmuje decyzję, w jaki sposób zrealizuje to uprawnienie. Administrator może dokonać wyboru, czy udostępnia kopię dokumentów, czy też udostępnia kopię danych zawartych w tych dokumentach"[627]. Podmiot danych nie może więc zakwestionować formy, w jakiej administrator przekazał mu kopię danych, o ile został zrealizowany obowiązek podania treści przetwarzanych danych. Taka interpretacja zasługuje na aprobatę, ponieważ podanie treści danych osobowych stanowi realizację celu wprowadzenia przez prawodawcę tego prawa, tzn. umożliwienia osobie, której dane dotyczą, dowiedzenia się, jakie dane na jej temat są przetwarzane, a w razie stwierdzenia, że są np. nieaktualne, błędne czy przetwarzane z naruszeniem zasad określonych w art. 5 rozporządzenia 2016/679, możliwości skorzystania z innych przysługujących jej praw. Nie oznacza to jednak, że właściwe byłoby zlekceważenie okoliczności i sposobu przetwarzania danych osobowych oraz obowiązku ułatwiania podmiotowi danych wykonywanie jego uprawnień. W kontekście mediów społecznościowych jako przykład sposobu realizacji prawa uzyskania kopii danych osobowych EROD podaje umożliwienie użytkownikowi pobrania zawierającego je pliku z poziomu konta użytkownika[628]. Reasumując, sposób wydania kopii danych osobowych powinien być uzależniony od uwarunkowań

[625] Por. M. Sakowska-Baryła, *Komentarz do art. 15 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 10.
[626] Zgodnie z art. 15 ust. 3 i 4 rozporządzenia 2016/679, administrator może pobrać opłatę za wydanie drugiej i kolejnych kopii danych, a prawo uzyskania kopii nie może wpływać niekorzystnie wpływać na prawa i wolności innych.
[627] Decyzja Prezesa UODO z dnia 22.03.2019 r., sygn. ZSZZS.440.660.2018, https://uodo.gov.pl/decyzje/ZSZZS.440.660.2018 (dostęp: 04.05.2021).
[628] EROD, *Guidelines 01/2022*…, s. 44.

przetwarzania, poprzedzony upewnieniem się, że wnioskodawca jest osobą uprawnioną do jej otrzymania, a także że przy określaniu formy przekazania danych zostały spełnione wymogi związane z bezpieczeństwem danych zgodnie z art. 32 rozporządzenia 2016/679[629].

2. Uprawnienia korekcyjne

2.1 Sprostowanie danych osobowych

W myśl art. 16 rozporządzenia 2016/679, „Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe". Za nieprawidłowe można uznać dane, które są niezgodne ze stanem faktycznym – np. są nieaktualne lub zawierają błędy[630]. Sprostowanie danych osobowych jest uprawnieniem skorelowanym z ciążącym na administratorze obowiązkiem przestrzegania zasady prawidłowości danych (art. 5 ust. 1 lit. d rozporządzenia 2016/679). Przetwarzanie nieprawidłowych danych osobowych może nieść negatywne konsekwencje zarówno dla podmiotu danych, jak i administratora – bez względu na to, z jakiego powodu zaistniała niezgodność danych ze stanem faktycznym – a nawet prowadzić do naruszenia ochrony danych osobowych w rozumieniu art. 4 pkt 12 rozporządzenia 2016/679[631].

Przepis art. 16 rozporządzenia 2016/679 nie przewiduje żadnych ograniczeń związanych z realizacją określonego w nim uprawnienia sprostowania danych osobowych. Sprostowanie następuje zatem bez konieczności dodatkowego umotywowania przez osobę, której dane dotyczą, swojego żądania. Powinna ona jednak wykazać, że nieprawidłowość zaistniała[632]. W zależności od celów i sposobów przetwarzania, sprostowanie danych osobowych może nastąpić w wyniku złożenia przez osobę, której dane dotyczą, oświadczenia lub przedłożenia administratorowi dokumentu, potwierdzającego zmianę danych lub dowodzącego, jakie dane są prawidłowe. W przypadku usług społeczeństwa informacyjnego, oprócz pierwszego z wymienionych sposobów – oświadczenia, które przykładowo może być przesłane pocztą elektroniczną – dobrą praktyką jest umożliwienie osobie, której dane dotyczą, samodzielnej zmiany swoich danych przetwarzanych

[629] Tamże, s. 19.
[630] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 288.
[631] Prezes UODO nałożył administracyjną karę pieniężną w wysokości 85 588 zł na administratora będącego przedsiębiorcą prowadzącym działalność ubezpieczeniową, za przesłanie danych osobowych klienta na nieprawidłowy adres poczty elektronicznej, co skutkowało naruszeniem poufności danych. Błędny adres poczty elektronicznej został podany przez samego klienta. Prezes UODO stwierdził, że „administrator danych dopuszczający możliwość wykorzystania do komunikacji z klientem pocztę elektroniczną powinien mieć świadomość ryzyk związanych np. z nieprawidłowym podaniem przez klienta adresu poczty elektronicznej i w celu ich minimalizacji przedsięwziąć odpowiednie środki organizacyjne i techniczne, jak np. weryfikacja podanego adresu, czy też szyfrowanie przesyłanych w ten sposób dokumentów" – decyzja Prezesa UODO z dnia 9 grudnia 2020 r., DKN.5131.5.2020, https://uodo.gov.pl/decyzje/DKN.5131.5.2020 (dostęp: 04.05.2021).
[632] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 289.

przez administratora, poprzez udostępnienie funkcji edycji pól zawierających dane osobowe, w ramach tzw. konta użytkownika. Te funkcje powinny być zaprojektowane w taki sposób, by zmiana danych osobowych była łatwa i intuicyjna, zwłaszcza wtedy, gdy ma korzystać z nich dziecko. Sprostowanie danych osobowych może więc nastąpić poprzez wpisanie nowych lub prawidłowych danych osobowych przez dziecko korzystające z usługi lub przez przedstawiciela ustawowego, jeśli przewidziano dla niego taką możliwość.

Przepis art. 16 rozporządzenia 2016/679 przewiduje również prawo żądania uzupełnienia niekompletnych danych osobowych, co może nastąpić poprzez złożenie oświadczenia. Uzupełnienie niekompletnych danych osobowych powinno mieć miejsce z uwzględnieniem celów przetwarzania, tzn. nie powinno być od niego oderwane i prowadzić do naruszenia zasady minimalizacji danych osobowych.

2.2 Usunięcie danych osobowych

Przez usunięcie danych osobowych można rozumieć działanie skutkujące „zupełnym wykreśleniem (skasowaniem) informacji z zasobów administratora”[633], a zatem zaprzestaniem ich przetwarzania. Usuwanie danych osobowych może polegać na niszczeniu nośników, na których są utrwalone lub na takiej zmianie danych, że identyfikacja osoby, której dane dotyczą, nie jest możliwe[634]. W celu zadośćuczynienia wyrażonej w art. 5 ust.1 lit. e rozporządzenia 2016/679 zasadzie ograniczenia przechowywania, administrator powinien usunąć dane osobowe po upływie dopuszczalnego czasu ich przetwarzania. W określonych przypadkach będzie na nim ciążył obowiązek usunięcia danych na żądanie osoby, której dane dotyczą. Przepis art. 17 rozporządzenia 2016/679 określa przesłanki spełnienia żądania usunięcia danych osobowych („prawa do bycia zapomnianym” – taka nazwa również pojawia się w tytule przepisu), działania, jakie powinien podjąć administrator w związku z realizacją tego prawa, a także okoliczności, które wyłączają dopuszczalność usunięcia danych osobowych.

Zgodnie z art. 17 ust. 1 rozporządzenia 2016/679, administrator ma obowiązek usunąć dane osobowe dotyczące osoby, która tego żąda, jeśli: 1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane; 2) osoba, której dane dotyczą, cofnęła zgodę na przetwarzanie danych osobowych i nie ma innej podstawy prawnej przetwarzania; 3) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania, o którym mowa w art. 21 ust. 1 rozporządzenia 2016/679 i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania; 4) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania na mocy art.

[633] M. Jagielski, *Prawo do ochrony…*, s. 137.
[634] Por. M. Krzysztofek, *„Prawo do bycia zapomnianym” i inne aspekty prywatności w epoce Internetu w prawie UE,* „Europejski Przegląd Sądowy” 2012, nr 8, s. 31.

21 ust. 2 rozporządzenia 2016/679 (tzn. gdy sprzeciw dotyczy przetwarzania danych osobowych na potrzeby marketingu bezpośredniego); 5) dane osobowe były przetwarzane niezgodnie z prawem[635]; 6) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie UE lub prawie państwa członkowskiego, któremu podlega administrator; 7) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 rozporządzenia 2016/679 – tzn. w przypadku przetwarzania danych osobowych na podstawie zgody i w ramach usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

W motywie 65 preambuły do rozporządzenia 2016/679 prawodawca zaakcentował, że prawo do usunięcia danych „ma znaczenie w przypadkach, gdy osoba, której dane dotyczą, wyraziła zgodę jako dziecko, gdy nie była w pełni świadoma ryzyka związanego z przetwarzaniem, a w późniejszym czasie chce usunąć takie dane osobowe, w szczególności z internetu". Dzieci, zwłaszcza nastolatkowie, chętnie dzielą się informacjami z życia swojego oraz znajomych, nad którym jednak tracą kontrolę, co może obrócić się przeciwko nim i przykładowo stać się powodem przykrego ośmieszenia[636]. Z tych względów w katalogu przesłanek powodujących po stronie administratora powstanie obowiązku usunięcia danych osobowych na wniosek podmiotu danych znalazła się okoliczność zebrania danych osobowych w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 rozporządzenia 2016/679. Ponadto warte poparcia jest dodatkowe wyjaśnienie zawarte w motywie 65 preambuły do rozporządzenia 2016/679, iż „osoba, której dane dotyczą, powinna móc wykonywać to prawo, mimo że już nie jest dzieckiem".

W doktrynie rozważano, jak rozumieć zawarcie w art. 17 ust. 1 lit. f rozporządzenia 2016/679 odesłania do art. 8 ust. 1 rozporządzenia 2016/679 – czy intencją prawodawcy było objęcie prawem do usunięcia danych wszystkich przypadków zebrania danych w związku ze świadczeniem usług społeczeństwa informacyjnego czy tylko tych, w których przetwarzane są dane dzieci w kontekście oferowanych im bezpośrednio usług społeczeństwa informacyjnego. Uznano, że właściwe jest stanowisko drugie[637]. Nie wydaje się jednak, by istotnie ograniczało to

[635] Przez niezgodność z prawem należy rozumieć nie tylko niezgodność z rozporządzeniem 2016/679, ale również innymi unijnymi lub krajowymi aktami prawnymi, które mają zastosowanie do określonego przetwarzania danych osobowych – por. EROD, *Wytyczne 5/2019 w sprawie kryteriów dotyczących prawa do bycia zapomnianym w sprawach dotyczących wyszukiwarek internetowych na podstawie RODO*, przyjęte 07.07.2020 r. (wersja 2.0), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_pl (dostęp: 04.05.2021), s. 12.

[636] Por. K. Eichhorn, *Why an internet that never forgets is especially bad for young people*, „MIT Technology Review" 27.12.2019, https://www.technologyreview.com/2019/12/27/131123/internet-that-never-forgets-bad-for-young-people-online-permanence/ (dostęp 04.05.2021).

[637] Por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 17 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Ogólne rozporządzenie…*, Legalis, teza 12; podobnie M. Jabłoński, J. Węgrzyn, *Prawo do bycia zapomnianym*, Wrocław 2021, s. 178.

uprawnienia podmiotów danych - dzieci, ponieważ wciąż mogą – o ile podstawą prawną przetwarzania danych jest zgoda – żądać usunięcia danych na podstawie art. 17 ust. 1 lit. b rozporządzenia 2016/679.

W myśl art. 17 ust. 2 rozporządzenia 2016/679 administrator, który realizuje prawo do usunięcia danych osobowych obejmujące dane, które upublicznił, „biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje". Celem wprowadzenia tego przepisu jest wzmocnienie „prawa do bycia zapomnianym" w internecie[638], a zatem także w przypadku korzystania z usług społeczeństwa informacyjnego. W literaturze wskazuje się, że prawo do usunięcia danych osobowych składa się z dwóch uprawnień cząstkowych – żądania usunięcia danych osobowych oraz żądania, by administrator poinformował innych administratorów o woli osoby, której dane dotyczą, by informacje na jej temat zostały usunięte[639]. Wątpliwość może budzić to, jakie działania można uznać za „rozsądne". Wprowadzenie tego sformułowania, a także uzupełnienie pierwotnego projektu rozporządzenia 2016/679 o zastrzeżenie, że administrator uwzględnia „dostępną technologię i koszt realizacji", miało na celu ograniczenie i zracjonalizowanie obciążeń związanych z wypełnianiem omawianego obowiązku[640]. Genezy przepisu art. 17 ust. 2 rozporządzenia 2016/679 – lecz nie samego prawa do usunięcia danych osobowych, które istniało przed reformą[641] – można upatrywać w wyroku TSUE z dnia 13 maja 2014 r. w sprawie C-131/12[642], dzięki któremu zostało ono na gruncie rozporządzenia 2016/679 rozbudowane[643].

W powołanym wyżej orzeczeniu Trybunał pochylił się nad problemem indeksowania[644] przez wyszukiwarki internetowe treści stanowiących dane osobowe. Po wpisaniu w okno wyszukiwarki imienia i nazwiska możliwe jest w ciągu ułamków sekundy znalezienie informacji (np. zdjęć, artykułów, filmów) o tej osobie, pochodzących z różnych źródeł i nierzadko nieaktualnych – pochodzących np. sprzed kilku lat. Jak podkreślił Trybunał, umożliwia to „wszystkim internautom

---

638 Por. motyw 66 preambuły do rozporządzenia 2016/679.

639 P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 17 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Ogólne rozporządzenie…*, Legalis, teza 6.

640 W. Gregory Voss, *The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation*, „Journal of Internet Law" 2014, vol. 18, nr 1, s. 5-6.

641 Por. art. 32 ust. 1 pkt 6 uodo z 1997 r. oraz art. 12 lit. b, c dyrektywy 95/46.

642 Wyrok TSUE z dnia 13.05.2014 r. w sprawie C-131/12, Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), M. Costesze Gonzálezowi.

643 S. Żyrek, *Prawo do bycia usuniętym z listy wyników wyszukiwarki internetowej – wprowadzenie i wyrok Trybunału Sprawiedliwości z 13.05.2014 r., C-131/12, Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi,* „Europejski Przegląd Sądowy" 2019, nr 6, s. 50.

644 Na gruncie omawianego orzeczenia, przez indeksowanie można rozumieć wyświetlanie stron internetowych w określonym porządku (por. M. Wróbel, *Prawo do „bycia zapomnianym" – glosa – C-131/12*, „Monitor Prawniczy" 2017, nr 2, s. 108), będące wynikiem zautomatyzowanego przetwarzania.

otrzymanie mającego postać listy wyników wyszukiwania ustrukturyzowanego przeglądu dotyczących tej osoby informacji, jakie można znaleźć w Internecie, dotyczących potencjalnie całego szeregu aspektów jej życia prywatnego (…)" i z tego względu może oddziaływać na prawa podstawowe określone w KPP – prawo do ochrony danych osobowych i prawo do prywatności. Trybunał orzekł zatem, że operator wyszukiwarki powinien być zobowiązany do usunięcia z listy wyników wyszukiwania linków do stron internetowych, publikowanych przez podmioty trzecie[645], wyświetlonych dzięki posłużeniu się imieniem i nazwiskiem osoby żądającej usunięcia danych osobowych jako kryterium wyszukiwania. Operator wyszukiwarki, w zakresie operacji przetwarzania polegających na indeksowaniu, jest bowiem administratorem danych osobowych. Ta sprawa jest przykładem ilustrującym znaczenie prawa do usunięcia danych osobowych dla użytkowników usług społeczeństwa informacyjnego, którego zastosowanie nie jest rzecz jasna ograniczone do działalności wyszukiwarek internetowych.

Nie można pominąć, że prawo do usunięcia danych jest krytykowane ze względu liczne ograniczenia, które wykluczają jego zrealizowanie[646]. W myśl art. 17 ust. 3 rozporządzenia 2016/679, do okoliczności wyłączających jego realizację prawodawca zaliczył niezbędność przetwarzania: 1) do korzystania z prawa do wolności wypowiedzi i informacji; 2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa UE lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (czyli gdy przetwarzanie opiera się na art. 6 ust. 1 lit. c lub e rozporządzenia 2016/679 w związku z właściwymi przepisami); 3) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h oraz i, art. 9 ust. 3 rozporządzenia 2016/679; 4) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 rozporządzenia 2016/679; 5) do ustalenia, dochodzenia lub obrony roszczeń. Jak wynika z powyższego katalogu, zastosowanie prawa do usunięcia danych osobowych jest istotnie ograniczone względem podmiotów publicznych, działających na

[645] Nawet jeśli link prowadzi do legalnie publikowanych treści – Trybunał stwierdził, że prawa określone w art. 7 i 8 KPP „są co do zasady nadrzędne nie tylko wobec interesu gospodarczego operatora wyszukiwarki internetowej, lecz również wobec interesu, jaki ten krąg odbiorców może mieć w znalezieniu rzeczonej informacji w ramach wyszukiwania prowadzonego w przedmiocie imienia i nazwiska tej osoby. Taka sytuacja nie ma jednak miejsca, jeśli ze szczególnych powodów, takich jak rola odgrywana przez tę osobę w życiu publicznym, należałoby uznać, że ingerencja w prawa podstawowe tej osoby jest uzasadniona nadrzędnym interesem tego kręgu odbiorców polegającym na posiadaniu, dzięki temu zawarciu na liście, dostępu do danej informacji". Orzeczenie wywołało dyskusję na temat relacji prawa do ochrony danych osobowych i prawa do informacji – głos na ten temat zabierał w swoim orzecznictwie także ETPCZ, który z kolei akcentował znaczenie prawa do pozyskania informacji, leżącego w interesie publicznym – por. W. Wątor, *Prawo do bycia zapomnianym a swoboda wypowiedzi – glosa do wyroku Europejskiego Trybunału Praw Człowieka z 28.06.2018 r., 60798/10 i 65599/10, M.L. i W.W. przeciwko Niemcom,* „Europejski Przegląd Sądowy" 2019, nr 5, s. 46-50.

[646] Por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 17 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Ogólne rozporządzenie…*, Legalis, teza 27.

podstawie i w granicach przepisów prawa, lub podmiotów prywatnych, jeśli przetwarzanie danych osobowych odbywa się w celu wypełnienia obowiązków nałożonych na nie na mocy prawa (art. 6 ust. 1 lit. c rozporządzenia 2016/679). Natomiast w przypadku świadczenia usług społeczeństwa informacyjnego, gdzie dominującymi przesłankami legalizującymi przetwarzanie są zgoda (art. 6 ust. 1 lit. a rozporządzenia 2016/679), niezbędność przetwarzania do zawarcia i wykonania umowy (art. 6 ust. 1 lit. b rozporządzenia 2016/679) oraz prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f rozporządzenia 2016/679), prawo żądania usunięcia danych osobowych doznaje najmniej ograniczeń. Jednak nawet w przypadku usług społeczeństwa informacyjnego usunięcie danych osobowych może nastręczać praktycznych trudności. Jak zauważa M. Matysiak, „w przypadku niektórych typów gier (np. gier o mocnym aspekcie wieloosobowym) trudne może być zapewnienie graczom prawa do usunięcia ich danych. Takie roszczenie ze strony gracza w niektórych grach wieloosobowych może realnie wpłynąć na sytuację innych użytkowników tej gry”[647]. Iluzoryczność prawa do usunięcia danych osobowych może wynikać także z faktycznych, technicznych ograniczeń w jego pełnym zrealizowaniu. Nawet w przypadku, którego dotyczył wyrok TSUE w sprawie C-131/12, nie zawsze dochodzi w istocie do usunięcia danych osobowych – jak wyjaśnia EROD, żądanie usunięcia danych „z listy wyników wyszukiwania nie skutkuje całkowitym usunięciem danych osobowych. Dane osobowe istotnie nie zostaną usunięte ani ze źródłowej strony internetowej ani z indeksu i pamięci podręcznej dostawcy wyszukiwarki internetowej. Osoba, której dane dotyczą, może na przykład dążyć do usunięcia danych osobowych z indeksu wyszukiwarki internetowej, które mają swoje źródło w mediach, takich jak artykuł prasowy. W takim przypadku link do danych osobowych może zostać usunięty z indeksu wyszukiwarki internetowej. Artykuł, o którym mowa, pozostanie jednak w zakresie kontroli mediów i może być nadal publicznie dostępny, nawet jeżeli nie będzie widoczny w wynikach wyszukiwania na podstawie zapytań zawierających co do zasady imię i nazwisko osoby, której dane dotyczą”[648]. Użytkownicy usług społeczeństwa informacyjnego powinni być świadomi, że mimo zrealizowania przez administratora żądania usunięcia danych i poinformowania o żądaniu innych administratorów, odzyskanie pełnej kontroli nad danymi upublicznionymi w internecie jest zazwyczaj niemożliwe.

2.3 Ograniczenie przetwarzania

Osoba, której dane dotyczą, na podstawie art. 18 ust. 1 rozporządzenia 2016/679 jest uprawniona do żądania od administratora ograniczenia przetwarzania danych osobowych.

[647] M. Matysiak, *Ochrona prywatności użytkowników gier wideo – zarys problematyki prawnej*, [w:] „Monitor Prawniczy” dodatek: *Prawo nowych technologii - dane osobowe i prywatność, cyberbezpieczeństwo, handel elektroniczny, innowacje, internet i media, prawo IT*, X. Konarski (red.), 2020, nr 20, s. 30.
[648] EROD, *Wytyczne 5/2019*…, s. 6.

Ograniczenie przetwarzania zostało zdefiniowane przez prawodawcę w art. 4 pkt 3 rozporządzenia 2016/679, lecz przez usterki tej definicji, naświetlone w rozdziale I niniejszej rozprawy, może budzić wątpliwości interpretacyjne. Należy w tym miejscu wskazać, że ograniczenie przetwarzania polega na poprzestaniu wyłącznie na przechowywaniu danych osobowych – niedokonywaniu żadnych innych operacji[649], chyba że zgodnie z art. 18 ust. 2 rozporządzenia 2016/679 wystąpi jedna z przesłanek: 1) zgoda podmiotu danych; 2) przetwarzanie w celu ustalenia, dochodzenia lub obrony roszczeń; 3) przetwarzanie w celu ochrony praw innej osoby fizycznej lub prawnej; 4) przetwarzanie z uwagi na ważne względy interesu publicznego UE lub państwa członkowskiego.

W art. 18 ust. 1 lit. a-d rozporządzenia 2016/679 wymieniono enumeratywnie przesłanki określające sytuacje, w których podmiot danych może żądać zrealizowania jego uprawnienia w przedmiocie ograniczenia przetwarzania – jest to przewidziane odpowiednio w przypadku: 1) kwestionowania prawidłowości danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych; 2) niezgodności przetwarzania z prawem, podczas gdy osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania; 3) gdy administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń; 4) wniesienia sprzeciwu na mocy art. 21 ust. 1 rozporządzenia 2016/679 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą. Warunkiem żądania ograniczenia przetwarzania w związku z ostatnią ze wskazanych okoliczności jest wcześniejsze złożenie sprzeciwu wobec przetwarzania[650], a przynajmniej równoczesne. Pozostałe również są funkcjonalnie powiązane z innymi uprawnieniami przysługującymi osobie, której dane dotyczą – dla przykładu, między żądaniem ograniczenia przetwarzania w przypadku kwestionowania prawidłowości danych a uprawnieniem do sprostowania danych osobowych (art. 16 rozporządzenia 2016/679) może występować współzależność[651]. Uprawnienie polegające na ograniczeniu przetwarzania i jego wiodący cel trafnie scharakteryzował M. Rojszczak wskazując, że „jest środkiem przejściowym pomiędzy przetwarzaniem danych na zasadach ogólnych a ich usunięciem – i może być stosowane w szczególności w trakcie rozpatrywania zgłoszonego żądania sprostowania danych lub sprzeciwu co do ich dalszego przetwarzania”[652].

---

[649] A. Nerka, *Komentarz do art. 18 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 6.
[650] M. Czerniawski, *Komentarz do art. 18 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 535.
[651] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 308.
[652] M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019, s. 216.

Zgodnie z art. 19 rozporządzenia 2016/679 na administratorze, który ograniczył przetwarzanie danych osobowych zgodnie z art. 18 rozporządzenia 2016/679, ciąży obowiązek poinformowania o tym odbiorcy, któremu ujawniono dane. Wyjątkiem od tej powinności jest niemożliwość jej wypełnienia lub sytuacja, w której wymaga to niewspółmiernie dużego wysiłku. Ponadto przepis ten przewiduje obowiązek poinformowania podmiotu danych, na jego żądanie, o powyższych odbiorach. W przypadku zamiaru reaktywowania przetwarzania po jego ograniczeniu, administrator również musi wypełnić obowiązek informacyjny – tym razem z własnej inicjatywy. Przepis art. 18 ust. 3 rozporządzenia 2016/679 nakłada bowiem na administratora obowiązek poinformowania osoby, która zażądała ograniczenia przetwarzania dotyczących jej danych osobowych, o zamiarze uchylenia ograniczenia. Konieczność spełnienia tego obowiązku przed wznowieniem operacji przetwarzania, które wykraczają poza przechowywanie, nie budzi wątpliwości z racji posłużenia się przez prawodawcę frazą, że administrator informuje o tym „przed uchyleniem ograniczenia przetwarzania".

Z perspektywy ochrony praw dzieci-użytkowników usług społeczeństwa informacyjnego potencjalnie każda przesłanka wymieniona w art. 18 ust. 1 lit. a-d rozporządzenia 2016/679 może znaleźć zastosowanie, a wykonanie przewidzianego w tym przepisie uprawnienia do ograniczenia przetwarzania przyczynić się do urzeczywistnienia kontroli podmiotu danych nad przetwarzaniem danych osobowych[653]. Ze względu na specyfikę wyżej wymienionych usług i zagrożenia związane ze stosowaniem innowacyjnych technik przetwarzania, nierzadko opierających się na wielu danych, pierwszoplanowego znaczenia może nabrać przesłanka z art. 18 ust. 1 lit. d rozporządzenia 2016/679, umożliwiająca ograniczenie przetwarzania w związku z wniesieniem sprzeciwu wobec przetwarzania, który pozwala oponować przeciw przetwarzaniu na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679, w tym profilowaniu. Oznacza to, że administrator powinien powstrzymać się od profilowania do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą. Zwłaszcza w kontekście usług społeczeństwa informacyjnego jest to istotny, swoisty tymczasowy środek zabezpieczający, ponieważ profilowanie jest często dokonywaną i nierzadko problematyczną z perspektywy praw podmiotów danych operacją przetwarzania.

[653] Por. A. Nerka, *Komentarz do art. 18 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 1.

3. Uprawnienia szczególne

3.1 Przenoszenie danych osobowych

Prawo do przenoszenia danych osobowych stanowi *novum* na gruncie przepisów o ochronie danych osobowych. Zgodnie z art. 20 ust. 1 rozporządzenia 2016/679 polega ono na tym, że osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego[654] dotyczące jej dane osobowe, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Ponadto, jak stanowi art. 20 ust. 3 rozporządzenia 2016/679, osobie, której dane dotyczą, przysługuje prawo żądania przesłania danych osobowych przez administratora bezpośrednio innemu administratorowi, jeśli jest to technicznie możliwe.

Wprowadzenie prawa do przenoszenia danych osobowych stanowi element szerszej koncepcji, wykraczającej poza zagadnienie ochrony danych osobowych[655]. KE wyjaśniła bowiem znaczenie prawa do przenoszenia danych osobowych w dokumencie proklamującym strategię utworzenia jednolitego rynku cyfrowego wskazując, że ma ono za zadanie m.in. ułatwić konsumentom zmianę dostawcy, z którego usług korzystają, w ten sposób doprowadzając do zwiększenia konkurencyjności na rynku usług cyfrowych[656]. Wracając na grunt rozporządzenia 2016/679, w motywie 67 preambuły prawodawca uzasadnił wprowadzenie prawa do przenoszenia danych osobowych potrzebą zapewnienia osobom, których dane dotyczą, większej kontroli w związku ze stosowaniem zautomatyzowanego przetwarzania. Prawo do przenoszenia danych ma za zadanie zapewniać osobie, której dane dotyczą, sposobność do „wykorzystania efektów swojej własnej działalności w większej liczbie serwisów internetowych"[657], a zatem także usług społeczeństwa informacyjnego. Z uwagi na powyższe intencje, prawo do przenoszenia danych osobowych ma zastosowanie w ściśle określonych przypadkach.

---

[654] Chodzi o przygotowanie danych w takiej formie, by nadawały się do przekazania innemu administratorowi i dalszego przetwarzania w sposób zautomatyzowany. Szerzej na ten temat por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 317. Do powszechnie znanych formatów nadających się do odczytu maszynowego zalicza się np. *Comma Separated Values* (CSV), *JavaScript Object Notation* (JSON), *Extensible Markup Language* (XML) – por. J. Wong, T. Henderson, *The right to data portability in practice: exploring the implications of the technologically neutral GDPR*, „International Data Privacy Law" 2019, nr 3, s. 176.

[655] Spotkało się to z krytyką ze strony niektórych państw członkowskich UE, które na etapie prac legislacyjnych nad rozporządzeniem 2016/679 podnosiły, że prawo do przenoszenia danych powinno być wprowadzone w regulacjach w dziedzinie ochrony konkurencji i konsumentów – por. I. Graef, M. Husovec, N. Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Laws*, „German Law Journal" 2018, nr 6, s. 1364.

[656] Komunikat z dnia 5 maja 2015 r. Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Strategia jednolitego rynku cyfrowego dla Europy, COM(2015) 192 final, www.eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52015DC0192&from=EN, (dostęp 22.02.2020); por. także Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia…*, s. 4.

[657] W. R. Wiewiórowski, *Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy" 2017, nr 5, s. 24.

Prawo do przenoszenia danych osobowych przysługuje podmiotowi danych, gdy przetwarzanie opiera się na podstawie jego zgody lub na umowie, a także jest dokonywane w sposób zautomatyzowany (por. art. 20 ust. 1 lit. a, b rozporządzenia 2016/679). Niezbędne jest zatem kumulatywne spełnienie przesłanek odnoszących się do podstawy prawnej przetwarzania oraz sposobu przetwarzania. Przetwarzanie przez administratora danych osobowych na innej przesłance niż zgoda lub umowa, np. w ramach prawnie uzasadnionego interesu w myśl art. 6 ust. 1 lit. f rozporządzenia 2016/679, wyłącza możliwość spełnienia ewentualnego żądania przeniesienia danych[658].

W art. 20 ust. 1 lit. a rozporządzenia 2016/679 w zakresie, w jakim mowa w nim o zgodzie na przetwarzanie danych osobowych, prawodawca wskazał wprost, że chodzi o przetwarzanie w myśl art. 6 ust. 1 lit. a rozporządzenia 2016/679 lub art. 9 ust. 2 lit. a rozporządzenia 2016/679. Jednocześnie przepis art. 20 rozporządzenia 2016/679 milczy na temat przetwarzania danych osobowych dzieci. Warto zatem postawić pytanie czy prawo do przenoszenia danych osobowych znajduje zastosowanie w sytuacji, gdy stosownie do art. 8 ust. 1 rozporządzenia 2016/679 przetwarzane są dane osobowe dzieci w związku ze świadczeniem oferowanych im bezpośrednio usług społeczeństwa informacyjnego? Odpowiedź powinna być twierdząca, gdyż art. 8 ust. 1 rozporządzenia 2016/679 nie należy traktować jako odrębnej, samoistnej przesłanki legalizującej przetwarzanie – prawodawca wprost nawiązuje w nim do przetwarzania na podstawie zgody, tzn. gdy zastosowanie ma art. 6 ust. 1 lit. a rozporządzenia 2016/679, który został wymieniony w art. 20 ust. 1 lit. a rozporządzenia 2016/679. Przepis art. 8 ust. 1 rozporządzenia 2016/679 należy postrzegać jako doprecyzowujący zasady stosowania art. 6 ust. 1 lit. a rozporządzenia 2016/679 w szczególnym przypadku przetwarzania danych osobowych dzieci, za czym przemawia także bezpośrednie umiejscowienie go po przepisie określającym ogólne warunki ważności zgody (art. 7 rozporządzenia 2016/679). Ponadto, nawiązując do wzmiankowanego wyżej *ratio legis* prawa do przenoszenia danych osobowych, przetwarzanie danych osobowych w celu świadczenia usług społeczeństwa informacyjnego jest modelowym przykładem zastosowania tego uprawnienia. Wreszcie, odmienne stanowisko skutkowałoby ograniczeniem praw przysługującym dzieciom, co również nie korespondowałoby z celami reformy.

W art. 20 ust. 3 rozporządzenia 2016/679 wskazano m.in., że wykonanie prawa do przenoszenia danych osobowych pozostaje bez uszczerbku dla art. 17 rozporządzenia 2016/679 – który ustanawia prawo do usunięcia danych. Wprowadzenie takiego zastrzeżenia wyeliminowało wątpliwości czy przeniesieniu danych osobowych powinno towarzyszyć ich usunięcie przez „pierwotnego" administratora. Innymi słowy, skorzystanie przez podmiot danych z prawa

[658] J. Kaźmierczak, *Prawo do przenoszenia danych osobowych – wybrane zagadnienia na tle realizacji nowego uprawnienia przyznanego przez RODO*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2018, nr 4, s. 88.

przeniesienia nie kreuje automatycznie po stronie tego administratora obowiązku usunięcia, o ile osoba, której dane dotyczą, tego nie zażąda i nie zostaną spełnione przesłanki z art. 17 ust. 1 rozporządzenia 2016/679[659]. Dotyczy to każdego ze składników prawa do przenoszenia danych – zarówno możliwości otrzymania przez osobę, której dane dotyczą, danych osobowych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, jak i żądania przesłania danych osobowych przez administratora bezpośrednio innemu administratorowi. Należy zaznaczyć, że między prawem do przenoszenia danych a prawem dostępu do danych, w tym uzyskania ich kopii – pomimo, że mogą wydawać się podobne – występują znaczne różnice spowodowane ich całkowicie odmiennymi celami. Prawo dostępu do danych osobowych, o którym mowa w art. art. 15 rozporządzenia 2016/679, służy realizacji zasady przejrzystości przetwarzania i przez to doznaje mniejszych ograniczeń – przede wszystkim jego wykonanie nie jest uzależnione od podstawy prawnej przetwarzania[660].

Oprócz kryteriów podstawy i sposobu przetwarzania danych osobowych, kolejnym ograniczeniem wykonania prawa do przenoszenia danych osobowych jest zgodnie z art. 20 ust. 3 rozporządzenia 2016/679, okoliczność, że wpłynęłoby ono niekorzystnie na prawa i wolności innych. Należy przyjąć, że chodzi o inne osoby niż podmiot danych, który kieruje do administratora żądanie przeniesienia jego danych. W motywie 68 preambuły do rozporządzenia 2016/679 wyjaśniono bowiem, że gdy „określony zestaw danych osobowych odnosi się do więcej niż jednej osoby, której dane dotyczą, prawo do otrzymania danych osobowych nie powinno powodować uszczerbku dla praw i wolności innych osób, których dane dotyczą, na podstawie niniejszego rozporządzenia". Wydaje się więc, że przykładem niekorzystnego wpływu na prawa i wolności innych osób byłoby ujawnienie ich danych osobowych „przy okazji" realizacji prawa do przenoszenia danych na rzecz wnioskującej o to osoby. K. Szymielewicz zauważa, że w praktyce ocena, na czym w danej sytuacji polegałby niekorzystny wpływ na prawa i wolności innych osób, będzie dokonywana przez administratora, więc jej wyniki mogą być kontrowersyjne[661]. Subiektywna ocena administratora może ujemnie wpływać na zakres uprawnień osób, których dane dotyczą.

Jak wskazano wyżej, prawo do przenoszenia danych osobowych może mieć najszersze zastosowanie w obszarze usług świadczonych *online*, w tym usług społeczeństwa informacyjnego. Z wnikliwej analizy przeprowadzonej przez M. Czerniawskiego wynika, że przestrzeganie art. 20 rozporządzenia 2016/679 i zapewnienie osobom, których dane dotyczą, możliwości skorzystania

[659] Por. P. Fajgielski, *Prawo do przenoszenia danych*, „Informacja w administracji publicznej" 2017, nr 4, s. 29.
[660] Szerzej na ten temat por. K. Syska, *Prawo dostępu do danych a prawo przenoszalności – porównanie celu regulacji, zakresu i przesłanek stosowania*, „Prawo Mediów Elektronicznych" 2017, nr 3, s. 4-9.
[661] K. Szymielewicz, *Reforma europejskiego prawa o ochronie danych osobowych z perspektywy praw obywateli – więcej czy mniej ochrony?*, [w:] G. Sibiga (red.), *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, Warszawa 2016, s. 12.

z przewidzianego w nim uprawnienia, w praktyce oznacza nieodzowność wypełnienia przez administratora *de facto* kilkunastu obowiązków. Autor ten wymienia m.in. obowiązek identyfikacji podmiotu danych, precyzyjnego określenia zakresu danych objętych żądaniem przeniesienia, oceny możliwości technicznych, zapewnienia bezpieczeństwa przenoszonych danych, zwłaszcza w trakcie transmisji)[662]. Ponadto na gruncie rozważań na temat bezpieczeństwa L. Scudiero zauważa, że wykonanie prawa do przenoszenia danych powinno być poprzedzone weryfikacją tożsamości wnioskodawcy, ponieważ łatwe uzyskanie i przekazanie danych osobowych innemu podmiotowi może zachęcać do wykorzystania tej możliwości w celu popełniania przestępstw i tzw. kradzieży tożsamości[663]. Zbagatelizowanie przez administratora wyżej wskazanych obowiązków i zagrożeń może rodzić negatywne konsekwencje dla dziecka, przykładowo jeśli problematyczne okaże się ustalenie odpowiedniego zakresu danych, które mają podlegać przeniesieniu, a w razie problemów ze sprecyzowaniem wniosku przez dziecko, administrator określi ten zakres arbitralnie. W sytuacji, gdy podmiotem danych jest dziecko, administrator powinien dołożyć więc szczególnej staranności w informowaniu w przystępny sposób o uwarunkowaniach skorzystania z prawa do przenoszenia danych, a w stosownych przypadkach zachęcać dziecko do zwrócenia się o wsparcie do przedstawiciela ustawowego.

3.2 Sprzeciw wobec przetwarzania danych osobowych

Przepis art. 21 rozporządzenia 2016/679 przyznaje osobie, której dane dotyczą, istotne uprawnienia w kontekście świadczenia usług społeczeństwa informacyjnego. Zgodnie z art. 21 ust. 1 rozporządzenia 2016/679, przysługuje jej prawo wniesienia w dowolnym momencie sprzeciwu z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania opartego m.in. na art. 6 ust. 1 lit. f rozporządzenia 2016/679[664], w tym profilowania na tej podstawie. Wniesienie sprzeciwu powoduje, że administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie jednej z dwóch okoliczności: 1) ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą; 2) podstaw do ustalenia, dochodzenia lub obrony roszczeń. Obowiązek zrealizowania przez administratora uprawnienia, o którym mowa w art. 21 ust. 1 rozporządzenia 2016/679, a w

[662] M. Czerniawski, *Obowiązki administratora danych wynikające z prawa do przenoszenia danych*, [w:] „Monitor Prawniczy" dodatek: *Wdrażanie ogólnego rozporządzenia…*, s. 30-31.
[663] Por. L. Scudiero, *Bringing Your Data Everywhere: A Legal Reading Of The Right To Portability*, „European Data Protection Law Review" 2017, nr 1, s. 124.
[664] Ponadto prawo wniesienia sprzeciwu przysługuje także, gdy podstawą przetwarzania jest art. 6 ust. 1 lit. e rozporządzenia 2016/679 – czyli gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Prawodawca zawęził okoliczności, w których podmiotowi danych przysługuje uprawnienie do wniesienia sprzeciwu, do sytuacji, w których podstawą przetwarzania są dwie wskazane w omawianym przepisie przesłanki – zatem jeśli przetwarzanie opiera się na innej podstawie, np. zgodzie, art. 21 rozporządzenia 2016/679 nie znajduje zastosowania – szerzej na ten temat por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 325.

konsekwencji zaprzestania przetwarzania danych osobowych – oprócz drugiej z powyższych przesłanek – jest więc znacząco uzależniony od istnienia po stronie osoby, której dane dotyczą, szczególnej sytuacji, będącej powodem wniesienia przez nią sprzeciwu. Desygnaty pojęcia „szczególnej sytuacji", ze względu na jego nieostrość, muszą być ustalane na tle konkretnego stanu faktycznego[665]. W literaturze przedstawiono propozycje kryteriów pomocnych w ustaleniu, czy podmiot danych znajduje się w sytuacji, która rodzi obowiązek zrealizowania jej uprawnienia przez administratora. P. Barta, M. Kawecki i P. Litwiński wskazują na stan faktyczny, który nie istniał w momencie zbierania danych osobowych bezpośrednio od podmiotu danych, lub który – w przypadku zebrania danych z innych źródeł – istniał, lecz nie był znany administratorowi. Ponadto autorzy ci uważają, że szczególna sytuacja ma miejsce, gdy dochodzi do zaburzenia równowagi interesów osoby, której dane dotyczą i administratora[666]. Należy podkreślić, że w opinii EROD już sam fakt, że podmiot danych jest dzieckiem, stanowi czynnik przesądzający o zaistnieniu szczególnej sytuacji, o której mowa w art. 21 ust. 1 rozporządzenia 2016/679. Rada przywołała treść motywu 38 preambuły do rozporządzenia 2016/679, w którym prawodawca wyeksponował, że dzieci wymagają szczególnej ochrony danych osobowych[667]. Takie stanowisko zasługuje na poparcie. Wykonywanie uprawnień przysługujących dziecku powinno być ułatwione tak dalece, jak to możliwe. Wymaganie od dziecka należytego, szczegółowego uzasadnienia sprzeciwu stanowiłoby trudną do przezwyciężenia przeszkodę.

Zaistnienie szczególnej sytuacji podmiotu nie jest natomiast przesłanką wymagającą spełnienia w celu uwzględnienia sprzeciwu podmiotu danych, gdy dochodzi do przetwarzania danych osobowych w celu marketingu bezpośredniego. Prawodawca przewidział w tym wypadku dalej idącą ochronę. Specyficzną dla takiego przetwarzania danych osobowych podstawą prawną jest art. 6 ust. 1 lit. f rozporządzenia 2016/679 – prawodawca wskazał w motywie 47 preambuły do rozporządzenia 2016/679 cele marketingowe jako przykład działania realizowanego w ramach prawnie uzasadnionego interesu. Jednocześnie wprowadzone zostały dodatkowe regulacje, ułatwiające podmiotom danych doprowadzenie do zaprzestania przetwarzania ich danych osobowych, uniezależniające działania administratora od oceny spełnienia nieostrych kryteriów czy też wątpliwego co do obiektywności ważenia interesów. W motywie 38 preambuły do rozporządzenia 2016/679 uwypuklono, że szczególna ochrona dzieci powinna urzeczywistniać się przede wszystkim w związku z wykorzystywaniem ich danych osobowych do celów marketingowych, tworzenia profili osobowych lub profili użytkownika. W odniesieniu do

[665] Por. M. Sakowska-Baryła, *Komentarz do art. 21 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 9.
[666] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 21 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Ogólne rozporządzenie…*, Legalis, teza 4.
[667] EROD, *Wytyczne 5/2019*…, s. 13.

przetwarzania danych osobowych do celów marketingu bezpośredniego, prawo do wniesienia sprzeciwu jest bezwzględnie skuteczne[668], co należy uznać za słuszne rozwiązanie, szczególnie, że odnosi się także do profilowania. Stosownie do art. 21 ust. 2 rozporządzenia 2016/679, osoba, której dane dotyczą, może wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest z nim związane. Przepis art. 21 ust. 3 rozporządzenia 2016/679 stanowi wprost, że jeśli podmiot danych wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, nie wolno już przetwarzać danych osobowych do takich celów. Ponadto, co można uznać za ułatwienie osobie fizycznej wniesienie sprzeciwu, art. 21 ust. 5 rozporządzenia 2016/679 przewiduje, że w związku z korzystaniem z usług społeczeństwa informacyjnego może ona wykonać to prawo za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne. Uogólnienie polegające na uznaniu, że chodzi po prostu o umożliwienie wniesienia sprzeciwu drogą elektroniczną[669], wydaje się zbyt daleko idące – mimo że w motywie 59 preambuły użyto tego sformułowania – jeżeli będzie prowadziło do konstatacji, iż chodzi o wysłanie wiadomości za pośrednictwem poczty elektronicznej[670]. Tymczasem zdaje się, że intencja prawodawcy była inna, skoro posłużył się frazą odnoszącą się do „zautomatyzowanych środków" i wykorzystania „specyfikacji technicznych". Interpretacja tego fragmentu art. 21 ust. 5 rozporządzenia 2016/679 nie jest trywialna, jednakże należy zwrócić uwagę, że zgodnie z tym przepisem wykonanie prawa do wniesienia sprzeciwu powinno odbyć się w sposób zautomatyzowany, tzn. bez udziału człowieka, konieczności podjęcia przez niego działań – przynajmniej wtedy, gdy prawo sprzeciwu ma charakter bezwzględny. Większe wątpliwości może budzić zrozumienie, na czym ma polegać wykorzystanie „specyfikacji technicznych". Wyraz „specyfikacja" oznacza przede wszystkim „dokument wystawiony przez dostawcę towarów, dołączony do przesyłki, określający jej zawartość; wykaz zakupionych towarów; wyszczególnienie kosztów produkcji i kosztów handlowych związanych z obrotem przedsiębiorstwa"[671], zaś w j. angielskim słowo *specification*[672] oznacza szczegółowy opis jak coś powinno być zrobione, wykonane[673]. Bardziej trafne byłoby – zakładając, że wniesienie sprzeciwu winno być przystępne – przyjęcie, że chodzi o „funkcję", rozumianą jako „możliwość wykonania określonej operacji przez urządzenie lub program komputerowy"[674]. W motywie 32 preambuły do

[668] M. Czerniawski, *Komentarz do art. 21 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 556.
[669] Tamże, s. 559.
[670] Należy zaznaczyć, że nie ma przeszkód, by był to jeden z kanałów komunikacji z administratorem.
[671] *Internetowy słownik języka polskiego PWN*, https://sjp.pwn.pl/szukaj/specyfikacja.html (dostęp: 25.06.2020).
[672] Taki wyraz pojawia się w art. 21 ust. 5 rozporządzenia 2016/679 w jego anglojęzycznej wersji.
[673] Por. internetowy słownik języka angielskiego Cambridge, https://dictionary.cambridge.org/dictionary/english/specification (dostęp: 25.06.2020), tłum. własne autorki.
[674] *Internetowy słownik języka polskiego PWN*, https://sjp.pwn.pl/slowniki/funkcja.html (dostęp: 25.06.2020).

rozporządzenia 2016/679, w kontekście zgody na przetwarzanie danych osobowych, jako przykładowy sposób jej udzielenia w związku z korzystaniem z usług społeczeństwa informacyjnego wskazano wybór ustawień technicznych. Wydaje się to najwłaściwszym kierunkiem interpretacji, wskazówką wartą przeniesienia na grunt realizacji prawa do wniesienia sprzeciwu. Ilustracją tego typu mogą być popularne „suwaki" lub „przyciski", które bywają dostępne w panelach kont użytkowników usług społeczeństwa informacyjnego i pozwalają na zmianę indywidualnych ustawień w zakresie „ochrony prywatności". Takie rozwiązania można postrzegać jako najbardziej proste i intuicyjne, co ma wyjątkowo duże znaczenie, gdy z usług społeczeństwa informacyjnego korzystają dzieci.

3.3 Niepodleganie decyzji opierającej się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu

Przepis art. 22 ust. 1 rozporządzenia 2016/679 stanowi, że osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Celem tej regulacji jest ochrona podmiotu danych przed skutkami decyzji, podjętej na podstawie jego danych osobowych i bez udziału człowieka – osoby, która wziąwszy pod uwagę istotne, specyficzne w danej sprawie okoliczności, podjęłaby inną decyzję – możliwe, że korzystniejszą dla podmiotu danych[675]. W praktyce w procesie zautomatyzowanego podejmowania decyzji mogą być wykorzystane techniki o różnym stopniu zaawansowania. Możliwe jest zastosowanie prostego programu, który pobiera dane wejściowe, przypisuje je do zmiennej i porównuje z określoną wartością, by następnie podać wynik prawda lub fałsz na potwierdzenie lub zaprzeczenie spełnienia ustalonego kryterium[676]. Na popularności zyskuje przetwarzanie oparte na sztucznej inteligencji i tzw. uczeniu maszynowym (*machine learning*), w których system sam – bez potrzeby dodatkowego programowania przez człowieka – wykorzystując duże zbiory danych i „dane treningowe" (*training data*), uczy się dostrzegać wzorce, a następnie wywodzi z nich wnioski i wychwytuje nowe korelacje oraz tworzy prognozy[677].

Z art. 22 ust. 1 rozporządzenia 2016/679 wynikają dwie przesłanki, które muszą zostać spełnione kumulatywnie, by znalazł zastosowanie: 1) zautomatyzowane przetwarzanie danych osobowych, w tym profilowanie; 2) podjęcie decyzji, która wywołuje skutki prawne wobec

[675] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 332.
[676] Por. A. Kesa, T. Kerikmäe, *Artificial Intelligence and the GDPR: inevitable nemeses?*, „TalTech Journal of European Studies" 2020, nr 3, s. 74.
[677] H. J. Janssen, *An approach for a fundamental rights impact assessment to automated decision-making*, „International Data Privacy Law" 2020, nr 1, s. 81.

podmiotu danych lub w podobny sposób istotnie na niego wpływa[678]. Profilowanie zostało zdefiniowane przez prawodawcę w art. 4 pkt 4 rozporządzenia 2016/679 i szerzej omówione w rozdziale I niniejszej rozprawy. Jeśli chodzi natomiast o pojęcie decyzji, która wywołuje wobec osoby, której dane dotyczą, skutki prawne, Grupa Robocza Art. 29 wyjaśnia, że chodzi o wpływ decyzji na jej prawa określone w przepisach, np. odmowę lub przyznanie świadczenia socjalnego[679]. Natomiast przez decyzje, które wpływają na podmiot danych w podobny, istotny sposób, Grupa Robocza Art. 29 rozumie rozstrzygnięcia niosące ze sobą ryzyko „wywarcia istotnego wpływu na sytuację danej osoby, jej zachowanie lub podejmowane przez nią wybory; wywarcia długotrwałego lub trwałego wpływu na osobę, której dane dotyczą; lub w najbardziej ekstremalnym przypadku, doprowadzenia do wykluczenia lub dyskryminacji osób fizycznych”[680]. Na kanwie rozporządzenia 2016/679 termin „decyzja” słusznie postrzega się jako pojęcie autonomiczne, które „odnosi się do każdego jednostronnego ustalenia sytuacji osoby fizycznej, zatem nie tylko w sferze wykonywania władzy publicznej, ale w każdym obszarze aktywności związanej z przetwarzaniem danych osobowych i objętej zakresem stosowania RODO. (…) Nie istnieje również potrzeba istnienia sformalizowanej procedury wydania takiej decyzji; kluczowe pozostaje faktyczne podjęcie rozstrzygnięcia”[681]. W motywie 71 preambuły do rozporządzenia 2016/679 jako przykłady decyzji, o której mowa w art. 22 ust. 1 rozporządzenia 2016/679, podano „automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej”. W praktyce ocena powagi wpływu decyzji podjętej w sposób zautomatyzowany na osobę, której dane dotyczą, przez nieostre przesłanki zawarte w art. 22 ust. 1 rozporządzenia 2016/679, może nastręczać wielu trudności co powoduje ryzyko, że administratorzy nie będą przyjmować interpretacji ukierunkowanej na wzmocnienie ochrony praw podmiotów danych.

Należy zauważyć, że nie każda operacja profilowania będzie skutkowała podjęciem decyzji, o której mowa w art. 22 ust. 1 rozporządzenia 2016/679, a tym samym nie będzie podpadała pod przewidziane w nim ograniczenia. Celnie ujmuje to A. Mednis wskazując, że „relację między profilowaniem a podejmowaniem zautomatyzowanych decyzji można opisać w następujący sposób: analityk może stworzyć kategorie osób o określonych cechach, przypisać do nich konkretne osoby i na tym poprzestać. Stworzenie profilu nie musi skutkować jakimikolwiek działaniami wobec osoby profilowanej. Wynikiem profilowania może być też zautomatyzowana

[678] A. Mednis, *Prawo ochrony danych…*, s. 176.
[679] Por. Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego…*, s. 24.
[680] Tamże.
[681] G. Sibiga, *Wyłączenie zakazu zautomatyzowanego podejmowania decyzji w przepisach prawa polskiego w świetle wymagań ogólnego rozporządzenia o ochronie danych (RODO) – wybrane zagadnienia*, [w:] „Monitor Prawniczy” dodatek: *Wpływ technologii i technik informatycznych na ochronę danych osobowych. Aktualne problemy prawnej ochrony danych osobowych 2022*, G. Sibiga (red.), 2022, nr 21, s. 87.

decyzja, profilowanie może również zakończyć się innego rodzaju *rozstrzygnięciem* wobec osoby – rozstrzygnięciem, które nie będzie zautomatyzowaną decyzją"[682].

Prawodawca przewidział trzy przypadki, w których uprawnienie podmiotu danych polegające na niepodleganiu decyzji podjętej w sposób zautomatyzowany i wywołującej skutki prawne lub inne istotne, nie znajduje zastosowania. Mianowicie wyłączenie ma miejsce, gdy ta decyzja: jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem (art. 22 ust. 2 lit. a rozporządzenia 2016/679); jest dozwolona prawem UE lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą art. 22 ust. 2 lit. b rozporządzenia 2016/679); opiera się na wyraźnej zgodzie osoby, której dane dotyczą (art. 22 ust. 2 lit. c rozporządzenia 2016/679). Jednocześnie wprowadzono dodatkowe warunki mające na celu wzmocnienie ochrony praw osób, których dane dotyczą. W przypadku wyłączenia, o którym mowa w art. 22 ust. 2 lit. a rozporządzenia 2016/679 i art. 22 ust. 2 lit. c rozporządzenia 2016/679, jest nim – w myśl art. 22 ust. 3 rozporządzenia 2016/679 – wdrożenie przez administratora środków służących ochronie praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania zapadłej decyzji[683]. Ponadto, zgodnie z art. 22 ust. 4 lit. a rozporządzenia 2016/679, który dotyczy wszystkich wyłączeń z art. 22 ust. 2 lit. rozporządzenia 2016/679, decyzje nie mogą opierać się na szczególnych kategoriach danych osobowych. Z kolei warunek ten nie obowiązuje, jeśli przetwarzanie tego rodzaju danych odbywa się na podstawie art. 9 ust. 2 lit. a rozporządzenia 2016/679 lub art. 9 ust. 2 lit. g rozporządzenia – tj. gdy podstawą prawną przetwarzania jest wyraźna zgoda podmiotu danych lub przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa UE lub prawa państwa członkowskiego, a dodatkowo istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Choć wśród celów objęcia szczególną ochroną danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, a w konsekwencji ograniczenia ich wykorzystania w celu podejmowania decyzji w sposób zautomatyzowany, niewątpliwie można wskazać dążenie do zapobieżenia dyskryminacji, prawodawca pominął okoliczność, że częstym powodem nierównego traktowania są płeć i wiek, dlatego zasadnie postuluje się

[682] A. Mednis, *Prawo ochrony danych…,* s. 180.
[683] Szerzej na ten temat por. F. Geburczyk, *Prawa osób fizycznych w kontekście przetwarzania danych osobowych w procesach zautomatyzowanego podejmowania decyzji*, „Monitor Prawniczy" 2020, nr 11, s. 582-586 i tam powołana literatura.

zsynchronizowanie regulacji w dziedzinie prawa antydyskryminacyjnego i ochrony danych osobowych[684].

Analizowane w literaturze przykłady stosowania decyzji podejmowanych w sposób zautomatyzowany w rozumieniu art. 22 ust. 1 rozporządzenia 2016/679 najczęściej dotyczą sektora bankowego[685] i ubezpieczeniowego[686], w których analiza ryzyka oparta na indywidualnej sytuacji klienta odgrywa fundamentalną rolę w procesie określania warunków świadczenia usług i uregulowana jest przepisami prawa[687]. W przypadku usług społeczeństwa informacyjnego nie ulega wątpliwości, że profilowanie jest powszechnie wykorzystywane w szeroko rozumianym celu marketingowym, spersonalizowania oferty. Natomiast przetwarzanie prowadzące do podejmowania decyzji, o których mowa w art. 22 ust. 1 rozporządzenia 2016/679, może występować rzadziej z uwagi na konieczne kryterium wywoływania przez nią skutków prawnych lub innych istotnych, o podobnym wpływie. Należy przychylić się do poglądu, że trudno uznać, by przesłanie materiałów marketingowych do grupy osób, która została automatycznie wyselekcjonowana (przykładowo na podstawie historii ich zakupów), mogło istotnie na nie wpływać[688]. Podobne stanowisko zajęła wcześniej Grupa Robocza Art. 29, zaznaczając jednak, że w kontekście działań marketingowych w internecie nie powinno się *a priori* wykluczać wywarcia istotnego wpływu na podmioty danych, w szczególności jeśli przetwarzanie danych osobowych prowadzi do zróżnicowania ceny usługi lub zwiększenia podatności osób, których dane dotyczą, na podejmowanie niekorzystnych dla nich działań[689]. Jak zasadnie wskazuje M. Kupiec, stanowi to niebezpieczeństwo dla dzieci korzystających z usług społeczeństwa informacyjnego w sytuacji, gdy reklamy behawioralne wpływają na ich rozwój lub bazując na informacjach o nich, wykorzystują je w celu spotęgowania skłonności do ulegania przekazowi marketingowemu. Jako przykład autor ten podaje, za brytyjskim organem nadzorczym ds. ochrony danych osobowych, nakłanianie dzieci do podejmowania szkodliwych dla zdrowia wyborów żywieniowych[690].

---

[684] J. Niklas, *Problem dyskryminacji…,* s. 7.

[685] Na temat scoringu kredytowego w kontekście podejmowania decyzji, o których mowa w art. 22 ust. 1 rozporządzenia 2016/679 por. A. Nierodka, *Badanie zdolności kredytowej konsumentów*, [w:] I. Heropolitańska, A. Nierodka, T. Zdziarski, *Kredyty, pożyczki i gwarancje bankowe*, Warszawa 2021, s. 326-331.

[686] Por. D. Karwala, *Wpływ ogólnego rozporządzenia o ochronie danych osobowych na działalność zakładów ubezpieczeń – zagadnienia wybrane*, „Prawo Asekuracyjne" 2016, nr 4, s. 17-30; J. Byrski, *Przetwarzanie danych osobowych przez pośredników ubezpieczeniowych*, „Wiadomości Ubezpieczeniowe" 2019, nr 3, s. 32-34.

[687] Na temat prawnych regulacji dotyczących warunków podejmowania zautomatyzowanych decyzji przez banki por. A. Mednis, *Analityka w bankowości*, [w:] G. Szpor, K. Czaplicki (red.), *Internet. Analityka danych. Data Analytics*, Warszawa 2019, s. 95-108.

[688] X. Konarski, *Profilowanie danych osobowych…,* s. 50; podobnie także M. Mostowik, *Ochrona danych osobowych…*, s. 169.

[689] Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego…*, s. 25.

[690] Por. M. Kupiec, *Profilowanie dzieci dla celu marketingu cyfrowego w europejskim prawie ochrony danych osobowych. Między paternalizmem a potrzebą realizacji najlepiej pojętego interesu dziecka*, [w:] M. Sakowska-Baryła (red.), *Sztuczna inteligencja, transfery, odpowiedzialność i inne wyzwania ochrony danych osobowych*, Wrocław 2022, s. 434.

W motywie 71 preambuły do rozporządzenia 2016/679 prawodawca stwierdził, że przetwarzanie, o którym mowa w art. 22 ust. 1 rozporządzenia 2016/679, nie powinno dotyczyć dzieci. Teza ta zasługuje na aprobatę, niemniej niepokojące jest to, że nie znalazła odzwierciedlenia w normatywnej części rozporządzenia 2016/679. Przepis art. 22 rozporządzenia 2016/679 nie zawiera żadnej regulacji odnoszącej się *stricte* do przetwarzania danych osobowych dzieci. Grupa Robocza Art. 29 stanęła więc na stanowisku, że nie istnieje bezwzględny zakaz dokonywania tego rodzaju przetwarzania danych osobowych dzieci, jednocześnie postulując, by administratorzy go unikali i nie powoływali się na wyjątki ustanowione w art. 22 ust. 2 rozporządzenia 2016/679, chyba, że przetwarzanie ma służyć ochronie dobra dziecka[691]. Bez pogłębionej refleksji, która wykracza poza przedmiot niniejszej rozprawy, nie można negować istnienia celów, zwłaszcza realizowanych w interesie publicznym, które uzasadniałyby podejmowanie zautomatyzowanych decyzji na podstawie danych osobowych dziecka, jeśli miałoby się to odbywać na podstawie i zgodnie ze szczególnymi przepisami prawa powszechnie obowiązującego – w myśl art. 22 ust. 2 lit. b rozporządzenia 2016/679. Takie wykorzystywanie danych osobowych dziecka w celach komercyjnych może tymczasem wzbudzać sprzeciw, wziąwszy pod uwagę chociażby okoliczności – podstawy prawne – uchylające prawo do niepodlegania decyzjom podejmowanym w sposób zautomatyzowany. Mianowicie mowa o niezbędności przetwarzania do zawarcia i wykonania umowy lub wyraźnej zgodzie na przetwarzanie (odpowiednio art. 22 ust. 2 lit. a rozporządzenia 2016/679 i art. 22 ust. 2 lit. c rozporządzenia 2016/679). W przypadku zgody, należy pojmować ją zgodnie z definicją zawartą w art. 4 pkt 11 rozporządzenia 2016/679[692], ponadto konieczne jest uwzględnienie warunków jej ważności określonych w art. 7 rozporządzenia 2016/679. Należy postawić pytanie, czy powinno się także brać pod uwagę swoistą szczególną regulację dotyczącą zgody na przetwarzanie danych osobowych – art. 8 ust. 1 rozporządzenia 2016/679, przewidujący skuteczne wyrażenie zgody przez dziecko, które ukończyło 16. rok życia? Czy oznaczałoby to, że zgodę na podejmowanie decyzji, o których mowa w art. 22 ust. 1 rozporządzenia 2016/679 – z zastrzeżeniem spełnienia przesłanek określonych w art. 8 ust. 1 rozporządzenia 2016/679 i wymogu wyraźności zgody, wynikającego z art. 22 ust. 2 lit. c rozporządzenia 2016/679 – może skutecznie wyrazić dziecko samodzielnie? W świetle wyrażonej wprost w motywie 71 preambuły do rozporządzenia 2016/679 intencji prawodawcy, by takie przetwarzanie nie dotyczyło dzieci, i zastosowaniu wykładni celowościowej, odpowiedź powinna być przecząca. Odmienne podejście stwarzałoby ryzyko znacznego obniżenia poziomu ochrony praw dzieci – wszak zgoda, o której mowa w art. 22 ust. 2

[691] Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego…*, s. 32.
[692] M. Ciechomska, *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy" 2017, nr 5, s. 40.

lit. c rozporządzenia 2016/679, *de facto* uchyla zakaz ustanowiony w ust. 1 tego przepisu. Obawy, że dziecko nie będzie zdolne do podjęcia świadomej decyzji w tym zakresie są uzasadnione, nawet jeśli administrator skrupulatnie wypełniłby swój obowiązek informacyjny i zgodnie z art. 13 ust. 2 lit. f rozporządzenia 2016/679 uprzedziłby o zamiarze i zasadach podejmowania decyzji w sposób zautomatyzowany, o ich znaczeniu oraz przewidywanych konsekwencjach. Jak wskazano wyżej, Grupa Robocza Art. 29 podjęła próbę wykładni art. 22 rozporządzenia 2016/679 w związku z motywem 71 *in fine* preambuły do rozporządzenia 2016/679 w odniesieniu do przetwarzania danych osobowych dzieci, opowiadając się za wzmocnieniem ochrony ich praw, jednak nie można uznać tego za remedium na występujące w tej kwestii problemy. Po pierwsze wytyczne Grupy Roboczej Art. 29 – choć mają niebagatelne znaczenie dla interpretacji przepisów o ochronie danych osobowych – nie są wiążące dla administratorów ani organów nadzorczych ds. ochrony danych osobowych, które mogą przyjąć odmienne stanowisko i wykładnię[693]. Mimo wiodącej roli wykładni celowościowej prawa UE, oparcie się przez organ nadzorczy wyłącznie na powyższej interpretacji w przypadku skorzystania, w konsekwencji naruszenia rozporządzenia 2016/679, ze szczególnie dotkliwych dla administratora uprawnień naprawczych, stwarza zagrożenie, że tak motywowana decyzja organu zostałaby skutecznie zakwestionowana przed sądem administracyjnym. Przesłanką do nałożenia administracyjnej kary pieniężnej w wysokości do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, jest bowiem naruszenie praw podmiotu danych, o których mowa w art. 22 rozporządzenia 2016/679 (art. 83 ust. 5 lit. b rozporządzenia 2016/679), a ten nie kreuje żadnych szczególnych obowiązków ani ograniczeń w stosunku do przetwarzania danych osobowych dzieci. Po drugie, zgodnie z wytycznymi, przetwarzanie, o którym mowa w art. 22 ust. 1 rozporządzenia 2016/679, w niektórych przypadkach może być dopuszczalne, lecz dokument nie dostarcza żadnych praktycznych wskazówek na ten temat – nie wyczerpuje zagadnienia nawet na swoim poziomie. W przypadku przyjęcia powyższej tezy o dopuszczalności podejmowania decyzji w sposób zautomatyzowany w stosunku do dzieci, niezbędne byłoby dookreślenie przez prawodawcę specjalnych, specyficznych dla problematyki ochrony praw dzieci-użytkowników usług społeczeństwa informacyjnego warunków służących zapewnieniu odpowiedniego poziomu ochrony danych osobowych, zgodnie z założeniami unijnej reformy. W szczególności pożądane byłoby sformułowanie przez prawodawcą dozwolonych celów i podstaw prawnych przetwarzania oraz rodzajów danych osobowych. Zwiększyłoby to pewność prawa, a także ułatwiłoby egzekwowanie obowiązków związanych z ochroną danych osobowych dzieci w kontekście świadczenia usług społeczeństwa informacyjnego.

[693] M. Kupiec, *Profilowanie dzieci…*, s. 435.

4. Proceduralne ramy realizacji uprawnień przysługujących dziecku

Kluczowe zasady realizacji uprawnień osób, których danych dotyczą, oraz proceduralne aspekty reagowania na ich żądania, reguluje art. 12 rozporządzenia 2016/679. W art. 12 ust. 1 rozporządzenia 2016/679 nałożono na administratora obowiązek podjęcia środków pozwalających na udzielanie informacji, o których mowa w art. 13 i art. 14 rozporządzenia 2016/679, a także prowadzenie komunikacja w sprawach związanych z wykonywaniem uprawnień przewidzianych w art. 15-22 i art. 24 rozporządzenia 2016/679 w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka. Jak wyjaśnia Grupa Robocza Art. 29, „wymóg stosowania jasnego i prostego języka oznacza, że informacji należy udzielać w możliwie najprostszy sposób, bez stosowania złożonych struktur zdaniowych i językowych. Informacje powinny być konkretne i jednoznaczne; nie należy ich formułować przy pomocy pojęć abstrakcyjnych lub wieloznacznych ani pozostawiać dowolności interpretacji”[694]. Jest to jeden z przejawów respektowania zasady przejrzystości przetwarzania, sformułowanej w art. 5 ust. 1 lit. a rozporządzenia 2016/679, która stanowi jeden z fundamentów ochrony danych osobowych[695].

Przepis art. 12 ust. 1 *in fine* rozporządzenia 2016/679 określa także formę udzielenia informacji. Powinna być przekazana na piśmie, w tym w stosownych przypadkach elektroniczne. Ponadto w omawianym przepisie przewidziano dopuszczono także przekazanie informacji w formie ustnej pod warunkiem, że zażąda tego osoba, której dane dotyczą, a jej tożsamość potwierdzi się innymi sposobami[696].

Problem weryfikacji tożsamości podmiotu danych jest skomplikowany i nastręcza wielu trudności natury teoretycznej i praktycznej. Wprawdzie art. 12 ust. 6 rozporządzenia 2016/679 stanowi, że w razie uzasadnionych wątpliwości co do tożsamości osoby wnoszącej żądanie zgodnie z art. 15-21 rozporządzenia 2016/679, administrator może wymagać podania dodatkowych, niezbędnych informacji w celu potwierdzenia tożsamości, nie rozwiązuje to powstających dylematów. W pierwszej kolejności po otrzymaniu żądania realizacji uprawnienia związanego z przetwarzaniem danych osobowych, zadaniem administratora jest określenie, czy na podstawie danych podanych w tym wniosku jest w stanie wyszukać dane osobowe wnioskodawcy w swoich zasobach[697], a następnie sprawdzenie czy „okoliczności złożenia żądania

[694] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 9.
[695] J. Łuczak, *Komentarz do art. 12 RODO*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 466.
[696] Szerzej na ten temat por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 12 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Ogólne rozporządzenie…*, Legalis, teza 7.
[697] W zidentyfikowaniu czynności przetwarzania, w których występują, pomocny powinien być rejestr czynności przetwarzania prowadzony na podstawie art. 30 ust. 1 rozporządzenia 2016/679, przez co może pośrednio służyć także jako narzędzie wspierające podmioty danych w sprawowaniu kontroli nad swoimi danymi osobowymi - por. M.M. Bârsan, *A partial overview…*, s. 131.

(tj. m.in. przyjęty sposób komunikacji) w tym wskazany przez osobę zakres informacji umożliwia stwierdzenie, że żądanie pochodzi od osoby uprawnionej (tj. osoby, której dane dotyczą)"[698]. Wyszukanie danych osobowych może rodzić wiele trudności, zwłaszcza jeśli osoba, której dane dotyczą, nie jest zarejestrowanym użytkownikiem usługi, lecz korzysta ze strony internetowej, umożliwiającej zapisanie plików *cookies*, dzięki którym mogą być przetwarzane dane osobowe pod warunkiem spełnienia przesłanek z art. 4 pkt 1 rozporządzenia 2016/679[699]. Podstawowa metoda weryfikacji, polegająca na porównaniu danych osobowych zawartych we wniosku o realizację uprawnienia przysługującego osobie, której dane dotyczą, z danymi już posiadanymi przez administratora, może okazać się nieskuteczna, a wręcz niebezpieczna, jeśli w związku ze świadczeniem usługi społeczeństwa przetwarzane są podstawowe, zasadniczo niepoufne dane osobowe – takie jak imię, nazwisko, adres poczty elektronicznej – a podmiot danych występuje z wnioskiem o wydanie kopii danych osobowych związanych z korzystaniem z usługi, których zakres może być znacznie szerszy, lub o ich przeniesienie do innego administratora. Pochopna realizacja żądania skutkująca ujawnieniem danych osobowych nieuprawnionemu podmiotowi, np. osobie podszywającej się pod osobę, której dane dotyczą, oznaczałaby naruszenie ochrony danych osobowych, które w zależności od rodzaju danych oraz ich zakresu mogłoby nieść ze sobą ryzyko naruszenia praw i wolności podmiotu danych, skutkować np. kradzieżą tożsamości[700]. Jednocześnie należy pamiętać, że administrator musi przestrzegać zasady minimalizacji danych (art. 5 ust. 1 lit. c rozporządzenia 2016/679) i nie może przetwarzać nadmiarowych danych osobowych wyłącznie po to, by zastosować się do rozporządzenia 2016/679[701]. Ponadto na administratorze ciąży obowiązek ułatwiania osobie, której dane dotyczą, wykonania jej praw określonych w art. 15–22 rozporządzenia 2016/679 (por. art. 12 ust. 2 rozporządzenia 2016/679 i motyw 59 preambuły do rozporządzenia 2016/679). Oznacza to, że zarówno zbieranie danych osobowych w szerokim zakresie, jak i stosowanie skomplikowanych, uciążliwych procedur, może narazić administratora na zarzut nieprzestrzegania powyższych przepisów. W motywie 57 preambuły do rozporządzenia 2016/679 prawodawca wyjaśnił także, że „Weryfikacja tożsamości powinna obejmować cyfrową identyfikację osoby, której dane dotyczą, na przykład poprzez mechanizm uwierzytelniania, taki jak te same dane uwierzytelniające, których osoba, której dane dotyczą, używa, by zalogować się do usług internetowych oferowanych przez administratora".

[698] B. Żeromski, *Weryfikacja tożsamości na odległość*, [w:] „Monitor Prawniczy" dodatek: *Wpływ technologii i technik informatycznych…*, s. 51.
[699] Por. D. Nowak-Byrtek, *Realizacja prawa dostępu w związku z przetwarzaniem danych z plików cookies lub innych technologii śledzących – problemy wybrane*, [w:] „Monitor Prawniczy" dodatek: *Wpływ technologii i technik informatycznych…*, s. 67 i tam wskazane orzecznictwo.
[700] Por. M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej…*, Legalis, teza 7; B. Żeromski, *Weryfikacja tożsamości…,* s. 51.
[701] Tak można rozumieć zastrzeżenie znajdujące się w art. 12 ust. 6 rozporządzenia 2016/679, że pozostaje on bez uszczerbku dla art. 11 rozporządzenia 2016/679.

Prawodawca wskazuje w ten sposób preferowaną – choć nie jedyną dopuszczalną – metodę weryfikacji tożsamości, która w praktyce sprowadza się do zalogowania na konto użytkownika usługi. Skuteczne zalogowanie pozwala przyjąć, że wykonała je osoba uprawniona, ponieważ niezbędne jest do tego dysponowanie niezbędnymi informacjami, np. loginem i hasłem. W literaturze zaprezentowano pogląd, że administrator nie powinien kwestionować prowadzenia komunikacji za pośrednictwem poczty elektronicznej pod warunkiem, że wcześniej adres wnioskodawcy został potwierdzony[702]. W istocie jest to weryfikacja odbywająca się na analogicznej zasadzie jak wskazana w motywie 57 preambuły do rozporządzenia 2016/679, ponieważ dostęp do skrzynki poczty elektronicznej wymaga zalogowania do tej usługi, z tą różnicą, że konto pocztowe prowadzi inny podmiot niż administrator, który otrzymuje żądanie. Może być to potencjalnie obarczone większym ryzykiem, gdyż administrator nie wie, jakie zabezpieczenia są stosowane przez dostawcę usługi poczty elektronicznej. Problematyczna może być sytuacja, gdy korzystanie z danej usługi nie wiąże się z założeniem konta użytkownika, lub gdy mimo że konto istnieje, użytkownik utracił do niego dostęp. Wobec niemożności określenia jednej metody weryfikacji tożsamości, która byłaby adekwatna do wszystkich usług, administrator powinien samodzielnie dokonać oceny, uwzględniając stan faktyczny, jakie informacje są niezbędne do potwierdzenia tożsamości i zrealizowania wniosku, co rodzi poważne zagrożenia po jego stronie, a przede wszystkim osoby, której dane dotyczą.

Niebezpieczeństwo wydaje się jeszcze większe i bardziej znaczące, gdy w związku ze świadczeniem usług społeczeństwa informacyjnego przetwarzane są dane osobowe dziecka i chciałoby ono skorzystać z prawa do uzyskania kopii danych lub z prawa do przenoszenia danych. Należy pamiętać, że w przypadku usług społeczeństwa informacyjnego takich jak portale społecznościowe, kopia danych może obejmować całą aktywność użytkownika podejmowaną na przestrzeni lat. W zależności od sposobu korzystania z usługi – tendencji do zamieszczania mniej lub bardziej szczegółowych informacji na temat swojego życia – a także innych danych zbieranych przez dostawcę usługi, np. geolokalizacyjnych – kopia danych, zebrana przykładowo w jednym pliku, może stanowić pokaźny zestaw danych osobowych, który może być wykorzystany przykładowo w celu tzw. kradzieży tożsamości. Pomijając zagrożenie wydania kopii danych osobie nieuprawnionej, także sama osoba, której dane dotyczą, powinna ostrożnie postępować z otrzymanym plikiem. Niefrasobliwe zachowanie, przypadkowe przesłanie lub przechowywanie pliku na urządzeniu, które nie jest odpowiednio zabezpieczone, może skutkować ujawnieniem danych, czego konsekwencje zazwyczaj są nieodwracalne. Jeżeli w celu ułatwienia osobie, której dane dotyczą, dostawca usługi umożliwia pobranie kopii danych poprzez „jedno kliknięcie" na

[702] Por. K. Wygoda, *Komentarz do art. 12 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 6.

koncie użytkownika usługi społeczeństwa informacyjnego, dostęp do tego konta nie powinien być łatwy, wymagający podania trywialnego i krótkiego hasła[703], niezabezpieczony dwuskładnikowym uwierzytelnianiem.

Z kolei w przypadku wykonania prawa do przenoszenia danych należy zauważyć, że „pierwotny" administrator, który przesyła dane innemu, nie ponosi odpowiedzialności za przetwarzanie danych przez nowego administratora[704], nie ma więc żadnego obowiązku sprawdzenia czy dane osobowe po przekazaniu będą przetwarzane zgodnie z rozporządzeniem 2016/679, w tym także z poszanowaniem szczególnych regulacji odnoszących się do ochrony danych osobowych dzieci. Z uwagi na to, że prawo do przenoszenia danych osobowych w jednym z wariantów prowadzi do przekazania danych innemu administratorowi, jeśli „pierwotny" administrator przetwarzał dane osobowe w myśl art. 8 ust. 1 rozporządzenia 2016/679 po uzyskaniu zgody lub aprobaty przedstawiciela ustawowego, najwłaściwsze wydawałoby się spełnienie żądania dziecka pod warunkiem legitymowania się analogiczną akceptacją. Odmienne stanowisko przeczyłoby celom art. 8 ust. 1 rozporządzenia 2016/679, gdyż oznaczałoby zgodę na „obejście" wymogu wyrażenia zgody przez przedstawiciela ustawowego lub zaaprobowania zgody udzielonej wcześniej przez dziecko. Można również argumentować, że to nowy administrator powinien zadbać o legitymowanie się podstawą prawną przetwarzania danych osobowych i ewentualnie wystąpić do przedstawiciela ustawowego o potwierdzenie zgody. Takie podejście byłoby obarczone mankamentami. Po pierwsze, to podmiot danych decyduje, jakie dane mają być przekazane innemu administratorowi – dziecko może przykładowo pominąć dane kontaktowe swojego przedstawiciela ustawowego, zatem nowy administrator nie będzie nimi dysponował. Po drugie, od momentu otrzymania danych osobowych nowy administrator zaczyna je przetwarzać, a z uwagi na dobro dziecka wydaje się, że kwestia dopuszczalności takiego przetwarzania powinna być rozstrzygnięcia przed jego rozpoczęciem, ponieważ nie są znane jego skutki – nowy administrator spełnia obowiązek informacyjny na podstawie art. 14 rozporządzenia 2016/679 i w terminie określonym w art. 14 ust. 3 rozporządzenia 2016/679, a przepis ten nie nakazuje dopełnienia tego obowiązku natychmiast. W przypadku przetwarzania danych osobowych dziecka, które nie może w myśl art. 8 ust. 1 rozporządzenia 2016/679 wyrazić samodzielnie zgody na przetwarzanie danych osobowych w celu korzystania z usługi społeczeństwa informacyjnego, rozpoczęcie korzystania z innej usługi – które nastąpiłoby w wyniku skorzystania z prawa do przenoszenia danych – również nie powinno być uznane za

[703] Według wytycznych CERT Polska - Naukowej i Akademickiej Sieci Komputerowej, zalecane jest stosowanie długich haseł, tzn. składających się z co najmniej 14 znaków – por. *Ważne zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych*, https://cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf (dostęp: 31.08.2023).
[704] Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia…*, s. 7.

dopuszczalne bez spełnienia warunków związanych z udziałem przedstawiciela ustawowego w procesie udzielania zgody. Nie wynika to z przepisów rozporządzenia 2016/679 i należy postulować doprecyzowanie przez prawodawcę sposobu korzystania z uprawnień, o których mowa w art. 15 ust. 3 rozporządzenia 2016/679 i art. 20 rozporządzenia 2016/679 w sytuacji, gdy przysługują one dziecku.

Przepis art. 12 rozporządzenia 2016/679 określa terminy i formę, w jakich administrator powinien udzielić odpowiedzi na wniosek osoby, której dane dotyczą. Administrator powinien bez zbędnej zwłoki, nie później niż w ciągu miesiąca od otrzymania żądania, udzielić informacji w przedmiocie działań podjętych w związku z żądaniem na podstawie art. 15–22 rozporządzenia 2016/679, jednak w wyjątkowych przypadkach, uzasadnionych skomplikowanym charakterem żądania lub liczbą żądań, administrator może przedłużyć termin o kolejne dwa miesiące uprzedzając podmiot danych o przedłużeniu i wyjaśniając jego przyczyny (por. art. 12 ust. 3 i 4 rozporządzenia 2016/679).

Zgodnie z art. 12 ust. 1 rozporządzenia 2016/679, informacji udziela się na piśmie lub w inny sposób, w tym elektronicznie. Według motywu 59 preambuły do rozporządzenia 2016/679, powinnością administratora jest zapewnienie sposobności wnoszenia żądań drogą elektroniczną, w szczególności w przypadku przetwarzania danych osobowych drogą elektroniczną. Posłużenie się frazą „przetwarzanie danych osobowych drogą elektroniczną" sugeruje, że chodzi zwłaszcza o przypadek usług społeczeństwa informacyjnego. Dodatkowo art. 12 ust. 1 rozporządzenia 2016/679 wskazuje, że jeśli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się jej tożsamość. Ten sposób jest jednak wyjątkowo ryzykowny – gdy chodzi o kontakt telefoniczny, nie można mieć pewności, kim jest rozmówca, a możliwość weryfikacji tożsamości jest ograniczona. W dobie rosnącej popularności ataków typu *Caller ID Spoofing*[705], administrator z pewnością nie powinien opierać jej na sprawdzeniu, z jakiego numeru dzwoni wnioskodawca i czy pokrywa się on z tym, który administrator posiada.

Korzystanie przez podmiot danych z uprawnień związanych z przetwarzaniem dotyczących go danych osobowych jest co do zasady wolne od opłat, choć w przypadku żądań ewidentnie nieuzasadnionych lub nadmiernych z uwagi na ustawiczny charakter, administrator może pobrać rozsądną opłatę albo odmówić podjęcia działań (por. art. 12 ust. 5 rozporządzenia 2016/679). Za rozsądną opłatę należy uznać taką, która jest uzasadniona kosztami[706]. Zdaniem K. Wygody, o ewidentnie nieuzasadnionych żądaniach można mówić w przypadku, gdy są kierowane do

[705] *Caller ID Spoofing* polega na podszyciu się pod dowolnie wybrany numer telefonu dzięki dostępnym w internecie narzędziom – innymi słowy numer, który wyświetla się na ekranie telefonu, nie jest w rzeczywistości tym, z którego nawiązywane jest połączenie – por. Ministerstwo Cyfryzacji, *Czym jest spoofing? Jak go rozpoznać i nie dać się nabrać?*, https://www.gov.pl/web/cyfryzacja/czym-jest-spoofing--jak-go-rozpoznac-i-nie-dac-sie-nabrac (dostęp: 04.08.2022).
[706] P. Fajgielski, *Ogólne rozporządzenie…*, s. 247.

administratora w bardzo krótkich odstępach czasu, seryjne, a o nadmiernych jeśli prowadzą do dezorganizacji funkcjonowania podmiotu (administratora) lub są wnoszone w celach wykraczających poza te, jakim powinny służyć (nadużycie prawa)[707].

Szczególną regulację w zakresie opłat, dotyczącą wyłącznie prawa do otrzymania kopii danych osobowych, zawiera art. 15 ust. 3 rozporządzenia 2016/679. Zgodnie z nim, pierwsza kopia jest wolna od opłat, natomiast za kolejne administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Decyzja co do poboru opłaty i ustalenia jej wysokości – wobec braku szczegółowych regulacji w tym zakresie – należy do administratora, choć nie oznacza to, że ma całkowitą dowolność w kształtowaniu jej wysokości. Opłata powinna stanowić wyłącznie rekompensatę poniesionych przez niego kosztów, a nie może prowadzić do osiągania zysków[708].

Wprawdzie rozporządzenie 2016/679 nie różnicuje zasad pobierania opłaty ze względu na wiek osoby, której dane dotyczą, wydaje się jednak, że w przypadku dziecka uzależnienie realizacji jego uprawnienia od wniesienia opłaty może stanowić istotne utrudnienie, które nie do końca wydaje się uzasadnione, zwłaszcza jeśli w przypadku prawa uzyskania kopii danych między pierwszym a kolejnym żądaniem upłynął dłuższy czas. Ponadto należy zwrócić uwagę, że potrzeba ponownego otrzymania kopii danych może wynikać z wdrożenia przez administratora nowych operacji przetwarzania i chęci sprawdzenia, jakie dane osobowe w związku z tym przetwarza. W takim przypadku ponowne zwrócenie się o kopię danych nie powinno powodować możliwości obciążenia dziecka (czy też jego przedstawiciela ustawowego) opłatą. Wydaje się, że pożądane byłoby doprecyzowanie zasad pobierania opłaty, w tym wprowadzenie wyjątków – okoliczności, w których administrator nie mógłby jej naliczyć. Taki wyjątek powinien dotyczyć przede wszystkim przetwarzania danych osobowych dzieci.

Omówione w niniejszym rozdziale uprawnienia przysługują podmiotowi danych – dziecku, którego dane osobowe przetwarzane są w związku z korzystaniem z usług społeczeństwa informacyjnego. Przepisy rozporządzenia 2016/679 nie zawierają szczególnych regulacji w zakresie zasad wykonywania uprawnień przez dzieci i są z tego powodu krytykowane. Dla porównania, COPPA wprost nakłada obowiązek zamieszczenia na stronie internetowej przeznaczonej dla dzieci poniżej 13. roku życia sekcji dla rodziców, w której mogą znaleźć instrukcje dotyczące ich uprawnień odnoszących się do danych osobowych ich dzieci, w tym jak skontaktować się z operatorem strony w celu usunięcia danych oraz realizacji innych

[707] Por. K. Wygoda, *Komentarz do art. 12 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 9.
[708] Por. J. Łuczak, *Komentarz do art. 15 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 516.

uprawnień[709]. Dostrzegając liczne niejasności w obszarze wykonywania uprawnień przysługujących dziecku na podstawie rozporządzenia 2016/679, M. Kupiec podnosi zasadność wydania przez EROD wytycznych zawierających praktyczne przykłady, które stanowiłyby pomoc dla administratorów w ocenie, „od kiedy i w jakim stopniu powinni uwzględniać aktywny głos dziecka i dopuszczać go do współuczestniczenia w wykonywaniu przynależnych mu praw"[710]. Warto zwrócić uwagę, że przepisy rozporządzenia 2016/679 odnoszące się do wykonywania przez osoby, których dane dotyczą, przysługujących jej praw, mogą być doprecyzowane w branżowych kodeksach postępowania (por. art. 40 ust. 2 lit. f rozporządzenia 2016/679), podlegających zatwierdzeniu przez organ nadzorczy ds. ochrony danych osobowych i stanowiących swoiste *soft law*, jednak instrument ten nie jest wykorzystywany[711]. Pomijając zasygnalizowane wyżej obawy o bezpieczeństwo i dobro dziecka w razie samodzielnego wykonywania przez dziecko prawa dostępu do kopii danych lub ich przenoszenia, wydaje się, że nie powinno się ograniczać możliwości niezależnego, tzn. niewymagającego udziału przedstawiciela ustawowego, kierowania do administratora żądań na podstawie art. 15-22 rozporządzenia 2016/679. W szczególności nie powinno się tworzyć takich barier w przypadku, gdy dziecko może samo w myśl art. 8 ust. 1 rozporządzenia 2016/679 wyrazić zgodę na przetwarzanie danych osobowych lub gdy usługa społeczeństwa informacyjnego oferowana bezpośrednio dziecku ma charakter profilaktyczny lub doradczy, a korzystanie z niej nie powinno wymagać zgody przedstawiciela ustawowego (por. motyw 38 rozporządzenia 2016/679). Irlandzki organ nadzorczy ds. ochrony danych osobowych, podkreślając podmiotowość dziecka, stwierdza, że może ono samodzielnie kierować żądania do administratora, w tym także o wydanie kopii danych. Organ uznaje, że taka była intencja prawodawcy, co wywodzi z motywu 58 preambuły do rozporządzenia 2016/679[712], zgodnie z którym „dzieci zasługują na szczególną ochronę, wszelkie informacje i komunikaty – gdy przetwarzanie dotyczy dziecka – powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć". W motywie wskazano, że chodzi o „informacje i komunikaty", podobnie jak w art. 12 ust. 1 rozporządzenia 2016/679 oddzielono od siebie

[709] Por. F. Persano, *GDPR and Children Rights in EU Data Protection Law*, „European Journal of Privacy Law & Technologies. Special Issue", M. Foglia (red.), 2020, s. 35.

[710] M. Kupiec, *O potrzebie przyjęcia nowego podejścia do ochrony danych osobowych dzieci przez EROD. Uwagi w świetle Opinii nr 2/2009 Grupy Roboczej Art. 29 o ochronie danych osobowych dzieci*, [w:] „Monitor Prawniczy" dodatek: *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych. Aktualne problemy ochrony danych osobowych 2021*, G. Sibiga (red.), 2021, nr 23, s. 98.

[711] Jak wynika z opublikowanego przez EROD rejestru, w UE nie został dotąd zatwierdzony ani jeden kodeks regulujący problematykę ochrony danych osobowych dzieci (https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_pl, dostęp: 31.08.2023).

[712] Data Protection Commission, *Children, Parents and Data Protection: Can I make a complaint on behalf of my child?*, https://www.dataprotection.ie/sites/default/files/uploads/2022-06/Guidance%20Children%20Parents%20and%20Data%20Protection-%20Can%20I%20make%20a%20complaint%20on%20behalf%20of%20my%20child.pdf (dostęp: 15.04.2023), s. 2.

udzielanie informacji od prowadzenia komunikacji. Przez informowanie rozumie się więc wypełnianie obowiązków informacyjnych, o których mowa w art. 13 i 14 rozporządzenia 2016/679 (działanie jednostronne), zaś przez komunikowanie się – kontaktowanie się w sprawach dotyczących realizacji uprawnień osoby, której dane dotyczą, przewidzianych w art. 15-22 oraz art. 34 rozporządzenia 2016/679 (działanie obustronne)[713]. W tym świetle należy uznać interpretację irlandzkiego organu nadzorczego ds. ochrony danych osobowych za godną aprobaty. Podobne stanowisko zdaje się zajmować EROD wskazując w swoich wytycznych, że w zależności od dojrzałości dziecka, może ono potrzebować wsparcia innej osoby w wykonywaniu swoich uprawnień, np. przedstawiciela ustawowego[714]. Można tym samym rozumieć, że sam fakt bycia dzieckiem nie powinien automatycznie wykluczać samodzielnej realizacji uprawnień przysługujących na podstawie przepisów rozporządzenia 2016/679.

[713] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 243-244.
[714] EROD, *Guidelines 01/2022…*, s. 30.

ROZDZIAŁ IV
OBOWIĄZKI ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH DZIECKA I WYKAZYWANIE ZGODNOŚCI Z ROZPORZĄDZENIEM 2016/679

1. Obowiązek wdrożenia technicznych i organizacyjnych środków bezpieczeństwa

1.1 Uwzględnienie specyficznych uwarunkowań związanych z przetwarzaniem danych osobowych dziecka w fazie projektowania i przestrzeganie zasady domyślnej ochrony danych

Wraz z wejściem w życie rozporządzenia 2016/679 zasada uwzględniania ochrony danych osobowych w fazie projektowania przedsięwzięcia, które ma wiązać się z przetwarzaniem danych osobowych, stała się – w myśl art. 25 ust. 1 tego aktu – prawnym obowiązkiem administratora. Wcześniej koncepcja *privacy by design* uważana była za dobrą praktykę, ważny postulat sprzyjający wzmocnieniu ochrony danych osobowych i prywatności. Sformułowała go w latach 90. Ann Cavoukian, następnie rozwijając i wskazując na kilka elementów składowych – przede wszystkim na proaktywność, rozumianą jako zapobieganie naruszeniom (w opozycji do reaktywności, czyli zauważania potrzeby ochrony prywatności dopiero gdy zdarzy się incydent), stosowanie rozwiązań służących ochronie bez uszczerbku dla funkcjonalności i użyteczności systemu informatycznego oraz zachowanie przejrzystości[715]. Te postulaty zostały ujęte w Rezolucji w sprawie prywatności w fazie projektowania, przyjętej podczas 32 Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności w Jerozolimie w 2010 r., a w toku prac nad unijną reformą ochrony danych osobowych proponowano, by włączyć je do projektowanego rozporządzenia[716]. Znaczenie uwzględniania ochrony danych w fazie projektowania podkreślała także ENISA. W swoim raporcie opublikowanym w 2014 r. spostrzegła, że w tradycyjnym podejściu inżynierów brakuje świadomości w zakresie rozwiązań służącym ochronie prywatności i danych oraz sposobów ich wdrażania, zaś wiedza rozwijana przez specjalistów ochrony danych osobowych nierzadko ma znikome znaczenie praktyczne[717]. Agencja słusznie stwierdziła, że niezbędne jest podejście interdyscyplinarne, podczas gdy skuteczne stosowanie zasady uwzględniania ochrony danych w fazie projektowania dodatkowo utrudnia niejednolite oraz zbyt

[715] A. Cavoukian, *Privacy by Design. The 7 Foundational Principles*, https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (dostęp: 15.03.2023).
[716] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 355.
[717] ENISA, *Privacy and Data Protection by Design – from policy to engineering*, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (dostęp: 15.03.2023), s. 4.

wąskie rozumienie koncepcji ochrony prywatności, w którym sprowadza się ją do zachowania poufności informacji[718].

Przepis art. 25 ust. 1 rozporządzenia 2016/679 obliguje administratora do wdrażania, zarówno podczas projektowania nowych przedsięwzięć związanych z przetwarzaniem danych osobowych, jak i w czasie ich funkcjonowania, odpowiednich technicznych i organizacyjnych środków w celu spełnienia zasad ochrony danych osobowych, zwłaszcza zasady minimalizacji, oraz odpowiedniego zabezpieczenia przetwarzania. Mimo wymienienia przez prawodawcę tylko jednej z zasad przetwarzania danych osobowych, brzmienie tego przepisu nie pozostawia wątpliwości, że obejmuje swoim zakresem wszystkie zasady określone w art. 5 rozporządzenia 2016/679, co podkreśla EROD w swoich wytycznych[719]. W konsekwencji przyjęcie na gruncie rozporządzenia 2016/679 podejścia opartego na ryzyku, podobnie jak we wcześniej omówionych przepisach, art. 25 ust. 1 rozporządzenia 2016/679 przewiduje obowiązek badania ryzyka naruszenia praw i wolności podmiotów danych przy uwzględnieniu stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania danych osobowych[720].

Składową koncepcji *privacy* i *data protection by design* jest zasada *privacy by default* – domyślnej ochrony danych[721]. Na mocy art. 25 ust. 2 rozporządzenia 2016/679 stosowanie domyślnej ochrony danych stało się obowiązkiem administratora. Stosownie do tego przepisu, administrator wdraża techniczne i organizacyjne środki, które zapewniają domyślne przetwarzanie tylko danych osobowych niezbędnych do zrealizowania konkretnego celu. W art. 25 ust. 2 rozporządzenia 2016/679 prawodawca określił, że w celu wywiązania się z tego obowiązku należy wziąć pod uwagę ilość zbieranych danych osobowych, zakres ich przetwarzania[722], czas przechowywania oraz dostępność – podkreślając, że dane osobowe nie mogą być domyślnie udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych. Zasada domyślnej ochrony danych dotyczy zatem przede wszystkim ustawień, wstępnie skonfigurowanych przez administratora, które mogą być zmienione przez podmiot danych – np. jeśli użytkownik portalu społecznościowego świadomie podejmie decyzję o udostępnieniu swoich danych osobowych niegraniczonemu kręgowi odbiorców[723]. W motywie 78 preambuły do

[718] ENISA, *Privacy and Data Protection…*, s. 47.
[719] EROD, *Wytyczne nr 4/2019 dotyczące artykułu 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych*, przyjęte 20 października 2020 r., https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_pl.pdf (dostęp: 15.03.2023), s. 7.
[720] Por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 25 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 1.
[721] Por. K. Wygoda, *Komentarz do art. 25 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 5.
[722] Przez „zakres przetwarzania" można rozumieć rodzaj i częstotliwość operacji przetwarzania – por. Por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 25 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 7.
[723] Por. M. Bienias, *Ochrona danych w fazie projektowania oraz domyślna ochrona danych (privacy by design oraz privacy by default) w ogólnym rozporządzeniu o ochronie danych*, „Monitor Prawniczy" dodatek: *Ogólne*

rozporządzenia 2016/679 wskazano, że środki służące zadośćuczynieniu zasadzie uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony „mogą polegać m.in. na minimalizacji przetwarzania danych osobowych, jak najszybszej pseudonimizacji danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń".

EROD podaje przykłady działań, które powinny być podjęte w celu uwzględnienia poszczególnych zasad ochrony danych osobowych na etapie projektowania oraz w celu zapewnienia domyślnej ochrony. Ze względu na przedmiot niniejszej rozprawy na szczególną uwagę zasługują wskazówki odnoszące się do przetwarzania danych osobowych dzieci. Według EROD, przykładowym zagrożeniem, jakie powinien wziąć pod uwagę administrator analizujący ryzyko naruszenia praw i wolności pod kątem spełnienia wymogów z art. 25 rozporządzenia 2016/679, jest brak dobrowolności zgody na przetwarzanie danych osobowych udzielanej przez dzieci, jako „grupy szczególnie narażonej"[724]. Innymi słowy, przed rozpoczęciem przetwarzania, administrator powinien wnikliwie zbadać planowany proces pozyskiwania zgody dzieci pod względem jego zgodności z określonymi w art. 7 rozporządzenia 2016/679 warunkami ważności zgody. Bardzo istotne w kontekście przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego wydaje się to, jak od strony praktycznej wygląda sposób pozyskania zgody, np. formularz wypełniany przez podmiot danych – czy oświadczenia o wyrażeniu zgody na cele dodatkowe, wykraczające poza to, co niezbędne do świadczenia usługi, nie są wymuszane poprzez taką konfigurację formularza, która uniemożliwia rozpoczęcie korzystania z usługi bez udzielenia zgody. Dobrowolność wyrażonej przez dziecko zgody może także budzić uzasadnione wątpliwości w sytuacji, gdy administrator stosuje techniki nakłaniające do udzielenia zgody, wywierając w ten sposób wpływ na decyzję dziecka, co do zasady bardziej podatnego na taką perswazję niż osoba dorosła, z bogatszym doświadczeniem życiowym.

Obserwowane w internecie naganne praktyki przedsiębiorców, polegające na nakłanianiu konsumentów do podejmowania decyzji, które nie są zbieżne z ich rzeczywistą wolą lub wręcz dla nich niekorzystne, dzięki stosowaniu odpowiednio zaprojektowanych interfejsów[725], określa się terminem *dark patterns* – „ciemnych wzorców", którego autorstwo przypisuje się

rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016, G. Sibiga (red.), 2016, nr 20, s. 53-55.

[724] EROD, *Wytyczne nr 4/2019*…, s. 10.

[725] Wyraz „interfejs" wywodzi się z informatyki i jest niejednoznaczny. Na potrzeby dalszych rozważań najbardziej trafne wydaje się przyjęcie, że chodzi o „interfejs użytkownika", deifniowany jako „część programu obsługująca komunikację między nim a użytkownikiem" – *Encyklopedia PWN*, https://encyklopedia.pwn.pl/encyklopedia/interfejs%20użytkownika.html (dostęp: 15.03.2023).

H. Brignullowi[726]. Z czasem, w związku z unikaniem sformułowań nieintencjonalnie wywołujących negatywne skojarzenia lub powielających stereotypy, H. Brignull i inni współtwórcy witryny, opisującej złe praktyki, zaczęli operować terminem *deceptive patterns*[727], co można przetłumaczyć jako „zwodnicze wzorce". Wśród podanych na prowadzonej m.in. przez H. Brignulla stronie internetowej typów takich działań, wraz ze wskazaniem stosujących je usługodawców, uwagę zwracają zwłaszcza przykłady technik, które wydają się szczególnie niebezpieczne dla dzieci – polegające na manipulacji emocjami, wyświetlaniu fałszywych, pozytywnych recenzji i komentarzy o usłudze, utrudnianiu rezygnacji z usługi poprzez wyjątkowo skomplikowane procedury, przekazywaniu natarczywych komunikatów w celu namówienia użytkownika do pożądanego przez usługodawcę zachowania, utrudnianiu dostępu do informacji o warunkach świadczenia usługi.

Jako przykład karygodnych praktyk stosowanych w mediach społecznościowych można wskazać działania portalu Facebook – Federalna Komisja Handlu Stanów Zjednoczonych stwierdziła, że wprowadzenie istotnych zmian w ustawieniach prywatności, bez uprzedniego poinformowania o tym użytkowników, należy uznać za „zwodnicze" (*deceptive*) i nieuczciwe praktyki. Zmiany wdrożone na portalu polegały m.in. na tym, że zmodyfikowano wcześniejsze, indywidualne ustawienia prywatności wprowadzone przez użytkowników i bez ich zgody rozszerzono dostęp do ich danych osobowych[728], co na gruncie art. 25 ust. 2 rozporządzenia 2016/679 *in fine* stanowiłoby naruszenie obowiązku stosowania domyślnej ochrony danych osobowych. Z kolei w przypadku portalu Instagram, irlandzki organ nadzorczy ds. ochrony danych osobowych stwierdził naruszenie przepisów rozporządzenia 2016/679 polegające m.in. na domyślnym upublicznianiu danych osobowych dzieci wbrew zasadzie domyślnej ochrony, nieinformowaniu ich o celach takiego upubliczniania, zaniechania przeprowadzenia oceny skutków dla ochrony danych dzieci w zakresie zmiany typu konta i wiążącego się z tym nierozerwalnie opublikowania danych kontaktowych, które powoduje ryzyko wystąpienia zagrożenia w postaci niebezpiecznej, prowadzącej do nadużyć (*abusive*) komunikacji z dziećmi, np. w celu oszustwa[729]. Na administratora – Meta Platforms Ireland Limited – zostały nałożone administracyjne kary pieniężne w łącznej wysokości 405 milionów euro.

---

[726] A. Pawełko, *Autonomia woli konsumenta w kontekście praktyk typu dark patterns*, [w:] M. Namysłowska, K. Podgórski, E. Sługocka-Krupa (red.), *Wyzwania dla prawa konsumenckiego w wymiarze globalnym, regionalnym i lokalnym*, Warszawa 2022, Legalis.

[727] H. Brignull, M. Leiser, C. Santos, K. Doshi, *Deceptive Design*, https://www.deceptive.design, (dostęp: 15.03.2023).

[728] Por. E. Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, „Pace Law Review" 2020, vol. 40, issue 1, s. 332.

[729] Por. decyzja Data Protection Commission z dnia 02.09.2022 r. w sprawie IN-20-7-4, https://edpb.europa.eu/system/files/2022-09/in-20-7-4_final_decision_-_redacted.pdf (dostęp: 15.03.2023), w szczególności wnioski przedstawione na s. 137 i 151.

W kontekście przetwarzania danych osobowych w związku ze świadczeniem usług społeczeństwa informacyjnego, dokładniej mediów społecznościowych, EROD posługuje się z kolei terminem *deceptive design patterns*, rozumianym jako „interfejsy i kroki, przez jakie przechodzi użytkownik, ukierunkowane na wywarcie na niego wpływu by podjął niechciane działania wbrew swoim prawdziwym intencjom, które potencjalnie niosą dla niego szkodliwe skutki i często są sprzeczne z jego najlepiej pojętym interesem, a z drugiej strony są korzystne dla dostawcy usługi w aspekcie przetwarzania danych osobowych"[730]. EROD trafnie zauważa, że praktyki typu *deceptive design patterns* mogą wystąpić na każdym etapie „cyklu życia" konta w mediach społecznościowych – począwszy od rejestracji użytkownika, spełniania obowiązku informacyjnego w myśl art. 13 rozporządzenia 2016/679, pozyskiwania zgody, zawiadamiania o ewentualnych naruszeniach ochrony danych osobowych, aż po procedurę zamykania konta i usuwania danych[731]. W przypadku dzieci, EROD podkreśla wagę zagrożeń związanych z oddziaływaniem na ich emocje, co może skutkować podaniem danych osobowych w zbyt szerokim zakresie[732]. W następstwie zidentyfikowania niebezpieczeństw związanych z *deceptive design patterns* i typowych przejawów stosowania takich technik wywierania nacisku, w wytycznych przedstawiono listę dobrych praktyk pozwalających uniknąć stosowania takich działań, które można uznać za uniwersalne – adekwatne także do innych niż media społecznościowe usług społeczeństwa informacyjnego. Przykładowo, znalazły się wśród nich zalecenia, by ułatwiać podmiotom danych dostęp do polityk opisujących zasady przetwarzania, danych kontaktowych administratora i organu nadzorczego ds. ochrony danych osobowych (by złożenie skargi nie wymagało szukania dodatkowych informacji), definiować specjalistyczne terminy używając zrozumiałego języka, wyjaśniać skutki zmiany ustawień, wprowadzić formularz upraszczający wykonywanie uprawnień przysługujących na podstawie rozporządzenia 2016/679[733].

Adresowane głównie do inżynierów zalecenia związane z tworzeniem aplikacji mobilnych, w tym wskazówki pomagające stosować zasadę uwzględniania ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych opublikowała ENISA. W dokumencie nawiązano do opisanej w literaturze koncepcji „strategii projektowania prywatności" – rozumianej jako odrębny cel architektoniczny, służący osiągnięciu odpowiedniego poziomu ochrony, który wykracza poza

[730] EROD, *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them*, przyjęte 14 lutego 2023 r., https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_pl (dostęp: 15.03.2023), s. 3, tłumaczenie autorki.
[731] Tamże, s. 4.
[732] Tamże, s. 20.
[733] Tamże, s. 73-74.

klasyczne pojmowanie strategii architektonicznej w dziedzinie inżynierii oprogramowania[734]. Opisano cele, które powinny przyświecać twórcom aplikacji mobilnych – możliwie jak największe ograniczenie przetwarzania danych osobowych, uniknięcie korelacji danych osobowych dzięki ich logicznemu lub fizycznemu oddzieleniu, ograniczenie szczegółowości przetwarzanych danych, zapobieganie upublicznieniu danych osobowych, przejrzyste informowanie podmiotów danych o przetwarzaniu w sposób dostosowany do specyfiki korzystania z aplikacji na urządzeniu ze stosunkowo małym ekranem, wprowadzenie funkcjonalności umożliwiających podmiotom danych kontrolowanie przetwarzania danych, wdrażanie „przyjaznego prywatności" przetwarzania z zaangażowaniem z możliwością udowodnienia tego – wraz z przykładami, jak zrealizować te dyrektywy[735]. Podobnie jak w przypadku wytycznych EROD uprawniona jest teza, że rekomendacje ENISA – choć uchwycono w nich specyfikę przetwarzania danych osobowych w aplikacjach mobilnych – mogą być pomocniczo wykorzystywane przy tworzeniu innych usług, w tym usług społeczeństwa informacyjnego. Wdrożenie tych rozwiązań powinno być uwzględnione podczas projektowania przedsięwzięcia związanego z przetwarzaniem danych osobowych.

W swoich wytycznych EROD podkreśla szczególne znaczenie zakazu domyślnego udostępniania danych osobowych dzieci nieokreślonej liczbie osób, ponieważ informacje o nich mogą być wykorzystane do dalszego rozpowszechniania. Rada wyjaśnia, że „interwencją" podmiotu danych, o której mowa w art. 25 ust. 2 rozporządzenia 2016/679, może być przykładowo zgoda, wyrażona w następstwie zapytania o nią lub zaproponowanie użytkownikowi zmiany ustawień[736]. Udostępnienie, rozpowszechnienie danych osobowych zalicza się do operacji przetwarzania danych osobowych, w myśl definicji zawartej w art. 4 pkt 2 rozporządzenia 2016/679, zatem w przypadku oparcia takiego przetwarzania na podstawie zgody podmiotu danych, niewątpliwie to oświadczenie woli powinno zadośćuczynić wszystkim warunkom ważności zgody stosownie do art. 7 rozporządzenia 2016/679, a w przypadku dzieci – dodatkowo do art. 8 rozporządzenia 2016/679. W kontekście przetwarzania danych osobowych – szczególnie gdyby miało to dotyczyć dzieci – pomysł EROD, by propozycja zmiany domyślnych ustawień lub wyrażenia zgody na udostępnienie danych osobowych była inicjowana przez administratora, jest moim zdaniem niefortunny. Można przypuszczać, że dostawca usługi zwracając się z taką prośbą będzie promował, nawet pośrednio – przez sam fakt zainicjowania interakcji w tej sprawie – dzielenie się informacjami o sobie w szerokim zakresie, co może zachęcać dzieci do akceptowania

[734] ENISA, *Privacy and data protection in mobile applications. A study on the app development ecosystem and the technical implementation of GDPR*, https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications (dostęp: 15.03.2023), s. 51.
[735] Tamże, s. 51-54.
[736] EROD, *Wytyczne nr 4/2019*…, s. 15.

takiego stylu korzystania z portali społecznościowych oraz innych usług społeczeństwa informacyjnego. Podzielam podgląd komentatorów, że „istotą privacy by default jest to, by ograniczenie prywatności danej osoby lub rezygnacja z niej następowały na wyraźne żądanie osoby, której dane dotyczą”[737]. Słusznie natomiast EROD kładzie nacisk na zaplanowanie w ramach uwzględniania ochrony danych w fazie projektowania sposobu informowania dzieci o przetwarzaniu, by było ono zrozumiałe i przewidywalne[738], przeprowadzenie tzw. testu równowagi – ważenia interesów administratora i dzieci jako podmiotów danych (w przypadku oparcia przetwarzania ich danych na podstawie art. 6 ust. 1 lit. f) rozporządzenia 2016/679[739], mając na względzie brak równowagi sił), niewykorzystywanie słabości lub potrzeb podmiotów danych[740], ułatwianie dzieciom wykonania prawa sprostowania i prawa usuwania danych osobowych (a także dorosłym, jeżeli ich żądanie dotyczy danych, które były przetwarzane, gdy byli dziećmi)[741] – choć wypada zauważyć, że nie są to nowatorskie postulaty, lecz powtórzenie kwestii ujętych w rozporządzeniu 2016/679, dlatego wytyczne EROD mogą być krytykowane za zbyt dużą ogólność.

Wprowadzenie w rozporządzeniu 2016/679 obowiązku uwzględniania ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych zasługuje na aprobatę, choć moim zdaniem przepisowi art. 25 rozporządzenia 2016/679 można zarzuć zbyt dużą lakoniczność i brak podkreślenia ważkiego znaczenia tych zasad dla ochrony danych osobowych dzieci[742], nie wspominając już o uchwyceniu specyfiki ich potrzeb w kontekście korzystania z usług społeczeństwa informacyjnego. Analiza wybranych wytycznych[743] prowadzi do wniosku, że stosowanie tych zasad jest wieloaspektowe, a do wywiedzenia z nich konkretnych wymogów niezbędne jest poddanie interpretacji wszystkich zasad przetwarzania określonych w art. 5 rozporządzenia 2016/679 oraz przeanalizowanie prawdopodobieństwa i wagi ryzyka naruszenia praw lub wolności podmiotów danych. Nie będzie więc przesady w stwierdzeniu, że prawodawca

[737] D. Lubasz, K. Witkowska-Nowakowska, *Komentarz do art. 25 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 609-610.
[738] EROD, *Wytyczne nr 4/2019*…, s. 16.
[739] Tamże, s. 18.
[740] Tamże, s. 20.
[741] Tamże, s. 26.
[742] S. van der Hof, E. Lievens, *The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR*, referat wygłoszony 17.10.2017 r. na konferencji *Children and Digital Rights: Regulating Freedoms and Safeguards* w Londynie, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3107660 (dostęp: 15.03.2023), s. 10.
[743] Wytyczne dotyczące zasad *privacy* i *data protection by design* opublikowały także inne podmioty – por. Autoritat Catalana de Proteccio de Dades, *Privacy by design and privacy by default. A guide for developers*, https://apdcat.gencat.cat/web/.content/03-documentacio/documents/guiaDesenvolupadors/GUIA-PDDD_EN.pdf; Datatilsynet, *Software development with Data Protection by Design and by Default*, https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true; Commission Nationale de l'Informatique et des Libertés, *GDPR developer's guide*, https://www.cnil.fr/en/gdpr-developers-guide; Agencia Española de Protección de Datos, *A Guide to Privacy by Design*, https://www.aepd.es/es/documento/guia-privacidad-desde-diseno_en.pdf (dostęp: 15.03.2023).

stawia przed administratorem wymagające, ambitne zadanie, nie ułatwiając jego realizacji. Jak trafnie komentuje P. Fajgielski, „prawodawca unijny nie zdecydował się na przeniesienie ogólnych zasad PbD (*privacy by design* – przyp. autorki) do rozporządzenia, ograniczając się jedynie do wskazania samej koncepcji jako istotnej zasady nakładającej na administratora nowe obowiązki", a uwzględnianie przez administratora tych zasad prowadziłoby do efektywniejszego spełniania wymogów[744]. Rzetelne stosowanie się przez administratorów do obowiązków określonych w art. 25 rozporządzenia 2016/679 uważam za fundament należytej ochrony dzieci i świadczenia usług społeczeństwa informacyjnego z poszanowaniem prawa do ochrony danych osobowych. Projektowanie nowej usługi lub planowanie wprowadzanie zmian w istniejącej, np. nowej funkcjonalności, stanowią newralgiczne momenty, ponieważ jest to czas, gdy możliwe jest opracowanie i zaimplementowanie rozwiązań pozwalających na zapobieżenie zmaterializowaniu się ryzyka naruszenia praw lub wolności dzieci. Zbyt późne zorientowanie się przez administratora, że realizując biznesowy projekt pominął aspekty odnoszące się do ochrony danych osobowych, pociąga za sobą negatywne konsekwencje nie tylko dla podmiotów danych, ale też dla samego przedsiębiorcy – poprawianie usług jest zazwyczaj trudniejsze i bardziej kosztowne niż spełnienie właściwe zdefiniowanych wymagań na etapie alokowania zasobów.

1.2 Analiza ryzyka w celu doboru odpowiednich zabezpieczeń

Stosownie do art. 24 ust. 1 rozporządzenia 2016/679, obowiązkiem administratora jest wdrożenie technicznych i organizacyjnych środków w celu zgodnego z tym rozporządzeniem przetwarzania danych osobowych. Decyzja, jakie to mają być środki, należy do administratora, co jednak nie oznacza – jak trafnie orzekł Wojewódzki Sąd Administracyjny w Warszawie – że „mogą być dobierane w sposób całkowicie swobodny i dobrowolny, bez uwzględnienia stopnia ryzyka oraz charakteru chronionych danych osobowych"[745]. Przepis art. 24 ust. 1 rozporządzenia 2016/679 nakłada na administratora obowiązek uwzględnienia charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych. W przeciwieństwie do aktów wykonawczych wydanych na podstawie uodo z 1997 r. przed reformą, w przepisach rozporządzenia 2016/679 próżno szukać szczegółowych wymogów, jakie powinny być spełnione w celu ochrony, w tym zabezpieczenia danych osobowych. Stanowi to konsekwencję zmiany percepcji ochrony danych osobowych, czemu służyć ma unijna reforma, w kierunku podejścia opartego na ryzyku (*risk-based approach*) i zmiany modelu ochrony na

[744] P. Fajgielski, *Ogólne rozporządzenie*..., s. 355.
[745] Wyrok WSA w Warszawie z dnia 26 sierpnia 2020 r., sygn. II SA/Wa 2826/19, https://orzeczenia.nsa.gov.pl/doc/1156394101 (dostęp: 15.03.2023).

proaktywny oraz prewencyjny[746]. W nowym stanie prawnym to na administratorze ciąży obowiązek przeprowadzenia analizy ryzyka i zastosowania odpowiednich do niego technicznych i organizacyjnych środków bezpieczeństwa. W opinii polskiego organu nadzorczego ds. ochrony danych osobowych, „takie podejście umożliwia skoncentrowanie się na sytuacjach najwyższego ryzyka, przy jednoczesnym zachowaniu odpowiedniego poziomu ochrony, gdy to ryzyko jest niskie i nie wymaga całego instrumentarium środków przewidzianych przez rozporządzenie ogólne o ochronie danych"[747]. Prawodawca, kierując się zasadą proporcjonalności, nakłada obowiązek wdrożenia „odpowiednich" środków, a zatem nie chodzi o zabezpieczenia najlepsze i najdroższe z możliwych[748]. W art. 32 ust. 1 rozporządzenia 2016/679 – dotyczącym *stricte* bezpieczeństwa przetwarzania danych osobowych – oprócz powtórzenia czynników wymienionych w art. 24 ust. 1 rozporządzenia 2016/679, które należy wziąć pod uwagę przy doborze rozwiązań służących ochronie danych osobowych, prawodawca wskazuje konieczność uwzględnienia stanu wiedzy technicznej i kosztu wdrażania tych środków. Dodatkowo w art. 32 ust. 2 rozporządzenia 2016/679 doprecyzowano, że szacując ryzyko związane z przetwarzaniem danych osobowych, przede wszystkim powinno się skupić na ryzyku wynikającym z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób. Zachowując neutralność technologiczną[749], w art. 32 ust. 1 rozporządzenia 2016/679 wymieniono przykładowe techniczne i organizacyjne środki bezpieczeństwa: 1) pseudonimizację[750] i szyfrowanie danych osobowych; 2) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; 3) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; 4) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Decyzja o wdrożeniu tych środków, w tym o ich rodzaju – dla przykładu, w przypadku szyfrowania – o sile kryptograficznej zastosowanego algorytmu, zastosowaniu klucza

[746] Por. K. Wygoda, *Komentarz do art. 24 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.
[747] GIODO, *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku część 1*, https://archiwum.giodo.gov.pl/pl/1520282/10294 (dostęp: 15.03.2023), s. 4.
[748] Por. P. Fajgielski, *Ogólne rozporządzenie…,* s. 347.
[749] Por. motyw 15 preambuły rozporządzenia 2016/679.
[750] Zgodnie z definicją zawartą w art. 4 pkt rozporządzenia 2016/679, pseudonimizacja oznacza „przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej".

prywatnego lub publicznego, tzw. szyfrowania *end to end*[751] – lub innych rozwiązań, powinna być zatem uzależniona od wyników analizy ryzyka naruszenia praw lub wolności osób, których dane dotyczą.

Motyw 75 preambuły rozporządzenia 2016/679 wskazuje na dwa czynniki: prawdopodobieństwo i wagę ryzyka naruszenia praw lub wolności, oraz na potencjalne skutki naruszenia, które należy oceniać z perspektywy osób, których dane dotyczą: uszczerbek fizyczny, szkody majątkowe i szkody niemajątkowe. Prawodawca wymienił w nim także najbardziej doniosłe, negatywne skutki przetwarzania danych osobowych – m.in. dyskryminację, kradzież tożsamości lub oszustwo dotyczące tożsamości, stratę finansową, naruszenie dobrego imienia; okoliczności, które – jak można rozumieć wymienienie ich w omawianym motywie – ze swojej natury mogą powodować większe ryzyko dla podmiotów danych – przetwarzanie szczególnych kategorii danych osobowych, o którym mowa w art. 9 rozporządzenia 2016/679, ocenianie czynników osobowych (analizowanie lub prognozowanie upodobań, cech lub zachowań osób fizycznych) w celu tworzenia profili, przetwarzanie dużej ilości danych, wpływające na dużą liczbę osób; przetwarzanie danych osobowych osób wymagających szczególnej opieki – zaakcentowano, że dotyczy to w szczególności dzieci. Oznacza to, że fakt przetwarzania danych osobowych dzieci powinien być istotnym elementem analizy ryzyka.

Przepisy rozporządzenia 2016/679 nie definiują pojęcia „ryzyko" ani nie określają metody jego szacowania. Istnieje wiele metod analizowania ryzyka, które można podzielić na ilościowe (określa się w nich wartość konsekwencji zdarzenia i prawdopodobieństwa jego wystąpienia), jakościowe (określa się w nich konsekwencje i prawdopodobieństwo w sposób opisowy) oraz mieszane[752]. Polski organ nadzorczy ds. ochrony danych osobowych w wydanym przez siebie poradniku określa ryzyko jako „wpływ niepewności na cele", zaczerpnąwszy tę definicję z normy ISO/IEC 27005:2011, odnoszącej się do zarządzania ryzykiem w bezpieczeństwie informacji[753]. Wybór lub opracowanie metody służącej analizie ryzyka należy do administratora. Podmiot, który przetwarza dane osobowe dzieci, w ślad za treścią motywu 75 preambuły rozporządzenia 2016/679, powinien w stosowanych przez siebie procedurach analizy ryzyka uwzględnić ten

[751] Por. G. Spindler, P. Schmechel, *Personal Data and Encryption in the European General Data Protection Regulation*, „Journal of Intellectual Property, Information Technology and Electronic Commerce Law"2016, nr 2, s. 174-176.

[752] Por. B. Fischer, *Pojęcie analizy ryzyka przy przetwarzaniu danych osobowych,* [w:] G. Szpor, K. Czaplicki (red.), *Internet. Analityka danych…*, s. 370.

[753] GIODO, *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO…*, s. 6. Inne normy ISO dotyczące bezpieczeństwa informacji i ochrony prywatności również mogą być pomocne z perspektywy wdrażania zasad ochrony danych osobowych – por. M. Byczkowski, *Znaczenie norm ISO we wdrażaniu bezpieczeństwa technicznego i organizacyjnego wymaganego w RODO*, „Monitor Prawniczy" dodatek: *Wdrażanie ogólnego rozporządzenia…*, s. 17.

aspekt. Na krytykę zasługuje jednak brak odniesień do przetwarzania danych osobowych dzieci w kontekście analizy ryzyka w części normatywnej rozporządzenia 2016/679.

Ryzyko naruszenia praw lub wolności osób, których dane dotyczą powinno znajdować się w centrum zainteresowania podmiotu przeprowadzającego analizę. Przepisy rozporządzenia 2016/679 nie wymieniają, o jakie prawa lub wolności chodzi. W świetle art. 1 ust. 2 rozporządzenia 2016/679 nie ulega jednak wątpliwości, że należy interpretować je szeroko – prawodawca odwołał się do pojęcia praw podstawowych wskazując, że rozporządzenie 2016/679 chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych. W motywie preambuły rozporządzenia 2016/679 wyjaśniono, że nie narusza ono praw podstawowych, wolności i zasad uznanych w KPP, zapisanych w unijnych traktatach, zaś w motywie 73 wskazano uprawnienia podmiotów danych, o których mowa w art. 15-22 rozporządzenia 2016/679 z zastrzeżeniem, że ich ewentualne ograniczenia mogą być wprowadzane wyłącznie, jeśli są zgodnie z wymogami KPP i EKPCZ. W ten sposób prawodawca wskazał źródła prawa, w których określono prawa i wolności osób fizycznych, lecz nie jest to katalog zamknięty – należy zważać także na prawo konstytucyjne państw członkowskich UE[754]. Badanie wpływu przetwarzania danych osobowych na różne prawa i wolności, nie tylko prawa do ochrony danych osobowych czy prawa do prywatności, zasługuje na aprobatę, ponieważ naruszenia w tych dwóch obszarach mogą istotnie wpływać na inne. Oprócz doboru odpowiednich technicznych i organizacyjnych środków bezpieczeństwa, celem przeprowadzenia analizy ryzyka jest ustalenie, czy na administratorze ciąży dodatkowo obowiązek dokonania oceny skutków przetwarzania danych i skonsultowania planowanych operacji przetwarzania z organem nadzorczym ds. ochrony danych osobowych.

Należy zauważyć, że na niektórych podmiotach świadczących usługi społeczeństwa informacyjnego – dostawcach bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych[755] – będą ciążyć dodatkowe obowiązki związane z oceną ryzyka naruszenia praw podstawowych, między innymi prawa do ochrony danych osobowych (art. 8 KPP) i praw dziecka (art. 24 KPP). Wynika to z art. 34 rozporządzenia 2022/2065. Zgodnie z tym przepisem, podmioty te będą miały obowiązek przeprowadzać analizę ryzyka występowania tzw. ryzyka systemowego co najmniej raz w roku, chyba że wprowadzają nowe funkcje. Badając prawdopodobieństwo i wagę ryzyka systemowego, dostawcy usług będą musieli zwracać uwagę na to, czy nie przyczyniają się do jego wystąpienia czynniki takie jak projekt systemów

[754] Por. A. Krasuski, *Ryzyko naruszenia praw lub wolności osób fizycznych*, [w:] A. Krasuski, P. Siembida, *Analiza ryzyka w ochronie danych osobowych*, Warszawa 2022, s. 91-92.
[755] Przez „bardzo duże platformy internetowe" i „bardzo duże wyszukiwarki internetowe" należy rozumieć te, których średnia liczba aktywnych odbiorców w UE w ciągu miesiąca wynosi co najmniej 45 milionów i w stosunku do których KE wydała decyzję w trybie przewidzianym w art. 33 rozporządzenia 2022/2065.

rekomendacji, algorytmicznych[756], moderowania treści, warunki korzystania z usług, systemy wyboru i prezentowania reklam, praktyki związane z danymi. W art. 35 ust. 1 rozporządzenia 2022/2065 prawodawca wymienił przykładowe działania służące zmniejszeniu ryzyka, do których zaliczył dążenia do wzmocnienia ochrony praw dziecka, w tym wdrożenia mechanizmów służących weryfikacji wieku i możliwości sprawowani kontroli rodzicielskiej a także rozwiązania, które mają pomagać dzieciom w sygnalizowaniu oraz uzyskiwaniu wsparcia w przypadku „niegodziwego traktowania"[757]. Przepisy rozporządzenia 2022/2065 dotyczące analizy ryzyka z pewnością będą nastręczały trudności interpretacyjnych, zwłaszcza w pierwszych latach ich stosowania, jednak w porównaniu do analogicznych regulacji zwartych w rozporządzeniu 2016/679 są bardziej szczegółowe – prawodawca, wskazując główne obszary ryzyka systemowego i środki służące jego mitygowaniu, bezpośrednio odniósł się do zagadnienia ochrony dzieci, co może pozytywnie wpłynąć na respektowanie ich praw. Wydaje się, że w obliczu braku szczegółowych regulacji w zakresie sposobu prowadzenia analizy ryzyka, o której mowa w rozporządzeniu 2022/2065, w gestii administratora leży to, czy dokona jej w ramach ogólnej analizy ryzyka lub oceny skutków na podstawie rozporządzenia 2016/679, czy też potraktuje to jako odrębne działanie.

1.3 Ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym

Zgodnie z art. 35 ust. 1 rozporządzenia 2016/679, w przypadku przetwarzania danych osobowych, które z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, wymagane jest uprzednie dokonanie przez administratora oceny skutków dla ochrony danych. Przepis art. 35 ust. 7 rozporządzenia 2016/679 określa minimalny zakres oceny skutków, na którą powinny składać się systematyczny opis operacji i celów przetwarzania danych osobowych, w tym opis prawnie uzasadnionych interesów realizowanych przez administratora (co wskazuje na sytuację, w której przetwarzanie byłoby oparte na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679), ocena niezbędności i proporcjonalności przetwarzania w świetle jego celów, ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą, wskazanie środków służących zaradzeniu ryzyku, które powinny obejmować środki służące zapewnieniu bezpieczeństwa danych. Jak słusznie zauważono

[756] Na temat relacji oceny skutków stosowania algorytmów (*algorithmic impact assessment*) i oceny skutków dla ochrony danych prowadzonej na podstawie art. 35 rozporządzenia 2016/679 por. M. Kaminski, G. Malgieri, *Algorithmic impact assessments under the GDPR: producing multi-layered explanations*, „International Data Privacy Law" 2021, Vol. 2, nr 2.

[757] Pojęcie „niegodziwego traktowania" nie zostało zdefiniowane w przepisach rozporządzenia 2022/2065, wielokrotnie występuje w motywach jego preambuły zwłaszcza w kontekście wykorzystywania dzieci do celów seksualnych. Wydaje się, że należy traktować je jako klauzulę generalną i interpretować w konkretnym stanie faktycznym.

w literaturze, w celu wykazania niezbędności i proporcjonalności przetwarzania administrator powinien sprawdzić, czy planowane przetwarzanie danych osobowych jest zgodne z zasadami wynikającymi z art. 5 rozporządzenia 2016/679, w szczególności czy istnieje podstawa prawna umożliwiająca przetwarzanie i czy czas przechowywania danych oraz cele ich wykorzystywania są określane z uwzględnieniem wytycznych zawartych w motywie 39 preambuły rozporządzenia 2016/679[758]. Prawodawca podkreślił w nim konieczność „zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu". W ramach oceny skutków administrator powinien zatem poddać analizie, czy i w jakim zakresie przetwarzania danych osobowych można uniknąć, przykładowo osiągając założony cel bez zbierania danych osobowych lub, w razie ich przetwarzania, możliwie jak najbardziej skrócić ten czas i dane usuwać lub je anonimizować.

W przeciwieństwie do „ogólnej" analizy ryzyka, dokonanie oceny skutków nie jest obligatoryjne w każdym przypadku[759]. Przesłanki dokonania oceny skutków zostały określone w art. 35 ust. 3 rozporządzenia 2016/679 oraz w wydanym na podstawie art. 35 ust. 4 rozporządzenia 2016/679 komunikacie Prezesa UODO z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony[760]. Warto podkreślić, że żadne z tych źródeł nie zawiera zamkniętego katalogu okoliczności, które powodują powstanie obowiązku dokonania oceny skutków.

W przypadku przesłanek wynikających z rozporządzenia 2016/679, w kontekście świadczenia usług społeczeństwa informacyjnego potencjalnie może mieć zastosowanie art. 35 ust. 3 lit. a) i b) rozporządzenia 2016/679, które odnoszą się odpowiednio do: 1) prowadzenia systematycznej, kompleksowej oceny czynników osobowych opierającej się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i będącej podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną; 2) przetwarzania na dużą skalę szczególnych kategorii danych osobowych[761] lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych[762]. O spełnieniu pierwszej przesłanki można mówić w przypadku przetwarzania danych osobowych, o którym mowa w art. 22

[758] A. Yordanov, *Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation,* „European Data Protection Law Review" 2017, nr 4, s. 492.
[759] Grupa Robocza Art. 29, *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679*, przyjęte 4 kwietnia 2017 r., WP 248 rev.01, s. 5.
[760] M.P. z 2019 r. poz. 666, dalej jako: „komunikat Prezesa UODO".
[761] Art. 9 ust. 1 rozporządzenia 2016/679.
[762] Art. 10 rozporządzenia 2016/679.

rozporządzenia 2016/679, w sposób „systematyczny", czyli regularny (lub uporządkowany), zaś ocena będąca jego wynikiem powinna być „kompleksowa" – przez co można rozumieć ocenę całościową, a nie cząstkową[763]. Profilowanie jest często dokonywaną przez podmioty świadczące usługi społeczeństwa informacyjnego operacją przetwarzania danych osobowych, wątpliwości może jednak wzbudzać to, czy zawsze towarzyszy temu zautomatyzowane podejmowanie decyzji mającej istotne skutki dla osób, których dane dotyczą – brak tego elementu znacząco zawęża zmaterializowanie się przesłanki dokonania oceny skutków, o której mowa w art. 35 ust. 3 lit. a) rozporządzenia 2016/679. Druga z omawianych przesłanek odnosi się do przetwarzania na dużą skalę danych osobowych, które prawodawca uznał za wymagające szczególnej ochrony.

W celu oceny, czy przetwarzanie danych osobowych odbywa się na „dużą skalę", Grupa Robocza Art. 29 zaleca wzięcie pod uwagę kilku czynników: liczbę osób, których dane dotyczą, ilość lub zakres danych, czas trwania przetwarzania, zasięg geograficzny, a jako przykład przetwarzania na dużą skalę podaje m.in. wykorzystywanie danych na potrzeby reklamy behawioralnej w kontekście działania wyszukiwarek internetowych[764]. W motywie 91 preambuły rozporządzenia 2016/679 prawodawca wskazał, że operacje przetwarzania „o dużej skali" to takie, „które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko, (…) na przykład gdy zgodnie ze stanem wiedzy technicznej stosowana jest na dużą skalę nowa technologia (…)". W przypadku usług społeczeństwa informacyjnego ta przesłanka potencjalnie mogłaby mieć zastosowanie do przetwarzania danych osobowych użytkowników portalu, poprzez który pozyskiwane są informacje o ich preferencjach lub cechach, należące do szczególnych kategorii danych osobowych – na przykład dotyczące stanu zdrowia, światopoglądu, orientacji seksualnej.

Jeśli chodzi o przesłanki obligujące administratora, który świadczy usługę społeczeństwa informacyjnego, do dokonania oceny skutków wynikające z komunikatu Prezesa UODO, należy zwrócić uwagę na kryteria – rodzaje operacji przetwarzania polegające na: 1) ewaluacji, w tym profilowaniu i prowadzeniu analizy behawioralnej „w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych", czego przykładem jest profilowanie użytkowników portali społecznościowych w celu wysyłania im informacji handlowej[765]; 2) podejmowaniu decyzji, które wywołują istotne skutki dla osoby fizycznej, w sposób zautomatyzowany, czego przykładem jest profilowanie w ramach programów

[763] Por. P. Fajgielski, *Ogólne rozporządzenie…,* s. 441.
[764] Grupa Robocza Art. 29, *Wytyczne dotyczące inspektorów ochrony danych („DPO")* przyjęte 13 grudnia 2016 r., WP243, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-officer_pl (dostęp:15.03.2023), s. 25.
[765] Punkt 1 załącznika do komunikatu Prezesa UODO.

marketingowych i monitorowanie preferencji związanych z zakupami[766]; 3) systematycznym monitorowaniu miejsc dostępnych publicznie, jeśli stosowane jest rozpoznawanie cech znajdujących się w nich obiektów, czego przykładem jest przetwarzanie, w tym przesyłanie, danych osobowych z wykorzystaniem urządzeń IoT takich jak opaski medyczne lub smartwache[767]; 4) pozyskiwaniu danych osobowych, o których mowa w art. 9 i 10 rozporządzenia 2016/679, poprzez aplikacje służące do obsługi elektronicznych czytników książek, gazet, czego przykładem są aplikacje typu *life-logging*[768]; 5) przetwarzaniu danych biometrycznych w celu identyfikacji osoby fizycznej, czego przykładem jest weryfikacja tożsamości przy wykorzystaniu takich danych w aplikacjach, urządzeniach; 6) przetwarzanie danych osobowych na dużą skalę, czego przykładem jest funkcjonowanie portali społecznościowych, serwisów umożliwiających oglądanie filmów w modelu subskrypcyjnym[769]; 7) analizie danych osobowych pochodzących z różnych źródeł w celu profilowania, czego przykładem jest także są portale społecznościowe[770]; 8) przetwarzanie danych geolokalizacyjnych, powstających w związku z korzystaniem z urządzeń IoT, w tym jako metadanych[771].

Każdy z powyższych przykładów może dotyczyć przetwarzania danych osobowych dzieci, ale tylko jeden – znajdujący się w punkcie 10 załącznika do komunikatu Prezesa UODO – dotyczy bezpośrednio ich, ponieważ mowa w nim o usługach i interaktywnych zabawkach dla dzieci. Niektóre usługi i zabawki, mimo że stworzone z myślą o najmłodszych, niosą poważne zagrożenia dla ochrony danych osobowych dzieci, a nawet ingerują w prywatność ich rodzin. Można przypuszczać, że intencją Prezesa UODO było ujęcie w wykazie zabawek połączonych z internetem, które – w ślad za pojęciem „internetu rzeczy" (*IoT*) – określa się mianem „internetu zabawek" (*Internet of Toys*, również skrótowiec *IoT*). Można do nich zaliczyć urządzenia, które

[766] Punkt 2 załącznika do komunikatu Prezesa UODO.

[767] Punkt 3 załącznika do komunikatu Prezesa UODO. Wątpliwości może budzić, dlaczego w ocenie organu nadzorczego korzystanie z urządzeń IoT – w omawianym punkcie podano przykłady tzw. technologii ubieralnych – podpada pod monitorowanie miejsc dostępnych publicznie, które powszechnie kojarzone jest przede wszystkim z miejskim monitoringiem wizyjnym, a wspomniane urządzenia mogą być używane w domu lub innym miejscu, niebędącym miejscem publicznym.

[768] Punkt 4 załącznika do komunikatu Prezesa UODO. W dokumencie nie wyjaśniono pojęcia *life-logging*. Można je rozumieć jako zbieranie informacji o życiu i aktywnościach danej osoby, pozyskanych z różnych źródeł, w tym używanych przez nią urządzeń, aplikacji (np. o prowadzonej korespondencji e-mail, nawykach dotyczących słuchania muzyki, listy słuchanych utworów, historii wyszukiwania i pobierania plików przez wyszukiwarkę internetową, zdjęć, notatek, danych o położeniu, przemieszczaniu się – danych geolokalizacyjnych) – por. szerzej na ten temat K. O'Hara, M. M. Tuffield, N. Shadbolt, *Lifelogging: Privacy and Empowerment with Memories for Life*, „Identity in the Information Society" 2009, nr 1, s. 155-172. W 2012 roku szwedzka firma stworzyła urządzenie wielkości znaczka pocztowego, które przypina się do ubrania. Urządzenie wykonuje zdjęcie co 30 sekund, co ma zapewnić udokumentowanie wszystkich zdarzeń z życia właściciela (Puls Biznesu, *Lifelog, czyli zarejestruj całe swoje życie*, https://www.pb.pl/lifelog-czyli-zarejestruj-cale-swoje-zycie-715844, dostęp: 15.03.2023). Produkt nie odniósł komercyjnego sukcesu m.in. z powodu obaw użytkowników o prywatność i firma zakończyła działalność w 2016 r. (BBC, *Shutter falls on life-logging camera start-up Narrative*, https://www.bbc.com/news/technology-37497900, dostęp: 15.03.2023).

[769] Punkt 7 załącznika do komunikatu Prezesa UODO.

[770] Punkt 8 załącznika do komunikatu Prezesa UODO.

[771] Punkt 10 i 12 załącznika do komunikatu Prezesa UODO.

są połączone z internetem i wyposażone przykładowo w kamerę, mikrofon, czujniki, oprogramowanie pozwalające na rozpoznawanie głosu, obrazu, nagrywanie i przechowywanie na serwerach (w tzw. chmurze), sterowanie przez aplikację na smartfonie[772]. Takie zabawki mogą monitorować stan zdrowia dziecka, rejestrować zachowania, a więc korzystanie z pozornie zwykłego przedmiotu może oznaczać przetwarzanie szerokiego zakresu danych osobowych, także należących do szczególnych kategorii w rozumieniu art. 9 ust. 1 rozporządzenia 2016/679. Oprócz wątpliwości natury prawnej i etycznej, czy tak daleka ingerencja w prywatność powinna być dopuszczalna, istotne są również aspekty bezpieczeństwa zgromadzonych informacji i danych osobowych. W przeszłości było to przedmiotem debaty, zwłaszcza w Niemczech, w związku z lalką *My Friend Cayla*, która została wycofana z rynku m.in. z powodu niewystarczających zabezpieczeń połączenia Bluetooth, co umożliwiało nawiązanie kontaktu z lalką przez osoby trzecie[773]. Obowiązek przeprowadzenia oceny skutków w przypadku interaktywnych zabawek połączonych z internetem można wywieść także z wytycznych Grupy Roboczej Art. 29, w których pojawiły się dwa relewantne kryteria – przetwarzanie danych w ramach tzw. internetu rzeczy i przetwarzanie danych osób wymagających szczególnej opieki, a zatem dzieci[774].

Przesłanki obligujące administratora do przeprowadzenia oceny skutków w związku z planowanym przetwarzaniem tak wielu danych osobowych dotyczących dzieci z wykorzystaniem nowych technologii nie powinny moim zdaniem wynikać wyłącznie z wytycznych organów nadzorczych ds. ochrony danych osobowych, lecz stosowny wymóg powinien mieć swoje źródło bezpośrednio w akcie prawnym – art. 35 rozporządzenia 2016/679. Dzięki temu istnienie obowiązku oceny skutków w powyższych okolicznościach nie budziłoby wątpliwości interpretacyjnych – taki obowiązek nie konkretyzowałby się tylko w przypadku uznania przez administratora, że zachodzi wysokie ryzyko naruszenia praw lub wolności dzieci na podstawie ogólnej analizy ryzyka lub analizy kryteriów znajdujących się w wytycznych. Przeprowadzenie oceny skutków „polega w znacznym stopniu na przewidywaniu wszystkich niekorzystnych skutków danej operacji dla interesów podmiotów danych”[775], dlatego powinno mieć szczególne znacznie dla ochrony praw dzieci – dzięki rzetelnie dokonanej ocenie możliwe jest uniknięcie zmaterializowania się zagrożeń, których skutki w warunkach świadczenia usług społeczeństwa

[772] G. Mascheroni, D. Holloway, *Introducing the Internet of Toys,* [w:] G. Mascheroni, D. Holloway (red.), *The Internet of Toys. Practices, Affordances and the Political Economy of Children's Smart Plays*, Cham 2019, s. 2.

[773] Por. odpowiedź KE z dnia 22 marca 2017 r. na pytanie nr E-001901-17, https://www.europarl.europa.eu/doceo/document/E-8-2017-001901_EN.html (dostęp: 15.03.2023); Reuters, *Germany bans talking doll Cayla, citing security risk, https://www.reuters.com/article/us-germany-cyber-dolls-idUSKBN15W20Q* (dostęp: 15.03.2023).

[774] I. Milkaite, E. Lievens, *The Internet of Toys: Playing Games with Children's Data?,* [w:] G. Mascheroni, D. Holloway (red.), *The Internet of Toys…,* s. 296.

[775] A. Mednis, *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych*, „Monitor Prawniczy” dodatek: *Ogólne rozporządzenie o ochronie danych...*, s. 32.

informacyjnego są trudne lub niemożliwe do odwrócenia. Ponadto sprzyjałoby to spójnemu stosowaniu rozporządzenia 2016/679 w UE i zapewnieniu podobnego, wysokiego poziomu ochrony danych osobowych dzieci we wszystkich państwach członkowskich. W obecnym stanie prawnym, na podstawie art. 35 ust. 4 rozporządzenia 2016/679, organ nadzorczy w każdym państwie opracowuje własny wykaz, który co do zasady oddziałuje „lokalnie”[776]. W opinii EROD wykazy nie muszą być identyczne – stwarzają bowiem możliwość uchwycenia „kontekstu krajowego lub regionalnego i powinny uwzględniać ustawodawstwo lokalne”[777]. O ile Prezes UODO w swoim wykazie uwzględnił operacje przewarzania danych osobowych dzieci związku z oferowaniem im interaktywnych zabawek i usług, nie oznacza to, że podobne rozwiązania znalazły się w wykazach innych organów. Celem wykazów krajowych organów nadzorczych nie powinno być więc rozwiązywanie problemów systemowych, czy też uzupełnianie swoistych luk, w sytuacji gdy zagrożenia wymagające od administratorów pogłębionej analizy występuje powszechnie, a nie tylko lokalnie.

Jeżeli w rezultacie przeprowadzenia oceny skutków dla ochrony danych okaże się, że przetwarzanie wiązałoby się z wysokim ryzykiem, gdyby nie zostały wdrożone minimalizujące je środki, zgodnie z art. 36 ust. 1 rozporządzenia 2016/679 administrator ma obowiązek skonsultować się organem nadzorczym, przedkładając mu ocenę skutków oraz informacje wskazane w art. 36 ust. 3 rozporządzenia 2016/679. Przyczyny niewdrożenia środków minimalizujących ryzyko mogą być różne, przykładowym powodem może być niewiedza[778]. W motywie 94 preambuły rozporządzenia 2016/679 mowa o opinii administratora, „że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia”, co sugeruje przyczyny o podłożu biznesowym oraz finansowym, z kolei w wytycznych Grupy Roboczej Art. 29 wyjaśniono ogólnie, że chodzi o sytuacje, gdy poziom ryzyka szczątkowego jest wysoki. Obowiązek konsultacji z organem nadzorczym istnieje, jeśli mimo występowania takiego ryzyka administrator nie odstępuje od zamiaru rozpoczęcia planowanego przetwarzania i poszukuje rozwiązania, które pozwoli uczynić to bezpiecznie i zgodnie z prawem. W odpowiedzi na wniosek o konsultacje organ nadzorczy może udzielić administratorowi

[776] Zgodnie z art. 35 ust. 6 rozporządzenia 2016/679, jeśli czynności przetwarzania wskazane w opracowanym przez dany organ nadzorczy wykazie są związane z: 1) oferowaniem towarów lub usług osobom, których dane dotyczą; 2) monitorowaniem ich zachowania w kilku państwach członkowskich; 3) wpływem na swobodny przepływ danych osobowych w UE – przed przyjęciem wykazu organ nadzorczy powinien zastosować tzw. mechanizm spójności, o którym mowa w art. 63 i nast. rozporządzenia 2016/679. W przypadku opracowania wykazu operacji przetwarzania podlegających ocenie skutków, w myśl art. 64 ust. 1 lit. a) rozporządzenia 2016/679, opinię w jego przedmiocie wydaje EROD.

[777] EROD, *Opinia nr 17/2018 w sprawie projektu wykazu sporządzonego przez właściwy polski organ nadzorczy dotyczącego rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych (art. 35 ust. 4 RODO)*, przyjęta 25 września 2018 r., https://edpb.europa.eu/sites/default/files/files/file1/2018-09-25-opinion_2018_art._64_pl_sas_dpia_list_pl.pdf (dostęp: 15.03.2023), s. 3.

[778] Por. P. Fajgielski, *Ogólne rozporządzenie…,* s. 450.

pisemnych zaleceń lub skorzystać z innych uprawnień. Wprowadzenie instytucji uprzednich konsultacji jest konsekwencją zmiany podejścia do ochrony danych osobowych – przekonania, że identyfikacja zagrożeń i dobór adekwatnych środków ochrony jest obowiązkiem administratora, a także dostrzeżeniem potrzeby szczegółowej analizy skomplikowanych procesów przetwarzania danych osobowych. D. Krajewska-Kekusz określa uprzednie konsultacje jako „dialog między administratorem a organem nadzorczym, prowadzący do celu, jakim jest wyeliminowanie zagrożeń praw i wolności osób, których dane dotyczą”[779]. Tak rozumiana instytucja uprzednich konsultacji mogłaby stanowić ważny mechanizm przyczyniający się do wzmocnienia poziomu ochrony danych osobowych dzieci w związku ze świadczeniem usług społeczeństwa informacyjnego powodujących wysokie ryzyko naruszenia praw lub wolności. Dotychczas jednak praktyczne znaczenie uprzednich konsultacji jest znikome – w latach 2018-2021 do Prezesa UODO wpłynęły nieliczne wnioski z konsultacje, a z informacji zawartych w sprawozdaniach organu nadzorczego wynika, że tylko jeden z nich potencjalnie dotyczył przetwarzania danych osobowych dzieci. W przypadku wspomnianego wniosku organ wskazał, że z jego treści „nie wynikało też, czy wnioskodawca uwzględnił wszystkie kategorie osób, do których może być adresowana usługa, ani w jaki sposób będzie weryfikowany wiek osób. Organ nadzorczy podkreślił, że RODO przewiduje szczególne rozwiązania związane z zabezpieczeniem praw dzieci” [780]. Oznacza to, że procedura uprzednich konsultacji może mieć także walor edukacyjny, uświadamiający administratorów w zakresie ciążących na nich obowiązkach i prawach osób, których dane dotyczą.

2. Obowiązki związane z wystąpieniem naruszenia ochrony danych osobowych

2.1 Stwierdzenie naruszenia i analiza ryzyka

Zgodnie z definicją zawartą w art. 4 pkt 12 rozporządzenia 2016/679, naruszeniem ochrony danych osobowych jest „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych”. W opinii Grupy Roboczej Art. 29 naruszenie ochrony danych osobowych stanowi rodzaj incydentu bezpieczeństwa, który może polegać na naruszeniu

[779] D. Krajewska-Kekusz, *Uprzednie konsultacje: cele, warunki i przebieg (zarys problemu)*, „Informacja w administracji publicznej” 2018, nr 2, s. 9.
[780] Por. sprawozdanie z działalności Prezesa UODO w 2021 roku, https://uodo.gov.pl/pl/487/2279 (dostęp: 15.03.2023), s. 209.

poufności, dostępności, integralności danych[781]. Naruszenie ochrony danych osobowych, o którym mowa w art. 4 pkt 12 rozporządzenia 2016/679, wiąże się z naruszeniem technicznych i organizacyjnych środków bezpieczeństwa danych wdrożonych w celu zapewnienia bezpieczeństwa przetwarzania[782], dlatego należy odróżnić je od innych naruszeń przepisów o ochronie danych osobowych, np. dotyczących obowiązków informacyjnych[783]. Do przykładowych zdarzeń, które mogą skutkować naruszeniem ochrony danych osobowych, można zaliczyć nieuprawniony dostęp do baz danych spowodowany błędami oprogramowania, błędami w nadawaniu uprawnień, zagubienie lub kradzież nośnika danych, skutki działania złośliwego oprogramowania[784]. Trojany umożliwiają uzyskanie kontroli nad komputerem poprzez podszywanie się pod aplikacje i uruchamianie niepożądanych funkcji, np. oprogramowanie typu *ransomware*[785]*,* które może doprowadzić do zaszyfrowania danych, a w konsekwencji – w razie braku możliwości ich odzyskania z kopii zapasowej – do utraty danych, tzn. naruszenia dostępności. Naruszenie ochrony danych osobowych może być spowodowane także wyłudzeniem danych (np. haseł) z wykorzystaniem socjotechnik polegających na podszyciu się pod inny podmiot (*phishing*)[786]. Stwierdzenie wystąpienia naruszenia ochrony danych osobowych nie zawsze jest oczywiste i natychmiastowe, ponieważ może wymagać podjęcia wielu czynności w celu ustalenia okoliczności incydentu. Grupa Robocza Art. 29 stoi na stanowisku, że stwierdzenie naruszenia ochrony danych osobowych następuje, gdy podmiot ma wystarczającą dozę pewności co do tego, że do niego doszło – moment ten musi być określany indywidualnie, z uwzględnieniem danego przypadku[787].

Brak adekwatnej i szybkiej reakcji na naruszenie ochrony danych osobowych może nieść poważne konsekwencje dla osób, których dane dotyczą – szkody majątkowe lub niemajątkowe, np. utrata kontroli nad danymi, kradzież tożsamości, dyskryminacja – dlatego unijny prawodawca przewidział w niektórych przypadkach obowiązek zgłoszenia naruszenia organowi nadzorczemu i poinformowania o naruszeniu osób, których dane dotyczą[788]. Istnienie tych obowiązków uzależnione jest od tego, czy naruszenie skutkuje odpowiednio ryzykiem lub wysokim ryzykiem naruszenia praw lub wolności osób fizycznych. W poradniku opublikowanym przez Prezesa

[781] Grupa Robocza Art. 29, *Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679*, przyjęte 3 października 2017 r., WP250, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-personal-data-breach-notification-under_pl (dostęp:15.03.2023), s. 8.
[782] Por. B. Fischer, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda, *Komentarz do art. 4 pkt 12 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.
[783] Por. P. Fajgielski, *Ogólne rozporządzenie…,* s. 140.
[784] Sprawozdanie z działalności Prezesa UODO w 2021 roku, https://uodo.gov.pl/pl/487/2279 (dostęp: 15.03.2023), s. 181-182.
[785] W. Nowak, *Specyfika zagrożeń w cyberprzestrzeni*, [w:] C. Banasiński, M. Rojszczak (red)., *Cyberbezpieczeństwo*, Warszawa 2020, s. 106.
[786] Tamże, s. 123.
[787] Grupa Robocza Art. 29, *Wytyczne dotyczące zgłaszania naruszeń* …, s. 12 i tam podane przykłady.
[788] Motyw 85 preambuły rozporządzenia 2016/679.

UODO podkreślono, że pierwszym krokiem po wykryciu naruszenia powinno być przeprowadzenie analizy ryzyka naruszenia praw lub wolności osób, których dane dotyczą[789], choć w praktyce powinno być nim podjęcie działań w celu przerwania stanu naruszenia i ustalenie przyczyn jego wystąpienia. Przepisy art. 33 i 34 rozporządzenia 2016/679, dotyczące obowiązków administratora w przypadku wystąpienia naruszenia ochrony danych osobowych, nie określają sposobu ani nawet kryteriów, które powinny być uwzględnione w procesie analizy ryzyka. Z motywów 75 i 76 preambuły rozporządzenia 2016/679 wynika natomiast, że należy oceniać wagę oraz prawdopodobieństwo wystąpienia ryzyka odnosząc je do charakteru, zakresu, kontekstu i celów przetwarzania danych. Grupa Robocza Art. 29 zaleca uwzględnienie w analizie kryteriów: 1) rodzaju naruszenia; 2) charakteru, wrażliwości i ilości danych osobowych – słusznie kładąc nacisk na to, czy naruszenie dotyczy pojedynczych danych, czy też zestawów danych dotyczących tej samej osoby fizycznej; 3) łatwość identyfikacji osób fizycznych; 4) wagę konsekwencji dla osób, których dane dotyczą, w tym na ile są one trwałe – jak długo mogą na nią oddziaływać w przyszłości; 5) cechy szczególne osoby, której dane dotyczą – Grupa Robocza Art. 29 zwraca w tym miejscu uwagę na sytuację dzieci, w przypadku których ryzyko związane z naruszeniem może być większe i administrator dokonujący analizy powinien na to zważać; 6) cechy szczególne samego administratora, gdy z racji realizowanych zadań przetwarzanie może powodować większe ryzyko, np. w przypadku podmiotów prowadzących działalność leczniczą i przetwarzających dane pacjentów; 7) liczba osób, których danych dotyczy naruszenie[790]. Te kryteria występują w metodzie opracowanej przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)[791], którą Grupa Robocza Art. 29[792], a w ślad za nią Prezes UODO[793], wskazuje jako przykładową, możliwą do stosowania. W tej metodzie okoliczność, że naruszenie ochrony danych osobowych dotyczy dzieci, akcentowana jest przy ustalaniu kontekstu przetwarzania i rodzaju danych – jeśli przetwarzane są podstawowe dane dzieci, a naruszenie może wpływać na ich bezpieczeństwo, stan psychiczny, zalecane jest rozważenie przypisania najwyższej oceny w czteropunktowej skali[794]. W literaturze podkreśla się, że zaletą metody opracowanej przez ENISA jest łatwość i szybkość przeprowadzenia analizy, poddaje się jednak pod wątpliwość jej obiektywność[795], ponieważ występujące w niej parametry w tym samym stanie faktycznym mogą być oceniane odmiennie

[789] UODO, *Obowiązki administratorów związane z naruszeniami ochrony danych osobowych*, https://archiwum.uodo.gov.pl/pl/134/1029 (dostęp: 15.03.2023), s. 7.
[790] Grupa Robocza Art. 29, *Wytyczne dotyczące zgłaszania naruszeń*…, s. 28-30.
[791] ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches*, https://www.enisa.europa.eu/publications/dbn-severity (dostęp: 15.03.2023).
[792] Grupa Robocza Art. 29, *Wytyczne dotyczące zgłaszania naruszeń* …, s. 30.
[793] UODO, *Obowiązki administratorów związane z naruszeniami…,* s. 16.
[794] ENISA, *Recommendations for a methodology*…, s. 9.
[795] W motywie 76 preambuły rozporządzenia rozporządzenia 2016/679 prawodawca podkreśla, że szacowanie ryzyka powinno odbywać się „na podstawie obiektywnej oceny".

przez różne osoby, np. przy szacowaniu łatwości identyfikacji osoby fizycznej na podstawie danych, których dotyczy naruszenie[796]. Wydaje się, że takie zagrożenie jest nieuniknione bez względu na sposób prowadzenia analizy ryzyka naruszenia praw lub wolności osób fizycznych oraz skutków, jakie może ze sobą pociągać, ponieważ jest to materia, która zawsze będzie w pewnym stopniu ocenna i uzależniona od wiedzy, umiejętności, a także doświadczenia, w tym życiowego, osób przeprowadzających analizę. Warto odnotować, że metoda opracowana przez ENISA powstała przed reformą ochrony danych osobowych – w 2013 r. W związku z reformą nie powstała inna, powszechnie zalecana przez europejskie organy nadzorcze ds. ochrony danych osobowych metoda, w której w ślad za celami reformy kwestia przetwarzania danych osobowych dzieci byłaby należycie uwypuklona.

Uwrażliwienie adresatów wytycznych opracowanych przez Grupę Roboczą Art. 29 na kryterium przetwarzania danych osobowych dzieci w trakcie analizy ryzyka prowadzonej po naruszeniu ochrony danych osobowych – zwrócenie uwagi na ich wyjątkową sytuację – zasługuje na pochwałę, niemniej jednak poprzestanie wyłącznie na zasygnalizowaniu tego problemu pozostawia niedosyt, podobnie jak inne wytyczne poświęcone naruszeniom ochrony danych osobowych – w sprawie ich zgłaszania organowi nadzorczemu. Wprawdzie w jednym z omawianych w nich przykładów naruszenie dotyczy danych osobowych dzieci, jednak jest to okoliczność nieistotna, ponieważ przykład ilustruje zdarzenie, które z uwagi na wcześniej wdrożone zabezpieczenia (szyfrowanie) nie powoduje ryzyka naruszenia praw lub wolności[797]. Większy walor edukacyjny miałby przykład, który prezentowałby naruszenie powodujące takie ryzyko, a ponadto różnicujący charakter i poziom ryzyka w zależności od kategorii osób, których dane dotyczą (dzieci i dorośli). Praktyczne znaczenie miałyby wytyczne, jak szacować ryzyko i jak powinien postąpić administrator w takiej sytuacji – jakie działania łagodzące skutki byłyby odpowiednie w przypadku dzieci. Obecnie, w razie naruszenia ochrony danych osobowych, które przykładowo wystąpiłoby w związku ze świadczeniem usług społeczeństwa informacyjnego i które dotyczyłoby danych osobowych dzieci (lub dzieci i dorosłych), administrator może posiłkować się ogólnymi wskazówkami, w których problematyka danych dzieci jest jedynie wzmiankowana. Nie wpływa to korzystnie ani na sytuację administratorów, ani osób, których dane dotyczą i wydanie wytycznych uzupełnionych o zagadnienia dotyczące postępowania w razie naruszenia ochrony danych osobowych dzieci lub wręcz poświęconych tylko temu zagadnieniu,

[796] P. Siembida, *Metody identyfikacji i szacowania ryzyka naruszenia praw lub wolności osób fizycznych*, [w:] A. Krasuski, P. Siembida, *Analiza ryzyka…*, s. 149.
[797] EROD, *Wytyczne 01/2021w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych* przyjęte 14 grudnia 2021 r., wersja 2.0, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_pl (dostęp: 15.03.2023), s. 27.

co poprzedziłyby konsultacje ze specjalistami (zwłaszcza z zakresu psychologii), uważam za pożądane.

2.2 Zgłoszenie naruszenia organowi nadzorczemu

W przypadku wystąpienia naruszenia ochrony danych osobowych, które powoduje ryzyko naruszenia praw lub wolności osób, których dane dotyczą, stosownie do art. 33 ust. 1 rozporządzenia 2016/679, administrator[798] ma obowiązek niezwłocznie, lecz nie później niż w ciągu 72 godzin od stwierdzenia naruszenia, zgłosić je organowi nadzorczemu ds. ochrony danych osobowych. Uzasadnienia wprowadzenia takiego obowiązku można doszukiwać się w potrzebie stworzenia mechanizmów odpowiedniego reagowania na naruszenia i ograniczania ich negatywnych skutków[799]. Prezes UODO stoi na stanowisku, że „zgłoszenia naruszenia ochrony danych osobowych pozwalają organowi nadzorczemu na właściwą reakcję mogącą ograniczyć skutki takich naruszeń, bowiem administrator ma obowiązek podjęcia skutecznych działań zapewniających ochronę osobom fizycznym i ich danym osobowym, które z jednej strony pozwolą na kontrolę skuteczności dotychczasowych rozwiązań, a z drugiej ocenę modyfikacji i usprawnień służących zapobieżeniu nieprawidłowościom analogicznym do objętych naruszeniem”[800].

Przepis art. 33 ust. 3 rozporządzenia 2016/679 określa minimalny zakres informacji, jakie powinien przekazać administrator zgłaszający naruszenie. Prawodawca zaliczył do nich: opis charakteru naruszenia (w tym określenie kategorii i przybliżonej liczby osób, których danych dotyczy naruszenie, kategorii i przybliżonej liczby wpisów danych osobowych), imię i nazwisko oraz dane kontaktowe inspektora ochrony danych (lub wskazanie innego punktu kontaktowego dla organu nadzorczego), opis potencjalnych konsekwencji naruszenia, opis środków, które zostały zastosowane lub są proponowane przez administratora, służące zaradzeniu naruszeniu, w tym ograniczeniu jego potencjalnych, niekorzystnych skutków. Dopuszczalne jest, w myśl art. 33 ust. 4 rozporządzenia 2016/679, przekazywanie powyższych informacji sukcesywnie, jeśli nie jest to możliwe w tym samym czasie. Za przykładową przyczynę późniejszego uzupełnienia

[798] Jeśli naruszenie ochrony danych osobowych wystąpiło u podmiotu przetwarzającego, nie zgłasza on tego zdarzenia bezpośrednio organowi nadzorczemu, lecz administratorowi, który powierzył mu przetwarzanie danych osobowych (art. 33 ust. 2 rozporządzenia 2016/679). Szerzej na temat roli podmiotu przetwarzającego w kontekście zgłaszania naruszeń por. M. Sakowska-Baryła, *Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu*, [w:] G. Szpor, K. Czaplicki (red.), *Internet. Przetwarzanie danych…*, s. 59-73.

[799] Por. P. Fajgielski, *Informowanie o naruszeniu ochrony danych osobowych w świetle przepisów ogólnego rozporządzenia o ochronie danych*, „Monitor Prawniczy” dodatek: *Ogólne rozporządzenie o ochronie danych...*, s. 43.

[800] Decyzja Prezesa UODO z 06.07.2022 r. w sprawie DKN.5131.34.2021, https://www.uodo.gov.pl/decyzje/DKN.5131.34.2021 (dostęp: 15.03.2023), w której organ nałożył na administratora administracyjną karę pieniężną za uchybienie ciążącym na nim na podstawie art. 33 i 34 rozporządzenia 2016/679 obowiązkom. Liczba zgłoszeń rośnie – w 2019 r. wyniosła 6039, w 2020 r. 7507, zaś w 2021 r. 12946 (sprawozdanie z działalności Prezesa UODO…, s. 176), czego przyczyną może być m.in. nakładanie kar za brak zgłoszenia.

zgłoszenia można uznać niemożność wskazania przez administratora adekwatnych sposobów zaradzenia naruszeniu ochrony danych osobowych przed zakończeniem wszystkich analiz[801].

Prezes UODO opracował formularz zgłoszenia naruszenia ochrony danych osobowych, z którego skorzystanie jest fakultatywne. Formularz zawiera punkt 4F, w którym administrator może zaznaczyć, że naruszenie ochrony danych osobowych dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku. Oprócz tego, w punkcie 7 „kategorie osób" w jednym z pól można wskazać, że zdarzenie dotyczy danych osobowych dzieci. W sprawozdaniach z działalności w latach 2018-2021[802] Prezes UODO nie informował o postępowaniach w sprawach naruszeń ochrony danych osobowych dzieci w związku ze świadczeniem usług społeczeństwa informacyjnego.

2.3 Zawiadamianie o naruszeniu osób, których dane dotyczą

W przypadku wystąpienia naruszenia ochrony danych osobowych, które powoduje wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, oprócz zgłoszenia naruszenia organowi nadzorczemu, zgodnie z art. 34 ust. 1 rozporządzenia 2016/679 administrator ma obowiązek niezwłocznie poinformować o zdarzeniu osobę, której dane dotyczą, o ile nie zostanie spełniona przynajmniej jedna przesłanka zwalniająca z tego obowiązku spośród wymienionych w ust. 3 tego przepisu. Prawodawca uznał, że zawiadomienie nie jest wymagane, o ile: 1) administrator zastosował organizacyjne i techniczne środki, dzięki którym osoba nieuprawniona nie może odczytać danych osobowych (np. dane były zaszyfrowane); 2) administrator wprowadził – już po wystąpieniu naruszenia[803] – środki eliminujące wysokie ryzyko naruszenia praw lub wolności; 3) zawiadomienie wymagałoby niewspółmiernie dużego wysiłku – wówczas administrator może poprzestać na wydaniu publicznego komunikatu lub w inny sposób przekazać informację o naruszeniu. Wobec tak sformułowanych przesłanek ocena, czy administrator jest uprawniony do odstąpienia od zawiadomienia, może okazać się dla niego bardzo problematyczna. Biorąc jednak pod uwagę różnorodność naruszeń ochrony danych osobowych, bardziej precyzyjne ujęcie tych przesłanek wydaje się niemożliwe. W literaturze zauważa się, że dzięki posłużeniu się przesłankom o charakterze niedookreślonym i ocennym, możliwe jest „efektywne dokonanie miarodajnych ustaleń w konkretnym przypadku naruszenia i środków podjętych przez administratora"[804]. W razie błędnej oceny sytuacji przez administratora, dzięki zgłoszeniu

[801] Por. W. Chomiczewski, *Komentarz do art. 33 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 715.
[802] Sprawozdania są dostępne na stronie https://uodo.gov.pl/pl/487/2279 (dostęp: 15.03.2023).
[803] Por. P. Fajgielski, *Ogólne rozporządzenie…,* s. 432.
[804] M. Sakowska-Baryła, *Komentarz do art. 34 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis.

naruszenia organowi nadzorczemu ma on sposobność interwencji polegającej na zażądaniu od administratora zawiadomienia osób, których dane dotyczą, o czym stanowi art. 34 ust. 4 rozporządzenia 2016/679.

W motywie 86 preambuły rozporządzenia 2016/679 wyjaśniono, że celem zawiadomienia osoby, której dane dotyczą, jest umożliwienie jej niezbędnych działań zapobiegawczych. Z tego względu treść zawiadomienia powinna zawierać przynajmniej informacje, o których mowa w art. 33 ust. 3 lit. b), c) i d) rozporządzenia 2016/679, tzn.: imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, opis możliwych konsekwencji naruszenia ochrony danych osobowych, środków, które administrator zastosował lub proponuje zastosować by zaradzić naruszeniu a także które służą zminimalizowaniu ewentualnych negatywnych skutków. Prezes UODO akcentuje potrzebę szczegółowego informowania o potencjalnych skutkach, np. „następstwem naruszenia Pana danych osobowych może być założenie na Pana dane osobowe konta internetowego (np. w serwisach społecznościowych), podszycie się pod inną osobę lub instytucję w celu wyłudzenia od Pani dodatkowych określonych informacji (np. danych do logowania, szczegółów karty kredytowej)", a także środkach, jakie może przedsięwziąć sama osoba, której dane dotyczą, np. „w celu zminimalizowania ewentualnych negatywnych skutków naruszenia zalecamy aby Pan/Pani skorzystał/a z możliwość założenia konta w systemie informacji kredytowej celem monitorowania prób uzyskania kredytu"[805]. Przepis art. 34 ust. 2 rozporządzenia 2016/679 nakazuje, by zawiadomienie było sformułowane jasnym i prostym językiem. Administrator powinien więc dostosować komunikat do odbiorców, biorąc pod uwagę zwłaszcza ich wiek i poziom wykształcenia[806].

Przepisy rozporządzenia 2016/679 ani motywy jego preambuły dotyczące zawiadamiania o naruszeniu ochrony danych osobowych osób, których dane dotyczą, nie odnoszą się do kwestii informowania dzieci o naruszeniu. Rodzi to szereg wątpliwości – począwszy od podstawowego pytania, kto w razie naruszenia ochrony danych osobowych dziecka powinien być o tym zawiadomiony – dziecko czy jego przedstawiciel ustawowy? Jak powinien postąpić administrator, który nie dysponuje danymi kontaktowymi przedstawiciela ustawowego dziecka? Czy w razie uznania, że o naruszeniu powinno być zawiadomione dziecko, uwzględnienie w przepisie art. 34 ust. 2 rozporządzenia 2016/679 obowiązku posługiwania się jasnym i prostym językiem wyczerpuje problematykę komunikowania się z dziećmi w sprawach naruszeń ochrony danych osobowych? Wykładnia językowa art. 34 ust. 1 rozporządzenia 2016/679 prowadzi do wniosku, że zawiadomienie powinno być skierowane do dziecka. Z drugiej strony rodzice, a w wyjątkowych

[805] UODO, *Obowiązki administratorów związane z naruszeniami…,* s. 27-28.
[806] Tamże, s. 25.

sytuacjach wyznaczony przez sąd opiekun[807], pełnią rolę przedstawicieli ustawowych dziecka. Za informowaniem przedstawicieli ustawowych przemawiają względy celowościowe zawiadamiania o naruszeniu – umożliwienie podjęcia działań w celu zapobieżenia negatywnym skutkom naruszenia. Można założyć, że osoba dorosła, działająca w interesie dziecka, z należytą powagą i troską o dobro dziecka odpowiednio zareaguje na zawiadomienie o naruszeniu. Takie stanowisko zaprezentowano w materiale informacyjnym opublikowanym na stronie internetowej UODO – wskazano w nim, że komunikat administratora adresowany jest „do rodziców albo innych opiekunów prawnych, jako osób sprawujących pieczę nad dobrami materialnymi i niematerialnymi dzieci – osób nieposiadających zdolności do czynności prawnych, a więc takich, które do czasu osiągnięcia pełnoletności nie mogą samodzielnie, w sposób skuteczny zabiegać o prawną ochronę swojego dobrostanu"[808]. Jednocześnie w tym samym materiale zacytowano wartą uwagi wypowiedź M. Młotkiewicz, naczelnik Wydziału Współpracy z Inspektorami Ochrony Danych w UODO, z której wynika potrzeba dostosowania przez administratora działań do wieku dziecka: „w przypadkach naruszeń wymagających powiadomienia osób, których zdarzenie dotyczy, rodzicom, ale też – zależnie od ich wieku – dzieciom, powinny być przekazane informacje: co się zdarzyło, jakie może to spowodować dla nich negatywne konsekwencje i jakie działania mogą oni podjąć, aby przed tymi konsekwencjami się obronić lub ograniczyć ryzyko ich wystąpienia (…). W przypadku dzieci młodszych dobrym rozwiązaniem może być skierowanie informacji jedynie do rodziców wraz z instrukcjami, w jaki sposób porozmawiać o naruszeniu z dzieckiem"[809]. W tej wypowiedzi słusznie moim zdaniem zasygnalizowano potrzebę dostosowania działań do wieku dziecka. Przyjęcie, że o naruszeniu należy zawsze informować wyłącznie przedstawiciela ustawowego, zdaje się pomijać fakt, że zgodnie z art. 8 ust. 1 rozporządzenia 2016/679 nastoletnie dziecko może samodzielnie wyrazić zgodę na przetwarzanie danych osobowych korzystając z usług społeczeństwa informacyjnego, a administrator zapewne nawet nie dysponuje danymi kontaktowymi rodzica lub opiekuna[810]. Informowanie dziecka o naruszeniu można postrzegać jako wyraz włączania go, jako podmiotu danych, w dotyczące go sprawy[811], co pomaga mu nabrać doświadczenia i wiedzy, które są potrzebne do funkcjonowania w społeczeństwie informacyjnym. Ponadto środki służące zapobieżeniu negatywnym skutkom naruszenia często polegają na określonym zachowaniu osoby, której dane dotyczą, np. na jej

[807] Por. art. 98 §1 i art. 155 §2 krio.
[808] UODO, *Dzieci mają prawo być informowane o naruszeniach, które ich dotyczą,* https://uodo.gov.pl/pl/138/1287 (dostęp: 04.01.2020).
[809] Tamże.
[810] Jeśli dziecko może zgodnie z prawem samodzielnie korzystać z usługi, przetwarzanie danych osobowych jego przedstawicieli ustawowych budziłoby wątpliwości w świetle zasad przetwarzania danych osobowych (zwłaszcza zasady ograniczenia celu i minimalizacji danych).
[811] Warto zwrócić uwagę na art. 24 ust. 1 KPP, zgodnie z którym poglądy dzieci są brane pod uwagę w sprawach, które ich dotyczą, stosownie do ich wieku i stopnia dojrzałości.

zwiększonej czujności i ostrożności wobec potencjalnych prób wyłudzenia danych osobowych, kradzieży tożsamości – co uzasadnia przekazanie stosownych zaleceń także samemu dziecku. Z drugiej strony nie wolno bagatelizować zagrożeń związanych z przekazaniem informacji o naruszeniu zbyt małemu dziecku, w formie niedostosowanej do jego możliwości poznawczych, poziomu wiedzy ogólnej i dojrzałości. Otrzymanie zawiadomienia o naruszeniu ochrony danych osobowych wywołuje stres u osób dorosłych, u dziecka może spowodować jeszcze większe obawy lub wręcz przeciwnie – informacja może zostać zignorowana, a tym samym cel zawiadomienia zniweczony. Problem informowania dzieci o naruszeniu ochrony danych osobowych i włączania je w sprawy dotyczące ich danych osobowych – co moim zdaniem jest zasadniczo właściwym kierunkiem, ponieważ sprzyja budowaniu ich świadomości w zakresie powszechnie występujących zagrożeń i przysługujących im praw – ma zatem nie tylko charakter prawny. Nieodzowne są interdyscyplinarne badania, w szczególności z udziałem psychologów i pedagogów, a następnie wprowadzenie prawnych regulacji (a przynajmniej wytycznych EROD) doprecyzowujących zasady zawiadamiania o naruszeniu ochrony danych osobowych dzieci. Byłoby to pożądane nie tylko z perspektywy wzmocnienia respektowania ich praw, lecz także z powodu sytuacji administratorów. Ze względu na wątpliwości interpretacyjne – które da się dostrzec nawet w lakonicznym materiale opublikowanym na stronie internetowej UODO – podmioty odpowiedzialne za ochronę danych osobowych działają w stanie poważnej niepewności, a ewentualne uchybienia związane z niewłaściwym postępowaniem w przypadku naruszenia ochrony danych osobowych zagrożone są odpowiedzialnością administracyjną (zwłaszcza w postaci administracyjnej kary pieniężnej) i cywilną.

3. Przekazywanie danych osobowych dziecka do państwa trzeciego

Rozdział V rozporządzenia 2016/679 reguluje zasady przekazywania (transferu)[812] danych osobowych m.in. do państw trzecich[813]. W prawie UE przez państwa trzecie rozumie się państwa, które nie należą do Europejskiego Obszaru Gospodarczego[814]. Brak przynależności określonego

[812] Pojęcia te mogą być stosowane zamiennie, określenie „transfer" wydaje się nawet bardziej trafne biorąc pod uwagę brzmienie pojęć występujących w rozdziale V rozporządzenia 2016/679 w j. angielskim – por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 522.

[813] Rozdział V dotyczy także przekazywania danych osobowych do organizacji międzynarodowych, czyli podmiotów działających na podstawie prawa międzynarodowego publicznego lub utworzonych na mocy umowy co najmniej dwóch państw (art. 4 pkt 26 rozporządzenia 2016/679). Ze względu na przedmiot niniejszej rozprawy zasadne jest skupienie uwagi wyłącznie na przekazywaniu danych osobowych do państw trzecich. Na temat ochrony danych osobowych w kontekście organizacji międzynarodowych por. C. Kuner, *The GDPR and International Organizations*, „American Journal of International Law Unbound" 2020, Vol. 114; P. Hustinx, *Data protection and international organizations: a dialogue between EU law and international law*, „International Data Privacy Law" 2021, Vol. 11, nr 2.

[814] Por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 44 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 9; EROD, *Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych*, wersja 2.0, przyjęta

państwa do EOG skutkuje przyjęciem założenia, że nie obowiązują w nim prawno-organizacyjne, pożądane standardy ochrony danych osobowych[815]. Pogląd o konieczności ograniczenia lub wręcz zakazania przekazywania danych do państw, które nie są sygnatariuszami porozumienia wyznaczającego wspólne, akceptowane przez strony normy ochrony danych, legł u podstaw kształtujących się od lat 80. XX w. rekomendacji i prawnych regulacji w dziedzinie transferów danych za granicę[816]. Ustanowienie zasad przekazywania danych osobowych do państw trzecich ma zapobiec osłabieniu ochrony praw podmiotów danych z powodu przekazania danych tam, gdzie nie występują odpowiednie mechanizmy ochrony – zwłaszcza, jeśli chodzi o transfer do państw o innej kulturze prawnej, w której prawo do ochrony danych osobowych nie jest zaliczane do praw człowieka[817]. Unijny prawodawca dostrzegł potrzebę i znaczenie transferów do państw trzecich, podkreślając w motywie 6 preambuły do rozporządzenia 2016/679, że „technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych". Ponadto w motywie 101 rozporządzenia 2016/679 zauważono, że przekazywanie danych osobowych do państw trzecich „jest niezbędnym warunkiem rozwoju handlu międzynarodowego i współpracy międzynarodowej", trafnie diagnozując uwarunkowania, które sprzyjają wzrostowi gospodarki cyfrowej. Globalizacja, prowadzenie działalności pozbawionej barier w postaci granic państw, naturalne dążenie przedsiębiorców do zmniejszania kosztów operacyjnych, a także obserwowany w UE deficyt specjalistów w dziedzinie technologii informacyjnych[818] – skutkują korzystaniem przez administratorów-dostawców usług społeczeństwa informacyjnego z usług (np. hostingu danych, wsparcia informatycznego) świadczonych przez podmioty przetwarzające z państw położonych na różnych kontynentach, np. Azji. Drugim istotnym z perspektywy tematu niniejszej rozprawy problemem jest świadczenie usług społeczeństwa informacyjnego przez podmioty prowadzące działalność w UE, a nawet posiadające siedzibę w państwie członkowskim, lecz powiązane kapitałowo i organizacyjne z podmiotami z państwa trzeciego, z związku z czym może dochodzić do ujawniania mu danych osobowych użytkowników usługi, także dzieci, jako administratorowi lub współadministratorowi.

18.06.2021 r., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_pl (dostęp: 15.03.2023), s. 29.

[815] Por. B. Marcinkowski, *Przekazywanie danych osobowych do państw trzecich. Ramy prawne i praktyka w świetle wyroków Schrems I i Schrems II*, „Monitor Prawniczy" dodatek: *Ocena i przegląd RODO…,* s. 69 i tam wskazana literatura.

[816] Por. M. Jagielski, *Prawo do ochrony…,* s. 190-198 i tam wskazane źródła.

[817] Por. D. Karwala, *Komercyjne transfery danych osobowych do państw trzecich*, Warszawa 2018, s. 27-30.

[818] Problem dotyczy przede wszystkim niewystarczającej liczby programistów – por. Europejski Urząd ds. Pracy, *Analysis of shortage and surplus occupations 2022*, https://www.ela.europa.eu/sites/default/files/2023-03/eures-labour-shortages-report-2022.pdf (dostęp:15.03.2023), s. 88.

Pojęcie przekazywania danych osobowych do państwa trzeciego nie zostało zdefiniowane w przepisach rozporządzenia 2016/679 i nastręcza wielu wątpliwości interpretacyjnych[819]. Na potrzeby niniejszej rozprawy i analizy zarysowanych wyżej, typowych dla usług społeczeństwa informacyjnego stanów faktycznych, można przyjąć, że przekazanie danych osobowych do państwa trzeciego obejmuje każdą operację przetwarzania, której „skutkiem jest ujawnienie tych danych odbiorcy będącemu w państwie trzecim"[820], np. wysłanie danych – utrwalonych na różnego rodzaju nośnikach – pocztą tradycyjną lub elektroniczną, wprowadzenie danych osobowych do bazy, z której mogą być pobrane lub do której można mieć wgląd[821], przy czym muszą być spełnione warunki przedstawione w wytycznych EROD – tzn. transfer danych osobowych do państwa trzeciego ma miejsce, gdy administrator lub podmiot przetwarzający („eksporter"), który ma obowiązek stosować przepisy rozporządzenia 2016/679, ujawnia dane osobowe innemu podmiotowi, będącemu administratorem, współadministratorem lub podmiotem przetwarzającym („importer"), znajdującemu się w państwie trzecim[822]. Zgodnie z orzeczeniem TSUE, za transfer do państwa trzeciego nie można natomiast uznać opublikowania danych osobowych na stronie internetowej, do której dostęp może mieć nieograniczony krąg osób – w wyroku z dnia 6 listopada 2003 r. w sprawie C-101/01, jeszcze na kanwie dyrektywy 95/46, Trybunał orzekł, że przekazywanie danych do państwa trzeciego „nie ma miejsca, w przypadku gdy osoba, która znajduje się w jednym z państw członkowskich, zamieszcza na stronie internetowej, przechowywanej przez dostawcę usług hostingowych mającego swoją siedzibę w tym samym państwie lub w innym państwie członkowskim, dane osobowe, czyniąc je w ten sposób dostępnymi dla każdego, kto połączy się z Internetem, w tym również dla osób, które znajdują się w państwie trzecim"[823]. Aktualność tego orzeczenia, ze względu na późniejsze rozstrzygnięcia TSUE, jest kwestionowana w literaturze[824]. Należy jednak zauważyć, że odrzucenie stanowiska o dyskwalifikacji publikacji danych osobowych w internecie – przy zachowaniu warunków ustalonych przez TSUE – jako przekazywania danych do państw trzecich, skutkowałoby absurdalną sytuacją, w której administrator nie miałby możliwości wywiązania się z obowiązków spoczywających na nim na mocy rozdziału V rozporządzenia 2016/679, a także art.

[819] Różne kierunki interpretacji, w tym w świetle orzecznictwa TSUE, przedstawiono w literaturze – por. I. Kowalczuk-Pakuła, M. Borkowski, *Co to jest transfer danych?*, [w:] M. Sakowska-Baryła (red.), *Sztuczna inteligencja…,* s. 73-93.
[820] I. Kowalczuk-Pakuła, M. Chołuj, *Przekazywanie danych do państwa trzeciego – w poszukiwaniu definicji*, „Prawo Nowych Technologii" 2021, nr 1, s. 19.
[821] Por. D. Karwala, *Komercyjne transfery…*, s. 60.
[822] EROD, *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, wersja 2.0, przyjęta 14 lutego 2023, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_pl (dostęp: 15.03.2023), s. 7.
[823] Wyrok TSUE z dnia 06.11.2003 r. w sprawie C-101/01, Göta hovrätt – Szwecja przeciwko Bodil Lindqvist.
[824] Por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 44 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 2.

13 ust. 1 lit. f) oraz art. 14 ust. 1 lit. f) rozporządzenia 2016/679, ponieważ warunkiem *sine qua non* jest oznaczenie podmiotu i państwa, do którego dane osobowe są przekazywane.

Przepisy rozdziału V rozporządzenia 2016/679 określają warunki zgodnego z prawem przekazywania danych osobowych do państw trzecich. Wśród nich można wyróżnić trzy mechanizmy zapewniające legalność transferu: 1) ogólną zasadę (art. 45 rozporządzenia 2016/679), zgodnie z którą przekazanie danych osobowych może nastąpić, jeśli KE stwierdziła, że dane państwo trzecie, terytorium lub określony sektor (lub sektory) w tym państwie trzecim zapewnia odpowiedni poziom ochrony; 2) zapewnienie odpowiedniego poziomu ochrony nastąpi dzięki zastosowaniu jednego ze wskazanych rozwiązań w art. 46 rozporządzenia 2016/679, takich jak wiążące reguły korporacyjne, zawarcie umów z wykorzystaniem standardowych klauzul ochrony danych przyjętych przez KE lub organ nadzorczy, zatwierdzony kodeks postępowania, zatwierdzony mechanizm certyfikacji; 3) jeśli żadne z tych rozwiązań nie zostanie wdrożone – wyjątkowo w szczególnych przypadkach przekazanie może nastąpić pod warunkiem spełnienia jednej z przesłanek z art. 49 rozporządzenia 2016/679[825]. Prawodawca ustanowił w ten sposób swoistą trójstopniową hierarchię, według której należy w pierwszej kolejności oprzeć transfer danych o zabezpieczenie generalne, tzn. rozstrzygnięcie KE w przedmiocie adekwatnego stopnia (poziomu) ochrony w danym państwie trzecim, a jeśli nie jest to możliwe ze względu na brak takiej decyzji – zastosować rozwiązania o charakterze indywidualnym, tzn. bazującym na zabezpieczeniach zastosowanych przez podmioty uczestniczące w przetwarzaniu danych osobowych, określone w art. 46 rozporządzenia 2016/679, a jeśli to również jest niewykonalne, sięgnąć do szczególnych rozwiązań z art. 49 rozporządzenia 2016/679 traktując je jako wyjątek[826]. Takie podejście należy przyjąć z aprobatą, ponieważ KE przed wydaniem decyzji jest zobowiązana, w myśl art. 45 ust. 2 rozporządzenia 2016/679, ocenić praworządność, poszanowanie praw człowieka i podstawowych wolności, obowiązujące regulacje prawne, fakt istnienia i funkcjonowania niezależnego organu nadzorczego ds. ochrony danych osobowych, międzynarodowe zobowiązania państwa trzeciego, w tym udział „w systemach wielostronnych lub regionalnych", przez co można rozumieć przykładowo członkostwo w Radzie Europy, bycie stroną konwencji 108. Dotychczas KE wydała decyzję stwierdzającą odpowiedni poziom ochrony danych osobowych w odniesieniu do Andory, Argentyny, Kanady (w zakresie ograniczonym rodzajem sektora), Wysp Owczych, Guernsey, Izraela, Wyspy Man, Japonii, Jersey, Nowej Zelandii, Republiki Korei, Szwajcarii, Wielkiej Brytanii oraz Urugwaju[827]. Najnowsza decyzja

[825] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 524-525.
[826] Por. P. Drobek, *Komentarz do art. 44 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 860.
[827] Lista państw wraz z odnośnikami do poszczególnych decyzji jest dostępna na stronie internetowej: KE, *Adequacy decisions*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (dostęp: 15.03.2023).

KE została wydana 10 lipca 2023 r. i dotyczy przekazania danych osobowych do Stanów Zjednoczonych – podmiotów, które przystąpiły do programu *EU-US Data Privacy Framework* (opisanego w załączniku nr 1 do decyzji) i pomyślnie przeszły certyfikację[828]. Lista państw jest więc krótka. W przypadku tych, które się na niej nie znalazły, podmiot planujący przekazanie danych osobowych musi skorzystać z innych mechanizmów. W przypadku świadczenia usług społeczeństwa informacyjnego do adekwatnych do nich rozwiązań, uwzględniając także ich doniosłe znaczenie praktyczne, zaliczyć można standardowe klauzule ochrony danych przyjęte przez KE, wiążące reguły korporacyjne[829] oraz wyjątkowe okoliczności umożlwiające legalny transfer, związane ze zgodą podmiotu danych.

Przepis art. 46 ust. 2 lit. c) rozporządzenia 2016/679 stanowi, że administrator lub podmiot przetwarzający może przekazać dane osobowe do państwa trzeciego pod warunkiem zapewnienia odpowiednich zabezpieczeń w postaci standardowych klauzul ochrony danych osobowych, przyjętych przez KE. Innymi słowy, istotą tego zabezpieczenia jest zawarcie przez „eksportera" umowy z „importerem" – podmiotem z państwa trzeciego – z wykorzystaniem postanowień zatwierdzonych przez KE, *de facto* wzoru umowy. Dzięki temu „importer" jest na podstawie umowy zobowiązany do zapewnienia ochrony danych osobowych na podobnym poziomie, jak podmiot podlegający przepisom rozporządzenia 2016/679. KE wydała decyzję wykonawczą w tej materii[830], która może mieć zastosowanie – po wybraniu stosownych modułów (postanowień) – do następujących relacji między podmiotami mającymi uczestniczyć w przetwarzaniu danych osobowych: 1) „eksporter" i „importer" są odrębnymi administratorami; 2) „eksporter" jest administratorem, a „importer" podmiotem przetwarzającym dane osobowe w jego imieniu; 3) „eksporter" i „importer" są podmiotami przetwarzającymi (w stosunku do innego podmiotu-administratora); 4) „eksporter" jest podmiotem przetwarzającym, zaś „importer" administratorem

[828] Decyzja wykonawcza KE z dnia 10 lipca 2023 r. C(2023) 4745 final, https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf (dostęp: 15.07.2023). Decyzja została wydana po tym, jak TSUE stwierdził nieważność dwóch poprzednich w wyniku skarg wniesionych przez aktywistę M. Schremsa - szerzej na ten temat por. D. Karwala, *Krajobraz po wyroku Trybunału Sprawiedliwości w sprawie programu Bezpiecznej Przystani*, „Monitor Prawniczy" 2016, nr 10; P. Głąb, *Transfer danych osobowych do Stanów Zjednoczonych po stwierdzeniu nieważności decyzji w sprawie tarczy prywatności UE–USA*, „Radca Prawny. Zeszyty Naukowe" 2021, nr 1.

[829] Na temat innych rozwiązań umożliwiających przekazywanie danych osobowych do państw trzecich, o których mowa w art. 46 ust. 2 lit. e) i f) rozporządzenia 2016/679, por. EROD, *Wytyczne 04/2021 dotyczące kodeksów postępowania jako narzędzi do przekazywania danych*, wersja 2.0, przyjęte 22 lutego 2022 r., https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_pl; EROD, *Wytyczne 07/2022 dotyczące certyfikacji jako narzędzia do przekazywania danych*, wersja 2.0, przyjęte 14 lutego 2023 r., https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_pl (dostęp: 15.03.2023).

[830] Decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, Dz. Urz. UE L 199 z dnia 07.06.2021, s. 31-61, dalej jako: „decyzja KE 2021/914".

i jednocześnie podmiotem z państwa trzeciego[831]. Standardowe klauzule ochrony danych są jednym z najczęściej wykorzystywanych instrumentów pozwalających na przekazywanie danych osobowych do państwa trzeciego, o ile transfer nie jest możliwy w myśl ogólnej zasady określonej w art. 45 rozporządzenia 2016/679[832]. Podejście do korzystania z nich jako instrumentu legalizującego transfer danych osobowych uległo zmianom po budzącym kontrowersje wyroku TSUE z dnia 16 lipca 2020 r., w którym Trybunał stwierdził, że oprócz postanowień umowy zawartej między podmiotem przekazującym dane a odbierającym, w celu oceny, czy zapewniono odpowiedni stopień ochrony, należy uwzględnić „istotne elementy składające się na jego (państwa trzeciego – przyp. autorki) system prawny" w kontekście „ewentualnego dostępu organów władzy publicznej tego państwa trzeciego do przekazywanych w ten sposób danych osobowych"[833]. Zdaniem EROD oznacza to, że „eksporter" powinien, przed podjęciem decyzji o przekazaniu danych osobowych do państwa trzeciego na podstawie art. 46 ust. 2 lit. c) rozporządzenia 2016/679, rzetelnie zbadać i ocenić obowiązujące w nim regulacje w zakresie „udostępnienia danych osobowych organom publicznym lub przyznające takim organom publicznym prawo dostępu do danych osobowych (np. dla celów egzekwowania prawa karnego, nadzoru regulacyjnego lub bezpieczeństwa narodowego)", a także przeanalizować praktyki organów publicznych państwa trzeciego, przede wszystkim w celu zweryfikowania, czy ochrona przewidziana w aktach prawnych nie jest iluzoryczna[834]. W razie stwierdzenia nieprawidłowości należy powstrzymać się od przekazania danych osobowych lub wdrożyć tzw. środki uzupełniające – jako przykłady takich zabezpieczeń natury technicznej, wraz z warunkami, jakie powinny spełniać, EROD podaje szyfrowanie, pseudonimizację, „przetwarzanie dzielone" (podział informacji w taki sposób, że żaden z podmiotów z państw trzecich, świadczących usługi na rzecz „eksportera", nie jest w stanie na podstawie posiadanych fragmentów zidentyfikować osób, których dane dotyczą)[835]. Orzeczenie TSUE oraz zalecenia EROD stawiają przed administratorami i podmiotami przetwarzającymi, którzy podlegają pod przepisy rozporządzenia 2016/679, ogromne wyzwanie, które – jak nietrudno sobie wyobrazić – może przerosnąć wielu przedsiębiorców. Jak zauważa D. Karwala, „wymóg przeprowadzenia analizy rozwiązań prawnych obowiązujących w państwie trzecim wydaje się być zbyt wygórowany, w szczególności w odniesieniu do małych i średnich przedsiębiorców" wskazując, że przeszkodą mogą być

[831] W takiej sytuacji przekazanie danych osobowych do państwa trzeciego może przykładowo polegać na „zwróceniu" danych osobowych – tak postrzegają to europejskie organy nadzorcze ds. ochrony danych osobowych – por. EROD, *Guidelines 05/2021*…, s. 20.
[832] UODO, *Standardowe klauzule ochrony danych*, https://uodo.gov.pl/pl/535/2506 (dostęp: 15.03.2023).
[833] Wyrok TSUE z dnia 16.07.2020 r. w sprawie C-311/18, Data Protection Commissioner przeciwko Facebook Ireland Ltd, Maximillian Schrems.
[834] EROD, *Zalecenia 01/2020*..., s. 16-18.
[835] Tamże, s. 32-37. EROD podaje także przykłady środków w postaci dodatkowych postanowień umownych oraz zabezpieczeń organizacyjnych.

przykładowo różnice językowe[836]. O ile dążenie do zapewnienia wysokiego poziomu ochrony danych osobowych w przypadku przekazywania danych osobowych do państw trzecich kierunkowo niewątpliwie zasługuje na pochwałę, o tyle niepokojące może być to, czy wyżej opisany, pożądany sposób realizacji tego celu nie wywoła skutku odwrotnego do zamierzonego, tzn. czy interpretacja Trybunału i unijnych organów nadzorczych ds. ochrony danych osobowych, w których przyjęto nawet bardziej rygorystyczne stanowisko niż zaprezentował TSUE[837], nie zostanie zmarginalizowana. Słusznie zauważono w literaturze, że zalecenia wydane przez EROD mają charakter tzw. *soft law*, podczas gdy decyzja wykonawcza KE określająca standardowe klauzule ochrony danych osobowych, jako jedno ze źródeł prawa wtórnego UE, ma charakter tzw. *hard law*[838] – ponadto warto podkreślić, że decyzja KE 2021/914 została wydana niemal rok po zapadnięciu wyroku TSUE w sprawie C-311/18, zatem ustalenia Trybunału musiały być wzięte pod uwagę przez prawodawcę. Obiekcje UE w sprawie transferów do państw trzecich, motywowane głównie szerokim dostępem władz publicznych i służb specjalnych do danych osobowych, wywołują sceptycyzm w wymiarze moralnym – C. Kuner podnosi, że wątpliwości może wzbudzać to, czy UE sama jest w stanie sprostać wysokim standardom i wymogom stawianym państwom trzecim, biorąc pod uwagę postanowienia traktatów odnoszące się do bezpieczeństwa narodowego oraz współpracę niektórych państw członkowskich UE ze Stanami Zjednoczonymi w dziedzinie wymiany informacji wywiadowczych[839].

Przepis art. 47 rozporządzenia 2016/679 reguluje warunki stosowania innego mechanizmu, dzięki któremu dopuszczalny jest transfer danych osobowych do państw trzecich – tzw. wiążące reguły korporacyjne, zdefiniowane w art. 4 pkt 20 rozporządzenia 2016/679 jako „polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium państwa członkowskiego, przy jednorazowym lub wielokrotnym przekazaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą". Wiążące reguły korporacyjne cieszą się zainteresowaniem dużych, międzynarodowych koncernów z rozmaitych sektorów, np. finansowego, farmaceutycznego, telekomunikacyjnego[840], mogłyby być wykorzystywane także przez działających globalnie dostawców usług społeczeństwa informacyjnego. Oparcie transferu danych osobowych na tym instrumencie jest możliwe pod

[836] D. Karwala, *Znaczenie soft law dla transferów danych osobowych do państw trzecich na przykładzie zaleceń EROD 01/2020,* „Monitor Prawniczy" dodatek: *Działania instytucji i organów…*, s. 39.
[837] Tamże, s. 38.
[838] D. Karwala, *Transfer Impact Assessment – nowy wymóg związany z międzynarodowym przekazywaniem danych osobowych*, [w:] M. Sakowska-Baryła (red.), *Sztuczna inteligencja…*, s. 105.
[839] Por. C. Kuner, *The Internet and the Global Reach of EU Law*, [w:] M. Cremona, J. Scott (red.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, Oxford 2019, s. 142.
[840] Por. M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni…*, s. 233.

warunkiem zatwierdzenia wiążących reguł korporacyjnych przez organ nadzorczy ds. ochrony danych osobowych zgodnie z tzw. mechanizmem spójności, o którym mowa w art. 63 rozporządzenia 2016/679 – tzn. w ramach współpracy organów w celu spójnego stosowania rozporządzenia 2016/679 w UE, po uzyskaniu opinii EROD[841]. Mechanizm wiążących reguł korporacyjnych ma mieszany charakter – prywatnoprawny i publicznoprawny – ponieważ na jego wdrożenie składają się dwa czynniki: opracowanie i uzgodnienie treści porozumienia w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą, a następnie zatwierdzenie przez organ nadzorczy ds. ochrony danych osobowych[842]. W art. 47 ust. 2 rozporządzenia 2016/679 prawodawca ustanowił otwarty katalog kilkunastu obszarów tematycznych, które stanowią minimalny, wymagany zakres regulacji zawartych w wiążących regułach korporacyjnych. Zgodnie z celem przyświecającym wszystkim rozwiązaniom przewidzianym w rozdziale V rozporządzenia 2016/679, zasadzającym się na dążeniu do zapewnienia odpowiedniego poziomu ochrony danych osobowych przekazywanych do państw trzecich, wiążące reguły korporacyjne w szczególności powinny normować sposób realizacji naczelnych zasad ochrony danych osobowych (art. 5 rozporządzenia 2016/679), praw podmiotów danych, w tym informowania o przetwarzaniu danych osobowych w oparciu o wiążące reguły korporacyjne oraz wnoszenia skarg, zadania inspektora ochrony danych lub innej osoby odpowiedzialnej m.in. za monitorowanie przestrzegania wiążących reguł korporacyjnych.

Najbardziej kontrowersyjne, zwłaszcza w przypadku przetwarzania danych osobowych dzieci, wydaje się zastosowanie szczególnego wyjątku pozwalającego na przekazanie danych do państwa trzeciego, o którym mowa w art. 49 ust. 1 lit. a rozporządzenia 2016/679. Przepis ten stanowi, że przekazanie danych osobowych do państwa trzeciego może nastąpić pod warunkiem wyraźnej zgody osoby, której dane dotyczą, która została poinformowana o ewentualnym ryzyku związanym z „proponowanym" przekazaniem – użycie przez prawodawcę takiego sformułowania jednoznacznie wskazuje na obowiązek uprzedniego, tzn. poprzedzonego udzielaniem zgody, ostrzeżenia o zagrożeniach[843]. Dodatkowo prawodawca doprecyzował, że chodzi o ostrzeżenie o ryzyku związanym z brakiem decyzji KE wobec państwa trzeciego, stwierdzającej odpowiedni poziom ochrony i odpowiednich zabezpieczeń, o których mowa w art. 46 ust. 2 rozporządzenia 2016/679. Pozyskanie zgody powinno spełniać wszystkie warunki jej ważności, o których mowa w art. 7 rozporządzenia 2016/679, zgoda „dorozumiana" ani udzielona po przekazaniu danych

[841] Szerzej na temat procedury i kryteriów zatwierdzania wiążących reguł korporacyjnych por. P. Drobek, *Komentarz do art. 47 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 879-886.
[842] Por. B. Marcinkowski, *Przepływy danych osobowych w międzynarodowych grupach kapitałowych*, „Monitor Prawniczy" dodatek: *Wpływ technologii i technik informatycznych…*, s. 60.
[843] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 561.

osobowych do państwa trzeciego nie czyni tej operacji przetwarzania legalną[844]. Na tym tle należy postawić pytanie, czy przekazanie do państwa trzeciego danych osobowych dziecka, przetwarzanych w związku ze świadczeniem usług społeczeństwa informacyjnego, jest dopuszczalne na podstawie wyraźnej zgody, a w przypadku odpowiedzi twierdzącej – kto może skutecznie złożyć takie oświadczenie – dziecko czy jego przedstawiciel ustawowy? Konstatując, że rozdział V rozporządzenia 2016/679 nie przewiduje szczególnych warunków transferu danych ze względu na okoliczność, że podmiotem danych jest dziecko[845], możliwe wydaje się zarysowanie dwóch linii argumentacji. W pierwszej, przy założeniu, że: 1) ogólne warunki legalności transferu danych osobowych do państw trzecich odnoszą się do przetwarzania danych osobowych wszystkich podmiotów danych, bez względu na ich wiek lub inne cechy szczególne; 2) zgoda na przetwarzanie danych osobowych stanowi jednostronną upoważniającą czynność prawną; 3) do oceny ważności czynności prawnych stosujemy przepisy kc – można sformułować wniosek, że zgodę na transfer (bez względu na kontekst, w jakim ma nastąpić) może wyrazić osoba o ograniczonej zdolności do czynności prawnych, czyli dziecko, które ukończyło trzynaście lat. Natomiast w drugiej, zakładając, że do zgody na przekazanie danych osobowych do państwa trzeciego – operacji przetwarzania powiązanej ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku – zastosowanie ma art. 8 rozporządzenia 2016/679[846], zgoda może być wyrażona na zasadach określonych w tym przepisie, tzn. przez dziecko, które ukończyło szesnaście lat, zaś w przypadku młodszej osoby jej przedstawiciel ustawowy, a jeśli zgodę wyraziła sama – powinno być to przez niego zaaprobowane. Obydwa stanowiska mogą budzić podobne, poważne zastrzeżenia. Zagrożone są bowiem dwa cele unijnej reformy dotyczącej danych osobowych: 1) ujednolicenie w UE przepisów, a tym samym poziomu ochrony w tej dziedzinie – przez to, że wariant pierwszy opiera się na przepisach krajowych – w tym wypadku rozważania opierają się na polskim kc[847], zaś w wariancie drugim występuje problem obniżenia przez niektóre państwa członkowskie granicy wieku dziecka, od którego może samodzielnie wyrazić zgodę w myśl art. 8 rozporządzenia 2016/679 – różnice są więc nieuniknione; 2) wzmocnienie poziomu ochrony praw dzieci w związku z przetwarzaniem –

[844] Por. B. Fischer, *Komentarz do art. 49 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 2; M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie…*, Legalis, *Komentarz do art. 8 rozporządzenia 2016/679,* teza 8.

[845] Ponadto warto zauważyć, że nienormatywna część rozporządzenia 2016/679, czyli preambuła, nie wyznacza kierunku interpretacji – milczy na temat pożądanego sposobu postępowania w takich sytuacjach.

[846] Na temat zasadności odwoływania się do art. 8 rozporządzenia 2016/679 na gruncie rozważań na temat art. 49 ust. 1 lit. a) rozporządzenia 2016/679 por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 561; B. Marcinkowski, *Przepływy danych osobowych…*, s. 63.

[847] Obowiązujące w państwach członkowskich UE regulacje dotyczące ograniczonej zdolności do czynności prawnych małoletnich, w tym progi wiekowe, nie są identyczne, jednak w literaturze zaproponowano możliwy kierunek harmonizacji – szerzej na ten temat por. L. Kociucki, *Zdolność do czynności prawnych w prawie europejskim – zagadnienia wybrane*, [w:] M. Andrzejewski, L. Kociucki, M. Łączkowska, A.N. Schulz (red.), *Rozprawy z zakresu prawa cywilnego. Księga Jubileuszowa Profesora Tadeusza Smyczyńskiego*, Toruń 2008, s. 32-36.

ponieważ w każdym wariancie, w zakresie jakim dziecko może zgodzić się na transfer danych samodzielnie, rodzi to wątpliwość, czy możliwe jest, by podjęło decyzję świadomie, gruntownie rozumiejąc konsekwencje i ewentualne zagrożenia. Uprzedzając o ryzyku związanym z przekazaniem danych osobowych w obliczu braku decyzji KE stwierdzającej odpowiedni poziom ochrony lub odpowiednich zabezpieczeń, o których mowa w art. 46 ust. 2 rozporządzenia 2016/679, administrator ma obowiązek sformułować taki komunikat czyniąc zadość warunkom przedstawionym w art. 12 rozporządzenia 2016/679[848], a więc informować w „przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka". Można przypuszczać, że nawet podejmując próbę przekazania ostrzeżenia w przystępny sposób, takie powiadomienie będzie trudne w odbiorze nawet dla osoby dorosłej – wydaje się to nieuniknione ze względu na poziom skomplikowania zagadnienia.

Przepisy rozdziału V rozporządzenia 2016/679 nastręczają wielu wątpliwości interpretacyjnych. Milczą na temat przetwarzania danych osobowych dzieci, w tym w związku ze świadczeniem usług społeczeństwa informacyjnego, którym ze względu na ich charakter może towarzyszyć przekazywanie danych osobowych do państw trzecich. Z pespektywy ochrony praw i wolności podmiotów danych, za najbezpieczniejszy instrument pozwalający na transfer uznać można decyzje KE stwierdzające odpowiedni poziom ochrony danych osobowych, jednak takie rozstrzygnięcia zostały wydane wobec nielicznych państw. Oznacza to konieczność sięgania przez „eksporterów" po inne rozwiązania. W przypadku zawierania umów z wykorzystaniem standardowych klauzul ochrony danych, jak i przetwarzania danych na podstawie wiążących reguł korporacyjnych, można mówić o swoistej „autoryzacji" treści tych dokumentów przez uprawniony organ – wszak standardowe klauzule, jako wzorcowe postanowienia umowne, są zatwierdzone przez KE, zaś wiążące reguły korporacyjne zapewniają jeszcze większe bezpieczeństwo dzięki zatwierdzeniu przez organ nadzorczy ds. ochrony danych osobowych ich zindywidualizowanego kształtu, dostosowanego do uwarunkowań przetwarzania w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą. Natomiast szczególny wyjątek dopuszczający przekazanie danych osobowych do państwa trzeciego na podstawie zgody, o czym mowa w art. 49 ust. 1 lit. a rozporządzenia 2016/679, wywołuje znaczące obawy i niepewność dotyczące praktycznych problemów stosowania tego przepisu w przypadku przetwarzania danych osobowych dzieci i możliwych konsekwencji – osłabienia poziomu ochrony ich praw i wolności. Próby odwoływania się do krajowych koncepcji i regulacji w dziedzinie oceny zdolności do czynności prawnych, choć niezbędne w istniejącym stanie prawnym – wobec

[848] Por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 49 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 3.

braku uregulowania przez unijnego prawodawcę węzłowych zagadnień przetwarzania danych osobowych dzieci, a w rezultacie występowania istotnych trudności interpretacyjnych – mogą przynieść niepożądane rezultaty w świetle celów unijnej reformy ochrony danych osobowych, tzn. niejednolite stosowanie przepisów rozporządzenia 2016/679 w UE. Z uwagi na ważkość problemu przekazywania danych osobowych dzieci do państw trzecich i zagrożenia związane z ewentualnym pozostawieniem tej decyzji dziecku, unijny prawodawca powinien doprecyzować w rozporządzeniu 2016/679, czy i pod jakimi warunkami przepis art. 49 ust. 1 lit. a rozporządzenia 2016/679 ma zastosowanie w odniesieniu do danych osobowych dzieci.

4. Rola inspektora ochrony danych w zapewnieniu ochrony danych osobowych dziecka

Choć korzyści ze wspierania administratora w realizacji obowiązków związanych z ochroną danych osobowych przez osobę posiadającą ekspercką wiedzę i doświadczenie w tej dziedzinie zostały dostrzeżone na długo przed unijną reformą ochrony danych osobowych, o czym świadczy istnienie prawnych regulacji dotyczących takiej funkcji[849], instytucja inspektora ochrony danych zyskała duże znaczenie pod rządami rozporządzenia 2016/679. Inspektor ochrony danych ma szczególne, wynikające z przepisów prawa kompetencje, z którymi skorelowane są ciążące na wyznaczającym go podmiocie obowiązki w zakresie stworzenia odpowiednich warunków umożliwiających inspektorowi niezależne wykonywanie zadań. Ponadto rozporządzenie 2016/679 przewiduje w określonych sytuacjach obowiązek wyznaczenia inspektora ochrony danych.

Zadania inspektora ochrony danych określa art. 39 ust. 1 rozporządzenia 2016/679. E. Bielak-Jomaa dzieli je na obowiązki informacyjno-doradcze, nadzorcze oraz komunikacyjne[850]. Inspektor ochrony danych informuje podmiot, który go wyznaczył, o spoczywających na nim obowiązkach w zakresie ochrony danych osobowych i doradza, jak należy właściwie je realizować, udziela także zaleceń dotyczących oceny skutków dla ochrony danych. W ramach działań nadzorczych monitoruje przestrzeganie rozporządzenia 2016/679 i innych regulacji, także wewnętrznych, które odnoszą się do ochrony danych osobowych – w tym monitoruje podział obowiązków, prowadzi działania zwiększające świadomość, szkolenia osób przetwarzających

[849] Uważa się, że instytucja inspektora ochrony danych wywodzi się z prawa niemieckiego – w 1977 r. została wprowadzona do niemieckiej ustawy o ochronie danych (*Bundesdatenschutzgesetz*), w ślad za nią podążały regulacje innych europejskich państw – por. M. Recio, *Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability*, „European Data Protection Law Review" 1/2017, s. 114 i tam powołana literatura. W Polsce, w wyniku nowelizacji uodo 1997 r., od 2015 r. istniała możliwość powołania administratora bezpieczeństwa informacji, do którego zadań należało przede wszystkim sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz prowadzenie związanej z tym dokumentacji (art. 36a ust. 2 uodo 1997 r.). Na temat różnic i podobieństw między administratorem bezpieczeństwa informacji a inspektorem ochrony danych por. K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań*, „Monitor Prawniczy" dodatek: *Ogólne rozporządzenie o ochronie danych...*, s. 75-81.

[850] E. Bielak-Jomaa, *Komentarz do art. 39 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO...*, s. 809.

dane osobowe i związane z tym audyty. Inspektor ochrony danych jest zatem edukatorem, popularyzatorem wiedzy i dobrych praktyk z zakresu ochrony danych osobowych – „odgrywa kluczową rolę w promowaniu kultury ochrony danych w organizacji”[851]. Z kolei do zadań o charakterze komunikacyjnym można zaliczyć pełnienie funkcji punktu kontaktowego dla organu nadzorczego oraz osób, których dane dotyczą – zgodnie z art. 38 ust. 4 rozporządzenia 2016/679, podmioty danych mogą kontaktować się z inspektorem w sprawach dotyczących przetwarzania oraz wykonywania związanych z tym swoich uprawnień. Dane kontaktowe inspektora ochrony danych są z tych względów publikowane przez podmiot wyznaczający oraz jest o nich zawiadamiany organ nadzorczy[852], a ponadto osobom, których dane dotyczą, dane kontaktowe inspektora są podawane m.in. przy okazji spełniania obowiązku informacyjnego na podstawie art. 13 lub 14 rozporządzenia 2016/679.

Inspektor ochrony danych, jak stanowi art. 37 ust. 5 rozporządzenia 2016/679, powinien być wyznaczony na podstawie swoich kwalifikacji zawodowych, przede wszystkim powinien posiadać fachową wiedzę na temat prawa i praktyk ochrony danych osobowych oraz umieć wypełniać zadania inspektora, dlatego istotne są również cechy osobowe i postawa etyczna osoby pełniącej tę funkcję[853]. Grupa Robocza Art. 29 podkreśla także przydatność znajomości sektora, w którym działa dany podmiot. Doniosłe znaczenie powinna mieć także świadomość, czyje dane osobowe podlegają przetwarzaniu – czy znajdują się wśród nich osoby zaliczane do grupy osób – jak określono w motywie 75 preambuły rozporządzenia 2016/679 – „wymagających szczególnej opieki, w szczególności dzieci”. Ze względu na akcentowaną w motywie 58 rozporządzenia 2016/679 konieczność objęcia dzieci szczególną ochroną, inspektor ochrony danych działający na rzecz podmiotu, który przetwarza dane osobowe dotyczące tej kategorii osób, wykonując swoje zadania z uwzględnieniem ryzyka związanego z operacjami przetwarzania[854], powinien brać pod uwagę specyficzne zagrożenia, sytuację dzieci i potencjalne skutki naruszeń w obszarze ochrony ich danych osobowych, które mogą być inne – bardziej dotkliwe – niż w przypadku nieprawidłowości dotyczących danych osób dorosłych. Realizując swoje zadania u podmiotu, który przetwarza dane osobowe dzieci – przykładowo monitorując przestrzeganie przez administratora zasady przejrzystości przetwarzania – inspektor ochrony danych powinien sprawdzić, czy informacje o przetwarzaniu danych osobowych kierowane do dzieci są, jak podkreślono w motywie 58 preambuły rozporządzenia 2016/679, „sformułowane tak jasnym i

[851] Grupa Robocza Art. 29, *Wytyczne dotyczące inspektorów*…, s. 15.
[852] Te obowiązki wynikają z art. 37 ust. 7 rozporządzenia 2016/679. Tryb zgłoszenia powołania, zmiany lub odwołania inspektora ochrony danych reguluje art. 10 uodo z 2018 r. Ponadto w art. 11 tej ustawy wprowadzono obowiązek udostępnienia na stronie internetowej (a jeżeli jej nie prowadzi – w miejscu prowadzenia działalności) danych inspektora obejmujących imię, nazwisko, adres poczty elektronicznej lub numer telefonu.
[853] Grupa Robocza Art. 29, *Wytyczne dotyczące inspektorów*…, s. 25.
[854] Uwzględnianie przez IOD ryzyka związanego z operacjami przetwarzania jest wymogiem wynikającym z art. 39 ust. 2 rozporządzenia 2016/679.

prostym językiem, by dziecko mogło je bez trudu zrozumieć". Doradzając podmiotowi świadczącemu dzieciom usługi społeczeństwa informacyjnego, inspektor mógłby rekomendować stosowanie określonych sposobów weryfikacji wieku dziecka lub pozyskania zgody opiekuna prawnego, dążąc do zapewnienia zgodności procesu pozyskania zgody na przetwarzanie danych osobowych w myśl art. 8 rozporządzenia 2016/679. Formułując zalecenia do oceny skutków dla ochrony danych, inspektor ochrony danych również mógłby zawrzeć w nich wytyczne w celu wzmocnienia ochrony danych osobowych dzieci. Szkoląc pracowników, inspektor może uwrażliwiać ich na potrzebę wprowadzenia dodatkowych zabezpieczeń w przypadku przetwarzania danych osobowych dzieci, uświadamiać, że dzieci są podmiotami danych, a kierowane przez nie pytania lub żądania odnoszące się do ochrony danych osobowych należy traktować z należytą powagą i odpowiednio na nie reagować, ułatwiając dzieciom możliwość wykonywania ich uprawnień związanych z przetwarzaniem. Kwalifikacje inspektora ochrony danych wykonującego tę funkcję w podmiocie, który przetwarza głównie dane osobowe dzieci, powinny w mojej ocenie obejmować rozumienie zasad przetwarzania danych osobowych określonych w art. 5 rozporządzenia 2016/679 i powiązanych z nimi obowiązków w kontekście przetwarzania danych dzieci i umiejętność wykorzystywania go w bieżącej pracy.

Wyznaczenie inspektora ochrony danych przez administratora i podmiot przetwarzający jest w wielu przypadkach obligatoryjne. Przesłankami, które potencjalnie mogą obligować podmiot świadczący usługę społeczeństwa informacyjnego do wyznaczenia IOD może być zaistnienie okoliczności wskazanych w art. 37 ust. 1 lit. b) lub c) rozporządzenia 2016/679[855], tzn. prowadzenie „głównej działalności", która polega na: 1) „operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę"; 2) „przetwarzaniu na dużą skalę" szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych. Ustanowione przez prawodawcę kryteria są nieostre, przez co mogą powodować trudności interpretacyjne. W zatwierdzonych przez EROD wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych zaproponowano interpretacje poszczególnych sformułowań użytych przez prawodawcę oraz podano przykłady sytuacji, w których istnieje konieczność powołania IOD. Przez „główną działalność" należy rozumieć „kluczowe operacje, które administrator lub podmiot przetwarzający podejmują, aby osiągnąć swoje cele" – nie są więc nimi operacje jedynie wspierające realizację pierwszoplanowych przedsięwzięć, takie jak wypłacanie wynagrodzeń pracownikom[856]. Wydaje się więc, że w

[855] Oprócz tych przesłanek, wyznaczenie IOD jest obowiązkowe w przypadku przetwarzania danych osobowych przez organy lub podmioty publiczne – por. art. 37 ust. 1 lit. a) rozporządzenia 2016/679.
[856] Grupa Robocza Art. 29, *Wytyczne dotyczące inspektorów*…, s. 24.

przypadku przedsiębiorcy za jego „główną działalność" należy uznać świadczenie usług klientom, sprzedaż towarów[857]. Ze względu na charakter i specyfikę usług społeczeństwa informacyjnego, a także naturalne dążenie usługodawców do dotarcia do jak najszerszego grona odbiorców, w przypadku tego typu usług spełnienie kryterium przetwarzania danych „na dużą skalę" jest bardzo prawdopodobne. Z podobnych powodów podmiotów świadczących usługi społeczeństwa informacyjnego może dotyczyć przesłanka „regularnego i systematycznego monitorowania osób, których dane dotyczą". Według Grupy Roboczej Art. 29, „w oczywisty sposób obejmuje ono wszystkie formy śledzenia i profilowania w internecie na potrzeby reklamy behawioralnej", choć podane przez nią przykłady świadczą o konieczności szerokiego rozumienia omawianego pojęcia – Grupa wymienia m.in. działalność marketingową opartą na danych, śledzenie lokalizacji użytkowników aplikacji mobilnych, monitorowanie samopoczucia poprzez tzw. technologie ubieralne, programy lojalnościowe, urządzenia działające w ramach IoT[858].

Wytyczne dotyczące inspektorów ochrony danych dostarczają pewnych wskazówek interpretacyjnych, słusznie jednak są krytykowane za duży poziom ogólności, znikome praktyczne znaczenie podanych w nich przykładów, wynikające z ich trywialności[859]. W zestawieniu z ogólnymi, odwołującymi się do nieostrych kryteriów przesłankami wyznaczenia IOD – których w przypadku art. 37 ust. 1 lit. b) rozporządzenia 2016/679 można wskazać pięć[860], a aby można było mówić o obowiązku wyznaczenia IOD, wszystkie powinny wystąpić kumulatywnie – ryzyko braku zaangażowania inspektora w przypadku operacji przetwarzania, które wymagałyby zaangażowania eksperta z zakresu ochrony danych osobowych, wydaje się wysokie. Zakładając, że działania inspektora ochrony danych istotnie przyczyniają się do zgodnego z prawem przetwarzania danych osobowych, a *ratio legis* nałożenia obowiązku jego wyznaczenia w określonych przypadkach, gdzie potencjalnie przetwarzanie może wywoływać negatywne skutki dla podmiotów danych, jest stosowanie dodatkowych zabezpieczeń organizacyjnych, błędna ocena stanu faktycznego a w konsekwencji niewyznaczenie inspektora może stanowić zagrożenie dla praw osób, których dane dotyczą. Należy zgodzić się z M. Sakowską-Baryłą, że choć z motywu 97 preambuły rozporządzenia 2016/679 wynika, że inspektor ochrony danych jest nie tyle rzecznikiem osób, których dane dotyczą, lecz osobą wspierającą administratora i podmiot przetwarzający, to „Znajomość prawa i praktyk po stronie IOD i rzetelne ich stosowanie można

[857] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 459.
[858] Grupa Robocza Art. 29, *Wytyczne dotyczące inspektorów…*, s. 26.
[859] Por. K. Cieniak, *Obowiązek wyznaczenia inspektora ochrony danych osobowych*, „Monitor Prawniczy" 2018, nr 16, s. 894.
[860] Tzn.: „główna działalność polega na...", „monitorowanie osób", prowadzone „regularnie" i „systematycznie", „na dużą skalę".

uznać za jedną z gwarancji praw podmiotu danych, które inspektor przy wykonywaniu swej funkcji zawsze musi brać pod uwagę”[861].

Mimo, że jednym z celów reformy ochrony danych osobowych było wzmocnienie poziomu ochrony danych osobowych dziecka, przepisy prawa ani nawet wytyczne Grupy Roboczej Art. 29 nie wymieniają przetwarzania danych osobowych dotyczących dzieci jako czynnika powodującego obowiązek wyznaczenia inspektora ochrony danych, co moim zdaniem zasługuje na krytykę. Dlatego opowiadam się za ponownym rozważeniem brzmienia art. 37 ust. 1 rozporządzenia 2016/679 i uzupełnienia go o przesłankę obligującą do powołania inspektora ochrony danych w przypadku przetwarzania danych osobowych dzieci w związku ze świadczeniem oferowanych im usług społeczeństwa informacyjnego.

5. Obowiązek wykazania przestrzegania przepisów rozporządzenia 2016/679

W myśl art. 5 ust. 2 rozporządzenia 2016/679, administrator ponosi odpowiedzialność za przestrzeganie zasad przetwarzania danych osobowych wymienionych w art. 5 ust. 1 rozporządzenia 2016/679 i musi być w stanie to wykazać – co prawodawca określił jako „rozliczalność” – ang. *accountability*. Ten wieloznaczny termin został zaczerpnięty z anglosaskiej kultury prawnej, którego esencją jest wywiązywanie się z obowiązków („wykonywanie odpowiedzialności”) i „umożliwienie stosownej weryfikacji”[862]. Wprowadzenie do rozporządzenia 2016/679 zasady rozliczalności podyktowane było dążeniem do urzeczywistnienia ochrony danych osobowych, przeniesieniem jej z „teorii do praktyki”[863]. Choć prawodawca powiązał rozliczalność z zasadami z art. 5 ust. 1 rozporządzenia 2016/679, w praktyce konieczność jej zachowania rozciąga się na wszystkie przepisy rozporządzenia 2016/679 z tego względu, że poszczególne obowiązki są skorelowane z tymi zasadami, wywodzą się z nich – przykładowo, informowanie podmiotów danych o przetwarzaniu w myśl art. 13 i art. 14 rozporządzenia 2016/679 ma swoje źródło w zasadzie przejrzystości, zatem uchybienie wskazanym przepisom powoduje jednocześnie naruszenie art. 5 ust. 1 lit. a) rozporządzenia 2016/679[864]. Zdaniem Prezesa UODO zasada rozliczalności nakłada na administratora „ciężar dowodowy, polegający na konieczności wykazania przez niego zarówno przed organem nadzorczym, jak również przed

[861] M. Sakowska-Baryła, *Wykonywanie funkcji inspektora ochrony danych – aspekty etyczne*, „Monitor Prawa Pracy” 2020, nr 12, s. 26.
[862] Grupa Robocza Art. 29, *Opinia 3/2010 w sprawie zasady rozliczalności*, przyjęta w dniu 13 lipca 2010 r., https://archiwum.giodo.gov.pl/pl/1520057/3732 (dostęp: 15.03.2023), s. 8.
[863] Tamże, s. 3.
[864] T. Kahler, *Accountability – the gravity centre of GDPR*, [w:] T. Kahler (red.), *Turning Point in Data Protection Law*, Baden-Baden 2020, s. 26.

podmiotem danych, dowodów na przestrzeganie wszystkich zasad przetwarzania danych”[865]. Rozliczalność polega zatem na paralelnym, faktycznym przestrzeganiu rozporządzenia 2016/679 i popieraniu tego dowodami, co powinno odbywać się w dwóch wymiarach: technicznym (informatycznym) oraz formalnym, rozumianym jako prowadzenie dokumentacji ochrony danych osobowych.

Warto na wstępnie wskazać, że w ogólnym ujęciu rozliczalność postrzegana jest także jako „właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi”[866]. Rozliczalność w aspekcie technicznym – w systemach informatycznych – polega przede wszystkim na możliwości: 1) zweryfikowania, czy przewidziana operacja przetwarzania danych została przeprowadzona zgodnie z założeniami (walidacja); 2) w razie wystąpienia błędu – ustalenia przyczyny, wskazania odpowiedzialnego komponentu (przypisanie); 3) rejestrowaniu informacji, które świadczą o przeprowadzeniu i wynikach działań określonych w pkt 1 i 2 (dowód). Między innymi z tego względu użytkownicy powinni posługiwać się unikalnymi identyfikatorami, których nie powinni zmieniać[867]. Rejestrowane winny być potrzebne informacje, w adekwatnym do celów zakresie – sposobem na uniknięcie przetwarzania nadmiarowych danych jest określenie ich zakresu na etapie opracowywania specyfikacji właściwości[868]. Zaniechanie prowadzenia szczegółowych dzienników zdarzeń (logów) i przechowywania ich przez odpowiedni czas, którego długość powinna być określona na podstawie wniosków z przeprowadzonej analizy ryzyka, w ocenie Prezesa UODO przesądza o naruszeniu obowiązku wdrożenia środków służących sprawnej i skutecznej identyfikacji ewentualnych naruszeń ochrony danych osobowych[869]. Prezes UODO zauważa, że „powszechnie przyjmuje się, że rozliczalność w systemach informatycznych jest realizowana w formie automatycznie generowanych zapisów (tzw. logów) zawierających określony zestaw informacji umożliwiający stwierdzenie kto, kiedy, jakie operacje, w odniesieniu do jakich danych wykonał w systemie.

---

[865] Decyzja Prezesa UODO z dnia 18 października 2019 r., ZSPU.421.3.2019, https://uodo.gov.pl/decyzje/ZSPU.421.3.2019 (dostęp: 15.03.2023). Należy podzielić stanowisko Prezesa UODO co do meritum, choć wątpliwości może budzić, czy istotnie pożądane (i konieczne) byłoby przedstawianie podmiotom danych dowodów w zakresie środków służących zabezpieczeniu danych, zwłaszcza technicznych, w celu wykazania przestrzegania zasady integralności i poufności (art. 5 ust. 2 lit. f rozporządzenia 2016/679). Ujawnienie szczegółów mogłoby wręcz zagrozić bezpieczeństwu, ponadto z art. 13, 14, 15 rozporządzenia 2016/679 nie wynika obowiązek wtajemniczania podmiotów danych w kwestie dotyczące *stricte* bezpieczeństwa przetwarzania.

[866] P. Drobek, *Komentarz do art. 5 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 340.

[867] Por. ENISA, *Privacy, Accountability and Trust – Challenges and Opportunities*, https://www.enisa.europa.eu/publications/pat-study (dostęp: 15.03.2023), s. 42.

[868] Tamże, s. 45.

[869] Por. decyzja Prezesa UODO z dnia 9 grudnia 2021 r., DKN.5130.2559.2020 r., https://www.uodo.gov.pl/decyzje/DKN.5130.2559.2020 (dostęp: 15.03.2023). W tej decyzji Prezes UODO potwierdził, że warto podążać za powszechnie znaną, dobrą praktyką służącą rozliczalności, polegającą na rejestrowaniu nazwy użytkownika, czasu dokonania operacji, jej rodzaju oraz jakich danych dotyczyła, mając jednak na względzie konieczność dostosowania zakresu tych informacji do konkretnego stanu faktycznego.

Szczegółowość zapisów logów jest kwestią indywidualną, uzależnioną od zaimplementowanych funkcjonalności oraz zadań użytkownika”[870].

Zachowaniu rozliczalności sprzyja także stosowanie systemów typu DLP (*Data Loss Prevention*), które, w zależności od rodzaju i sposobu konfiguracji, mogą zapobiegać naruszeniu poufności (np. dzięki automatycznemu blokowaniu przesyłania danych osobowych poza organizację), a w razie wystąpienia naruszenia ochrony danych osobowych mogą dostarczać nieodzownych informacji pozwalających na przeanalizowanie zdarzenia, pozyskanie dowodów przydatnych na potrzeby notyfikacji Prezesowi UODO – jak podkreślają M. Jakubik i K. Witas, „system DLP pozwala zapanować nie tylko nad poufnością danych, ale poprzez tworzenie i przechowywanie dzienników zdarzeń oraz rejestrowanie aktywności każdego użytkownika, któremu nadano dostęp, administrator zapewnia rozliczalność. W ten sposób administrator może wyciągać konsekwencje w przypadku zaistnienia naruszeń ochrony danych, co więcej może identyfikować przyczyny takich naruszeń, a nawet im zapobiegać”[871]. Stosowanie systemów typu DLP stanowi przykład technicznych rozwiązań, które może stosować administrator w celu wykazywania przestrzegania rozporządzenia 2016/679, istnieją także inne środki, temat ten jednak wykracza znacznie poza przedmiot niniejszej rozprawy i rozważania natury *stricte* prawnej.

W aspekcie formalnym – dokumentacyjnym, porównując przepisy rozporządzenia 2016/679 z przepisami uodo z 1997 r. można odnieść wrażenie, że w wyniku unijnej reformy istotnie poluzowano sztywne wymogi w zakresie prowadzenia dokumentacji ochrony danych osobowych, jednak po przeprowadzeniu wnikliwej analizy okazuje się, że jest to pozorne. Mimo braku nałożenia przez przepisy wielu obowiązków tego typu *expressis verbis*, w drodze wykładni można dojść do wniosku, że do zachowania rozliczalności niezbędne jest posiadanie i aktualizowanie licznych dokumentów. Już na etapie planowania przedsięwzięcia związanego z przetwarzaniem danych osobowych administrator powinien być w stanie wykazać, że zastosował się do art. 25 rozporządzenia 2016/679 – zasady uwzględniania ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych – w rezultacie czego wdrożył skuteczne rozwiązania, co zdaniem EROD może udowodnić dzięki dokumentacji, opisującej przyjęte przez niego wskaźniki ilościowe lub jakościowe[872]. Rada podkreśla także, że wewnętrzne polityki administratora powinny być zgodne z wymogami określonymi w art. 25 rozporządzenia 2016/679[873], co może przejawiać się w opisaniu w nich kroków, jakie powinny być podjęte przed rozpoczęciem lub zmianą procesu przetwarzania danych osobowych.

---

[870] Decyzja Prezesa UODO z dnia 21 sierpnia 2020 r., ZSOŚS.421.25.2019, https://www.uodo.gov.pl/decyzje/ZSOŚS.421.25.2019 (dostęp: 15.03.2023).
[871] M. Jakubik, K. Witas, *Systemy DLP a ochrona danych osobowych – zasada rozliczalności*, [w:] A. Gryszczyńska, G. Szpor, W.R. Wiewiórski (red.), *Internet Hacking*, Warszawa 2023, Legalis, pkt 6.
[872] EROD, *Wytyczne nr 4/2019*…, s. 8.
[873] Por. motyw 78 preambuły do rozporządzenia 2016/679.

W przypadku określania podstawy prawnej przetwarzania, warto udokumentować uzasadnienie – argumenty przemawiające za wyborem określonej przesłanki[874]. Szczególne wymogi występują, jeśli administrator przetwarza dane osobowe na podstawie zgody podmiotu danych – art. 6 ust. 1 lit. a rozporządzenia 2016/679 oraz do celów wynikających z prawnie uzasadnionych interesów – art. 6 ust. 1 lit. f rozporządzenia 2016/679. Gdy przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych (art. 7 ust. 1 rozporządzenia 2016/679). To na nim spoczywa ciężar dowiedzenia, że zgoda została udzielona, a ponadto, że zostały spełnione wszystkie warunki jej ważności, co potwierdził TSUE stwierdzając, że „do administratora danych należy wykazanie, że osoba, której dane dotyczą, poprzez czynne zachowanie wyraziła zgodę na przetwarzanie swych danych osobowych i że uprzednio uzyskała ona dotyczące wszelkich okoliczności związanych z przetwarzaniem tych danych informacje mające zrozumiałą i łatwo dostępną formę, wyrażone jasnym i prostym językiem oraz umożliwiające tej osobie łatwe ustalenie konsekwencji jej zgody, w efekcie czego uzyskuje się gwarancję, że zgoda ta została udzielona przy pełnej znajomości stanu rzeczy”[875]. Administrator powinien zatem dokumentować fakt uzyskania zgody, a potwierdzający go dowód przechowywać nie dłużej niż to konieczne, biorąc pod uwagę obiektywne kryterium, np. czas niezbędny na dochodzenie roszczeń i obronę przed nimi[876]. Informacja o udzielonej zgodzie powinna obejmować „kto udzielił zgody i jaką miała ona treść, kiedy została ona udzielona, jakie informacje otrzymał podmiot danych przy składaniu oświadczenia o wyrażeniu zgody, jakie informacje zostały udzielone o sposobie wyrażenia zgody, oraz czy zgoda została wycofana i jeśli tak, to kiedy”. EROD objaśnia, że administrator może prowadzić rejestr zgód, zaś „w kontekście internetowym administrator mógłby przechowywać informacje na temat sesji, w ramach której udzielono zgodę, wraz z dokumentacją obiegu zgody w czasie tej sesji, jak również kopię informacji przedstawionych wówczas osobie, której dane dotyczą”[877]. Oznacza to, że także spełnianie obowiązku informacyjnego, o którym mowa w art. 13 i art. 14 rozporządzenia 2016/679 wymaga należytego udokumentowania. Sytuacja administratora jest o wiele bardziej skomplikowana przy przetwarzaniu na podstawie zgody danych osobowych dzieci, korzystających z oferowanych im bezpośrednio usług społeczeństwa informacyjnego, czyli w myśl art. 8 rozporządzenia 2016/679. Trudności wynikają z obowiązku podjęcia działań w celu ustalenia wieku dziecka, zaś w niektórych przypadkach uzyskania aprobaty lub zgody

[874] Administrator ma obowiązek wykazać zasadność oparcia przetwarzania na określonej przesłance – por. decyzja Prezesa UODO z dnia 30 listopada 2022 r., DKN.5112.5.2021, https://www.uodo.gov.pl/decyzje/DKN.5112.5.2021 (dostęp: 15.03.2023).
[875] Wyrok TSUE z dnia 11.11.2020 r., C-61/19, Orange România SA.
[876] EROD, *Wytyczne 05/2020*…, s. 24.
[877] Tamże, s. 25.

przedstawiciela ustawowego. EROD podaje w wytycznych, na przykładzie internetowej platformy gier, syntetyczny opis czynności podejmowanych w tym celu, uwzględniając w nim nawiązanie kontaktu z przedstawicielem ustawowym[878]. Wprawdzie próżno szukać w tych wytycznych i rozporządzeniu 2016/679 obowiązku przyjęcia przez administratora procedury określającej stosowaną przez niego metodę sprawdzania wieku dziecka i czy przedstawiciel ustawowy wyraził lub zaaprobował zgodę, trudno jednak wyobrazić sobie możność wykazania przez niego przestrzegania właściwych przepisów rozporządzenia 2016/679, co więcej w sposób jednolity wobec wszystkich podmiotów danych, bez spisania takich zasad i zaznajomienia z nimi osób przetwarzających dane osobowe, jeśli miałyby wykonywać w związku z tym określone zadania. Natomiast decydując się na przetwarzanie danych osobowych na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679, administrator powinien przeprowadzić, a w myśl zasady rozliczalności także udokumentować, tzw. test równowagi, „którego celem jest uzyskanie bilansu ważenia ww. dóbr leżących zarówno po stronie podmiotu danych, jak i ich Administratorów. Jeżeli w rezultacie takiego testu okaże się, że cel określony przez danych Administratorów można osiągnąć w inny sposób, niż poprzez przetwarzanie danych osobowych w określony sposób i w określonym zakresie, a szczególnie gdy narusza ono prawa lub wolności podmiotu danych, należy uznać, że administrator nie ma podstaw do przetwarzania danych na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679”[879]. Przepis ten nakazuje administratorowi planującemu powołać się na określoną w nim przesłankę szczególne zwrócenie uwagi na okoliczność przetwarzania danych osobowych dzieci, co powinno znaleźć odzwierciedlenie w dokumentacji związanej z testem równowagi.

Jeśli chodzi o przepisy art. 32 i art. 35 rozporządzenia 2016/679, traktujące o zapewnieniu bezpieczeństwa, w tym o ogólnej analizie ryzyka, ocenie skutków dla ochrony danych, nie wskazują na obowiązek dokumentowania tych działań, aczkolwiek taka konieczność nie wzbudza wątpliwości w świetle zasady rozliczalności. Organ nadzorczy ds. ochrony danych osobowych prezentuje zarówno w materiałach edukacyjnych[880], jak i decyzjach administracyjnych[881] stanowisko, że analiza ryzyka powinna być przeprowadzona oraz udokumentowana w sposób pozwalający na wykazanie, że ryzyko zostało oszacowane oraz że wdrożono odpowiednie do niego środki ochrony. Udokumentowanie przeprowadzenia analizy ryzyka koresponduje z ogólną zasadą rozliczalności[882]. Dodatkowe wymagania wobec dostawców bardzo dużych platform

[878] Tamże, s. 31.
[879] Decyzja Prezesa UODO z dnia 30 listopada 2022 r., DKN.5112.5.2021, https://www.uodo.gov.pl/decyzje/DKN.5112.5.2021 (dostęp: 15.03.2023).
[880] GIODO, *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO…*, s. 11.
[881] Por. decyzja Prezesa UODO 21 sierpnia 2020 r., ZSOŚS.421.25.2019, https://www.uodo.gov.pl/decyzje/ZSOŚS.421.25.2019; decyzja Prezesa UODO z dnia 9 grudnia 2021 r., DKN.5130.2559.2020 r., https://www.uodo.gov.pl/decyzje/DKN.5130.2559.2020 (dostęp: 15.03.2023).
[882] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 349.

internetowych i bardzo dużych wyszukiwarek cyfrowych statuuje przepis art. 34 ust. 3 rozporządzenia 2022/2065, zgodnie z którym przechowują dokumenty potwierdzające odnoszące się do ocen ryzyka przez co najmniej trzy lata po ich przeprowadzeniu ocen ryzyka i na wniosek przekazują je m.in. KE.

Przepis art. 32 ust. 1 lit d rozporządzenia 2016/679 nakazuje „regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych", co może być realizowane przykładowo przez prowadzenie zewnętrznych lub wewnętrznych audytów. Za dowód przeprowadzenia audytu uważa się sprawozdanie wraz z informacjami, które zostały pozyskane w jego trakcie i stanowią podstawę ustaleń przedstawionych w raporcie, takie jak wyjaśnienia i kopie dokumentów złożone przez osoby uczestniczące w audycie, zrzuty ekranu z systemu informatycznego, notatki z przeprowadzonych czynności[883].

W kontekście oceny skutków dla ochrony danych A. Mednis wskazuje, że ze względów dowodowych oraz potencjalnie konsultacje z organem nadzorczym ds. ochrony danych osobowych „należy przyjąć, że ocena powinna powstać jako dokument na trwałym nośniku"[884]. Grupa Robocza Art. 29 wyjaśnia, że ocena skutków dla ochrony danych jest istotnym elementem rozliczalności i stoi na stanowisku, że powinna być udokumentowana, podobnie jak uzasadnienie nieprzeprowadzenia takiej oceny – administrator powinien wówczas „załączyć/zapisać poglądy inspektora ochrony danych"[885]. Podobnie, bardzo ogólnie, wypowiada się na ten temat polski organ nadzorczy ds. ochrony danych osobowych, zwracając uwagę, że „Oceny te powinny być dokumentowane przez administratora zgodnie z zasadą rozliczalności"[886]. Administrator przetwarzający dane osobowe dzieci w związku ze świadczeniem usług społeczeństwa informacyjnego, zarówno przy ogólnej analizie ryzyka, jak i ewentualnej ocenie skutków dla ochrony danych, powinien wziąć pod uwagę specyficzne zagrożenia właściwe dla tych podmiotów danych oraz przedstawić to w opracowanej dokumentacji.

Obowiązki, z jakimi wiąże się postępowanie w przypadku wystąpienia naruszenia ochrony danych osobowych, obejmują również posiadanie stosownej dokumentacji pozwalającej organowi nadzorczemu ds. ochrony danych osobowych weryfikować przestrzeganie regulacji w tym przedmiocie, o czym stanowi wprost art. 33 ust. 5 rozporządzenia 2016/679. Zgodnie z tym przepisem, administrator „dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze".

---

[883] Por. M. Sakowska- Baryła, M. Więckowska, *Dokumentacja monitorowania zgodności z RODO – audyty wewnętrzne i weryfikacja powierzenia przetwarzania*, [w:] M. Jagielski (red.), *Dokumentacja ochrony danych osobowych ze wzorami*, wyd. 2, Warszawa 2022, s. 378.
[884] A. Mednis, *Wymóg oceny skutków…*, s. 31.
[885] Grupa Robocza Art. 29, *Wytyczne dotyczące oceny skutków…*, s. 14. O prowadzeniu dokumentacji mowa także na s. 18 i 20.
[886] GIODO, *Jak stosować podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku część 2*, https://archiwum.giodo.gov.pl/pl/1520282/10294 (dostęp: 15.03.2023), s. 38.

Na podstawie decyzji Prezesa UODO w sprawie DKN.5131.49.2021 można wywieść, że stoi on na stanowisku, iż na dokumentację dotyczącą naruszeń ochrony danych osobowych powinien składać się ich rejestr oraz oceny ryzyka naruszenia praw i wolności podmiotów danych[887]. Dodatkowo, jak wskazuje Grupa Robocza Art. 29, administrator powinien dokumentować wszystkie naruszenia, także niepodlegające zgłoszeniu organowi nadzorczemu do spraw ochrony danych osobowych wraz z uzasadnieniem, a jeśli administrator zawiadomił podmioty danych o naruszeniu, winien przechowywać dowody na to, co pomoże mu wykazanie rozliczalności[888]. Co więcej, podobnie jak w wytycznych europejskich organów nadzorczych ds. ochrony danych osobowych[889], w literaturze słusznie zauważa się, że do właściwej obsługi naruszeń ochrony danych osobowych potrzebne jest wdrożenie procedury, która w przejrzysty sposób określa w szczególności, kto jest odpowiedzialny za zgłoszenie „wewnętrzne", jak wypełnić opracowany na te potrzeby formularz, jakie okoliczności należy odnotować i udokumentować, kto notyfikuje naruszenie Prezesowi UODO[890].

Przekazywanie danych osobowych do państw trzecich również wymaga podjęcia wysiłków polegających na odpowiednim udokumentowaniu przestrzegania zasad określonych w rozdziale V rozporządzenia 2016/679 – taką konieczność akcentuje się w przypadku korzystania ze standardowych klauzul ochrony danych, co zgodnie z orzecznictwem TSUE i zaleceniami EROD wymaga oceny, czy nieodzowne jest ocenienie potrzeby wprowadzenia dodatkowych środków ochrony, a w razie odpowiedzi pozytywnej udokumentowanie ich wdrożenia[891]. Na etapie wykonywania umowy zawartej z wykorzystaniem klauzul ochrony danych, KE zaznacza, że „strony powinny być w stanie wykazać przestrzeganie standardowych klauzul umownych. W szczególności podmiot odbierający dane powinien być zobowiązany do przechowywania odpowiedniej dokumentacji dotyczącej czynności przetwarzania, za które ponosi odpowiedzialność (…)"[892]. Wydaje się, że zastosowanie innych instrumentów transferu danych osobowych, zwłaszcza powołanie się na wyjątkowe przesłanki z art. 49 rozporządzenia 2016/679, też nie powinno pozostać bez śladu w dokumentacji ochrony danych osobowych.

Na gruncie przepisów rozporządzenia 2016/679 dotyczących inspektora ochrony danych, rozliczalność zapewniłoby posiadanie przez administratora i podmiot przetwarzający dowodów na włączanie go we wszystkie sprawy dotyczące ochrony danych osobowych zgodnie z art. 38 ust.

[887] Por. decyzja Prezesa UODO opublikowana na stronie internetowej dnia 1 marca 2023 r. (brak informacji o dacie wydania), DKN.5131.49.2021, https://uodo.gov.pl/pl/347/2657 (dostęp: 15.03.2023).
[888] Grupa Robocza Art. 29, *Wytyczne dotyczące zgłaszania*…, s. 31-32.
[889] Tamże, s. 32.
[890] Por. M. Sakowska-Baryła, *Zgłaszanie naruszenia*…, Legalis.
[891] EROD, *Zalecenia 01/2020*…, s. 10.
[892] Decyzja KE 2021/914, pkt 17 preambuły.

1 rozporządzenia 2016/679[893], a także na zapewnienie mu warunków, niezbędnych zasobów, pozwalających na należyte wykonywanie zadań określonych w art. 39 rozporządzenia 2016/679. W przypadku niezastosowania się do rekomendacji inspektora ochrony danych, odnotowanie powodów takiego postępowania uważa się za dobrą praktykę[894]. Natomiast podmioty, które nie zdecydowały się na wyznaczenie inspektora ochrony danych po przeprowadzeniu analizy, czy ten obowiązek ich dotyczy, powinny ją udokumentować[895].

Na administratorze ciąży szereg obowiązków powiązanych z wykonywaniem przez podmioty danych uprawnień przysługujących im na mocy przepisów rozdziału III rozporządzenia 2016/679, których należyte wypełnianie powinien być w stanie udowodnić stosownie do zasady rozliczalności. Dokumentowanie treści udzielonych odpowiedzi, formy, terminów i faktycznie podjętych działań (np. usunięcie danych osobowych, zrealizowanie prawa dostępu do danych osobowych zgodnie z art. 15 rozporządzenia 2016/679[896]) oraz sprawdzanie umocowania osoby działającej z upoważnienia podmiotu danych[897], warunkuje możność wykazania, że w procesie realizacji uprawnień nie dochodzi do nieprawidłowości. Rejestr wniosków i udzielanych na nie odpowiedzi będzie także przydatny dla samego administratora ze względów dowodowych w razie ewentualnych sporów[898]. Z drugiej strony zachowanie rozliczalności w kontekście realizacji uprawnień podmiotów danych może być wyzwaniem i wymaga szczególnej roztropności, ponieważ nadmierny formalizm może narazić administratora na zarzut uchybienia art. 11 rozporządzenia 2016/679, według którego należy powstrzymać się od przetwarzania danych osobowych wyłącznie w celu zastosowania się do przepisów rozporządzenia 2016/679 – prawodawca podkreśla tym samym nadrzędność ochrony prywatności i danych osobowych podmiotów danych, a pośrednio także zasady minimalizacji danych, nad wypełnianiem obowiązków wynikających z rozporządzenia 2016/679[899].

Pod rządami uodo z 1997 r. za istotny, organizacyjny środek ochrony danych osobowych uważano nadawanie upoważnień do przetwarzania danych osobowych i prowadzenie ewidencji osób upoważnionych, do czego zobowiązywały art. 37 i art. 39 uodo z 1997 r. Rozporządzenie 2016/679 nie statuuje wprost analogicznego obowiązku, jednak ze względu na brzmienie art. 29 rozporządzenia 2016/679, zgodnie z którym osoby działające z upoważnienia administratora lub

[893] Por. decyzja Prezesa UODO z dnia 21 sierpnia 2020 r., ZSOŚS.421.25.2019, https://www.uodo.gov.pl/decyzje/ZSOŚS.421.25.2019 (dostęp: 15.03.2023).
[894] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów…, s. 17.
[895] Por. E. Bielak-Jomaa, *Komentarz do art. 37 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 770.
[896] Por. EROD, *Guidelines 01/2022*…, s. 43.
[897] Tamże, s. 29.
[898] Por. J. Łuczak, *Komentarz do art. 12 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 471.
[899] Por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 11 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 1.

podmiotu przetwarzającego co do zasady przetwarzają dane osobowe wyłącznie na polecenie administratora, kontynuowanie praktyki nadawania upoważnień i prowadzenia ich ewidencji jest przez niektórych uważana za dobrą praktykę[900]. Należy jednak zgodzić się z poglądem, że decyzja o sposobie spełnienia i udokumentowania wymogu stawianego administratorowi oraz podmiotowi przetwarzającemu w art. 29 rozporządzenia 2016/679, leży w gestii adresatów zawartej w tym przepisie normy[901].

Przepis art. 30 rozporządzenia 2016/679 kreuje dodatkowy, tym razem wyrażony wprost, obowiązek dokumentacyjny po stronie administratora – prowadzenie rejestru czynności przetwarzania danych osobowych w formie pisemnej, w tym elektronicznej. Prowadzenie rejestru czynności przetwarzania ma na celu zachowanie zgodności z rozporządzeniem 2016/679 i umożliwienie organowi nadzorczemu ds. ochrony danych osobowych monitorowania operacji przetwarzania[902]. Może być także pomocne w usystematyzowaniu czynności przetwarzania, ocenie ich zgodności m.in. z wymogami prawnymi, analizie niezbędności podjęcia dodatkowych działań w odniesieniu do poszczególnych czynności, przykładowo przeprowadzenie oceny skutków dla ochrony danych[903]. W art. 30 ust. 1 rozporządzenia 2016/679 określono obligatoryjne informacje, które powinny zostać ujęte w rejestrze czynności przetwarzania – mianowicie dane o administratorze, współadministratorach, inspektorze ochrony danych (jeśli został wyznaczony), cele przetwarzania, opis kategorii osób, których dane dotyczą, oraz samych danych osobowych, kategorie odbiorców danych osobowych, także w państwach trzecich (w takim wypadku należy ponadto wskazać odpowiednie zabezpieczenia wdrożone w związku z transferem danych), a także – jeśli to możliwe – przewidywany termin usunięcia poszczególnych kategorii danych oraz ogólny opis technicznych i organizacyjnych środków bezpieczeństwa. Przez „opis kategorii osób, których dane dotyczą" rozumie się określenie pewnej zbiorowości, którą wyróżnia typowa cecha wspólna[904]. Dla przykładu, ze względu na dodatkowe obowiązki i uwarunkowania przetwarzania danych osobowych dzieci, można uznać, że administrator powinien zawrzeć taką informację w rejestrze, ponieważ zapewne byłaby ona istotna z perspektywy organu nadzorczego ds. ochrony danych osobowych i inspektora ochrony danych, monitorujących zgodność działań z rozporządzeniem 2016/679. Za kluczowe dla zrozumienia charakteru omawianej ewidencji jest jednak pojęcie „czynności przetwarzania", które – w przeciwieństwie do „przetwarzania" – nie

[900] Por. P. Kalina, *Dokumentacja ochrony danych osobowych w RODO*, „Informacja w administracji publicznej" 2018, nr 3, s. 32.
[901] Por. P. Fajgielski, *Upoważnienie do przetwarzania danych osobowych*, „Studia Prawnicze KUL" 2020, nr 1, s. 101.
[902] Por. motyw 82 preambuły rozporządzenia 2016/679.
[903] Por. UODO, *Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO*, https://uodo.gov.pl/data/filemanager_pl/708.pdf (dostęp: 15.03.2023), s. 5.
[904] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 396.

posiada definicji legalnej. Posłużenie się przez prawodawcę dwoma różnymi sformułowaniami wskazuje, że w rejestrze, o którym mowa w art. 30 ust. 1 rozporządzenia 2016/679, nie chodzi o wyszczególnienie wszystkich pojedynczych operacji przetwarzania, na które składa się czynność przetwarzania. Podobnie orzekł, częściowo powtarzając stanowisko organu nadzorczego ds. ochrony danych osobowych[905], WSA w Łodzi stwierdzając, że „czynności przetwarzania to zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane. Rejestr z kolei to opis poszczególnych zespołów operacji związanych zbiorczo z realizacją określonego celu przetwarzania"[906]. Podmiot przetwarzający także zobowiązany jest do prowadzenia podobnej ewidencji – rejestru kategorii czynności przetwarzania dokonywanych w imieniu administratora, o czym stanowi art. 30 ust. 2 rozporządzenia 2016/679. Przepis ten wyznacza zakres informacji, które powinny być ujęte w rejestrze podmiotu przetwarzającego – jest znacznie węższy w porównaniu do rejestru administratora, ponadto zamiast o czynnościach przetwarzania mowa w nim o „kategoriach przetwarzań" – co wynika z odmiennej roli i obowiązków tych podmiotów w procesie przetwarzania danych osobowych[907]. Prawodawca w art. 30 ust. 5 rozporządzenia 2016/679 przewidział wyłączenia spod obowiązku prowadzenia rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania w stosunku do podmiotu, który zatrudnia mniej niż 250 osób, jednak wprowadził dodatkowe warunki – zwolnienie nie ma zastosowania, o ile przetwarzanie danych osobowych przez taki podmiot „może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych, o czym mowa w art. 10". Analiza tak skonstruowanych wyłączeń – zwłaszcza kryterium odnoszącego się do „sporadyczności przetwarzania" – prowadzi do wniosku, że niewiele podmiotów będzie mogło z nich skorzystać[908], zatem trudno powiedzieć, by wzmiankowany w motywie 13 preambuły rozporządzenia 2016/679 zamiar odciążenia mikroprzedsiębiorstw, małych i średnich przedsiębiorstw, został zrealizowany.

Wskazanych wyżej obowiązków, służących wykazywaniu zgodności z rozporządzeniem 2016/679 w myśl zasady rozliczalności, nie należy traktować jako zamkniętego katalogu[909],

[905] Por. UODO, *Wskazówki i wyjaśnienia*…, s. 7.
[906] Wyrok WSA w Łodzi z dnia 12 lutego 2019 r., sygn. II SAB/Łd 181/18.
[907] Szerzej na temat różnic i uzasadnienia dla nich w kontekście rejestrów por. P. Fajgielski, *Rejestry czynności przetwarzania danych osobowych,* [w:] „Monitor Prawniczy" dodatek: *Wdrażanie ogólnego rozporządzenia…*, s. 37.
[908] Por. K. Cieniak, *Wybrane zagadnienia związane z obowiązkiem prowadzenia rejestru czynności przetwarzania*, „Monitor Prawniczy" 2018, nr 3, s. 164.
[909] W literaturze podawane są także przykłady innych dokumentów, których przedłożenia oczekuje Prezes UODO w toku prowadzonych postępowań, takich jak analiza poprzedzająca usunięcie danych osobowych czy instrukcja postępowania w przypadku ujawnienia danych osobowych w wyniku błędu pracownika, co przeczy tezie o „odformalizowaniu" ochrony danych osobowych pod rządami rozporządzenia 2016/679 – por. K. Gałęzowska, *Dokumentowanie zgodności z przepisami RODO*, „Monitor Prawniczy" dodatek: *Ocena i przegląd RODO…*, s. 43.

ponieważ zakres i przedmiot dokumentacji należy uzależnić od wielu czynników determinujących specyfikę przetwarzania danych osobowych przez określony podmiot. W prowadzonej przez siebie dokumentacji administrator świadczący dzieciom usługi społeczeństwa informacyjnego winien zawrzeć informacje o stosowanych rozwiązaniach służących respektowaniu ich szczególnej sytuacji, dostrzeżonej na gruncie przepisów rozporządzenia 2016/679.

ROZDZIAŁ V
ODPOWIEDZIALNOŚĆ ZA NARUSZENIA ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH DZIECKA

1. Odpowiedzialność administracyjna

1.1 Kluczowe zadania i uprawnienia organu nadzorczego z perspektywy ochrony danych osobowych dziecka

Kompetencje organu nadzorczego ds. ochrony danych osobowych, w przypadku Polski Prezesa UODO, zostały podzielone w przepisach rozporządzenia 2016/679 na zadania i uprawnienia. Dwadzieścia dwa zadania, które znalazły się w otwartym katalogu[910] w art. 57 ust. 1 rozporządzenia 2016/679, P. Fajgielski dzieli na pięć ogólnych grup – nadzorcze, doradcze, edukacyjne, związane ze współpracą z innymi organami nadzorczymi indywidualnie oraz skupionymi w EROD, inne zadania – do których prawodawca zaliczył m.in. monitorowanie zmian w dziedzinach mających znaczenie dla ochrony danych osobowych[911]. Ze względu na przedmiot rozprawy i niniejszego rozdziału warto zwrócić uwagę na wybrane zadania o charakterze nadzorczym oraz edukacyjnym.

Według P. Fajgielskiego do zadań nadzorczych zaliczyć można m.in. monitorowanie i egzekwowanie stosowania rozporządzenia 2016/679[912], rozpatrywanie skarg wniesionych przez podmioty danych[913], prowadzenie postępowań w sprawie stosowania rozporządzenia 2016/679[914]. Za najważniejsze, stanowiące trzon funkcjonowania organu nadzorczego, uznaje się monitorowanie – przez które można rozumieć „prowadzenie stałej obserwacji i kontroli procesów przetwarzania danych" oraz egzekwowanie – czyli korzystanie przez organ nadzorczy „z przewidzianych przepisami uprawnień, służących wykonywaniu obowiązków związanych z przetwarzaniem i ochroną danych"[915]. Natomiast działania o charakterze edukacyjnym polegają

[910] Prawo krajowe może przewidywać dodatkowe zadania – por. P. Litwiński, P. Barta, *Komentarz do art. 57 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 2 i tam podany przykład.
[911] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 598. Inny, bardziej rozdrobniony podział proponuje M. Sakowska-Baryła – por. M. Sakowska-Baryła, *Komentarz do art. 57 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 2. Z kolei A. Giurgiu i T. A Larsens, wychodząc z założenia, że wzmocnienie roli organów nadzorczych jest najbardziej kluczowe i pożądane w przypadku postępowań transgranicznych, dzielą zadania na realizowane samodzielnie, w granicach swojego terytorium, oraz w ramach współpracy międzynarodowej ze swoimi odpowiednikami z innych państw członkowskich UE – por. A. Giurgiu, T. A Larsens, *Roles and Powers of National Data Protection Authorities.*
Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?, „European Data Protection Law Review" 2016, nr 3, s. 347.
[912] Art. 57 ust. 1 lit. a rozporządzenia 2016/679.
[913] Art. 57 ust. 1 lit. f rozporządzenia 2016/679.
[914] Art. 57 ust. 1 lit. h rozporządzenia 2016/679.
[915] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 599.

m.in. na upowszechnianiu wśród administratorów i podmiotów przetwarzających wiedzy o spoczywających na nich obowiązkach[916], a w przypadku społeczeństwa popularyzowania wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienia tych zjawisk[917]. W art. 57 ust. 1 lit. b rozporządzenia 2016/679 podkreślono, że organ nadzorczy szczególną uwagę poświęca działaniom skierowanym do dzieci. Komentatorzy zasadnie zwracają uwagę na doniosłość tego zadania w związku z dynamicznym rozwojem usług społeczeństwa informacyjnego, wskazując że może być ono realizowane przykładowo poprzez organizowanie spotkań, warsztatów dla dzieci, a ponadto sygnalizują, że działania organu nadzorczego mogą być ukierunkowane na włączanie instytucji do promowania wśród dzieci wiedzy o ochronie danych osobowych[918]. Przykładem takich działań jest prowadzony przez Prezesa UODO ogólnopolski program edukacyjny „Twoje dane – Twoja sprawa", który jest skierowany do szkół podstawowych, ponadpodstawowych, ośrodków doskonalenia nauczycieli i polega na przygotowaniu nauczycieli do prowadzenia lekcji poświęconym ochronie danych osobowych, a następnie edukowaniu dzieci i młodzieży[919]. Na uwagę zasługuje również aktywność irlandzkiego organu nadzorczego na rzecz propagowania wiedzy o ochronie danych osobowych dzieci poprzez opracowanie cyklu poradników dla rodziców[920], a także materiałów informacyjnych kierowanych głównie do administratorów i podmiotów przetwarzających[921]. Warto także nadmienić, że brytyjski organ nadzorczy opracował dokument skierowany do dostawców usług społeczeństwa informacyjnego oferowanych dzieciom, nad którym rozpoczął prace jeszcze w czasie członkostwa Wielkiej Brytanii w UE, uwzględniając przepisy rozporządzenia 2016/679[922], przez co wciąż może być wykorzystywany pomocniczo. Z kolei francuski organ nadzorczy sformułował i wyjaśnił osiem rekomendacji w przedmiocie „cyfrowych praw dzieci", które przysługują im w związku z przetwarzaniem danych osobowych oraz o roli rodziców we wspieraniu dzieci, w tym

[916] Art. 57 ust. 1 lit. d rozporządzenia 2016/679.
[917] Art. 57 ust. 1 lit. b rozporządzenia 2016/679.
[918] Por. U. Góral, P. Makowski, *Komentarz do art. 57 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 936-937. Por. także U. Góral, *Rola organu ochrony danych w edukacji na temat prawa do prywatności i ochrony danych*, [w:] A. Fidelus, Z. Babicki (red.), *Prawa dziecka w wybranych kontekstach opiekuńczo-wychowawczych*, Warszawa 2019.
[919] Por. UODO, *Twoje dane – Twoja sprawa*, https://uodo.gov.pl/512 (dostęp: 15.03.2023).
[920] Data Protection Commission, *Protecting my child's data*, https://www.dataprotection.ie/sites/default/files/uploads/2023-04/DPC_ChildrensData_ProtectingThem.pdf; *My child's data protection rights – the basics,* https://www.dataprotection.ie/sites/default/files/uploads/2023-04/DPC_ChildrensRights_TheBasics.pdf; *Children's data and parental consent*, https://www.dataprotection.ie/sites/default/files/uploads/2023-04/DPC_ChildrensData_ParentalConsent.pdf; *Are there any limits on my child's data protection rights?*, https://www.dataprotection.ie/sites/default/files/uploads/2023-04/DPC_ChildrensData_Limits.pdf (dostęp: 15.04.2023).
[921] Data Protection Commission, *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*, https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (dostęp: 15.04.2023).
[922] ICO, *Age appropriate…,* s. 10.

sprawowaniu kontroli nad ich aktywnością w intrenecie z jednoczesnym poszanowaniem prywatności[923]. Uwrażliwianie przedstawicieli ustawowych na problem przetwarzania danych osobowych dzieci w związku ze świadczeniem usług społeczeństwa informacyjnego uważam za dobry kierunek, ponieważ to oni od najmłodszych lat kształtują zwyczaje młodych ludzi związane z korzystaniem z internetu.

Uprawnienia organu nadzorczego zostały w art. 58 rozporządzenia 2016/679 podzielone na trzy grupy: 1) dotyczące prowadzonych postępowań; 2) naprawcze; 3) dotyczące wydawania zezwoleń i doradcze. Ostatnie z nich, o których mowa w art. 58 ust. 3 rozporządzenia 2016/679, traktują m.in. o udzielaniu administratorowi i podmiotowi przetwarzającemu porad w procedurze uprzednich konsultacji[924], wydawania opinii przeznaczonych dla parlamentu narodowego, rządu państwa członkowskiego UE lub innych instytucji i organów oraz ogółu społeczeństwa we wszelkich sprawach związanych z ochroną danych osobowych, zgodnie z przepisami krajowymi[925], zatwierdzaniu wiążących reguł korporacyjnych – instrumentu legalizującego transfer danych osobowych do państwa trzeciego[926]. Dla ochrony danych osobowych dziecka i egzekwowania odpowiedzialności za ich przetwarzanie z naruszeniem rozporządzenia 2016/679 pierwszorzędne znaczenie mają uprawnienia przysługujące organowi nadzorczemu w ramach prowadzonych postępowań oraz uprawnienia naprawcze.

W toku postępowań uprawnienia organu nadzorczego mają przede wszystkim zapewnić mu możliwość rzetelnego ustalenia stanu faktycznego – polegają na uzyskiwaniu od administratora i podmiotu przetwarzającego dostępu do wszelkich niezbędnych danych osobowych i informacji[927], a także do pomieszczeń, w tym sprzętu i środków służących do przetwarzania danych[928]. Organ nadzorczy może nakazać dostarczenie informacji[929], a także prowadzić postępowania w formie audytów[930] oraz zawiadamiać administratora i podmiot przetwarzający o podejrzeniu naruszenia rozporządzenia 2016/679[931].

Realizacja uprawnienia organu nadzorczego, o którym mowa w art 58 ust. 1 lit. f rozporządzenia 2016/679 – prawa dostępu do pomieszczeń, sprzętu i środków wykorzystywanych w celu przetwarzania danych osobowych – odbywa się na zasadach określonych w prawie UE lub krajowym. W Polsce Prezes UODO może realizować powyższe uprawnienie w ramach postępowania kontrolnego, prowadzonego na podstawie przepisów uodo z 2018 r. Przepis art. 84

[923] CNIL, *Digital rights of children*, https://www.cnil.fr/en/digital-rights-children (dostęp: 15.04.2023).
[924] Por. art. 58 ust. 3 lit. a rozporządzenia 2016/679.
[925] Por. art. 58 ust. 3 lit. b rozporządzenia 2016/679.
[926] Por. art. 58 ust. 3 lit. j rozporządzenia 2016/679.
[927] Por. art. 58 ust. 1 lit. e rozporządzenia 2016/679.
[928] Por. art. 58 ust. 1 lit. f rozporządzenia 2016/679.
[929] Por. art. 58 ust. 1 lit. a rozporządzenia 2016/679.
[930] Por. art. 58 ust. 1 lit. b rozporządzenia 2016/679.
[931] Por. art. 58 ust. 1 lit. d rozporządzenia 2016/679.

ust. 1 pkt 1-5 uodo z 2018 r. wyznacza zakres uprawnień kontrolującego i doprecyzowuje sposób prowadzenia kontroli – począwszy od określenia godzin, w których czynności mogą być przeprowadzone (od 6:00 do 22:00), przez wymienienie rodzaju czynności – zaliczono do nich m.in. wgląd do dokumentów i informacji związanych bezpośrednio z przedmiotem kontroli, przeprowadzanie oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych wykorzystywanych do przetwarzania danych, żądanie złożenia pisemnych lub ustnych wyjaśnień, przesłuchiwanie osób w charakterze świadków, kończąc na zlecaniu sporządzenia ekspertyz i opinii. W odniesieniu do wglądu w dokumentację, kontrolowany administrator może być przykładowo zobowiązany do przedstawienia rejestru czynności przetwarzania danych osobowych (lub rejestru kategorii czynności przetwarzania danych, gdy kontrolowany jest podmiot przetwarzający), stosowanych klauzul zgody na przetwarzanie danych osobowych, klauzul informacyjnych, umów powierzenia przetwarzania danych osobowych[932], wewnętrznych procedur i polityk w dziedzinie ochrony danych osobowych, takich jak zasady postępowania w przypadku naruszenia ochrony danych osobowych[933]. Ponadto art. 85 rozporządzenia 2016/679 przewiduje, jeśli jest to niezbędne, możliwość korzystania przez Prezesa UODO z pomocy Policji przy wykonywaniu czynności kontrolnych. W myśl art. 88 uodo z 2018 r. kontrolujący sporządza protokół kontroli i przedstawia go kontrolowanemu w celu podpisania, który w ciągu 7 dni może to uczynić lub złożyć pisemne zastrzeżenia.

Z uprawnień naprawczych, o których mowa w art. 58 ust. 2 rozporządzenia 2016/679, organ nadzorczy korzysta, gdy dostrzega możliwość naruszenia przez administratora lub podmiot przetwarzający rozporządzenia 2016/679 przez planowane operacje przetwarzania danych osobowych – wówczas wydaje ostrzeżenie[934], zaś w razie stwierdzenia naruszenia rozporządzenia 2016/679 może korzystać z szeregu władczych kompetencji, których celem jest przywrócenie stanu zgodnego z prawem[935]. Organ nadzorczy dysponuje instrumentami o różnym stopniu dolegliwości. Może udzielić administratorowi lub podmiotowi przetwarzającemu upomnienia w sytuacji, gdy naruszenie jest „niewielkie lub jeżeli grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie”[936]. Wybór „najodpowiedniejszego” środka naprawczego należy do organu nadzorczego, który na podstawie obiektywnej oceny stanu faktycznego powinien

[932] Por. P. Fajgielski, *Ogólne rozporządzenie…,* s. 934; K. Kloc, *Komentarz do art. 84 uodo z 2018 r.*, [w:] D. Lubasz (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2019, s. 442.
[933] Por. A. Dmochowska, *Komentarz do art. 84 uodo z 2018 r.*, [w:] A. Dmochowska, A. Piotrowska, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 132.
[934] Por. art. 58 ust. 2 lit. a rozporządzenia 2016/679.
[935] Por. M. Sakowska-Baryła, *Komentarz do art. 58 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 8.
[936] Motyw 148 preambuły rozporządzenia 2016/679.

skorzystać z uprawnienia odpowiadającemu charakterowi, wadze i konsekwencjom naruszenia[937]. Organ nadzorczy może zatem nakazać: 1) spełnienie żądania podmiotu danych, wynikającego z uprawnień praw przysługujących jej na mocy rozporządzenia 2016/679[938]; 2) dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679, w stosownych przypadkach wraz ze wskazaniem sposobu i terminu; 3) zawiadomienie podmiotu danych o naruszeniu ochrony danych osobowych[939]; 4) sprostowanie, usunięcie danych osobowych lub ograniczenie ich przetwarzania na mocy art. 16-18 rozporządzenia 2016/679 oraz art. 17 ust. 2 i art. 19 rozporządzenia 2016/679, a także powiadomienie o tych czynnościach odbiorców, którym ujawniono dane[940]; 5) zawieszenie przepływu danych osobowych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej[941]. Ponadto do uprawnień organu nadzorczego należy m.in. wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania[942] oraz nałożenie administracyjnej kary pieniężnej zgodnie z art. 83 rozporządzenia 2016/679[943].

1.2 Nakładanie administracyjnych kar pieniężnych

Możliwość nałożenia na administratora i podmiot przetwarzający administracyjnej kary pieniężnej jest istotnym *novum*[944], jakie niesie ze sobą unijna reforma ochrony danych osobowych – ta kompetencja uzupełnia w rozporządzeniu 2016/679 inne, zasadniczo wzorowane na postanowieniach dyrektywy 95/46, uprawnienia organu nadzorczego[945]. Uzupełnia nie tylko w znaczeniu dosłownym – w myśl art. 58 ust. 2 lit. j rozporządzenia 2016/679 administracyjna kara pieniężna może być bowiem zastosowana oprócz innych środków naprawczych – ale i kwalitatywnym, ponieważ prawodawca wyposażył w ten sposób organ nadzorczy w narzędzie, którego wcześniejszy brak jest poczytywany za jeden z powodów niezadowalającej skuteczności

[937] Grupa Robocza Art. 29, *Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679*, przyjęte w dniu 3 października 2017 r., https://archiwum.giodo.gov.pl/pl/1520344/10432 (dostęp: 15.04.2023), s. 6.
[938] Por. art. 58 ust. 2 lit. c rozporządzenia 2016/679.
[939] Por. art. 58 ust. 2 lit. e rozporządzenia 2016/679. Chodzi tu o naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt 12 rozporządzenia 2016/679, dlatego to uprawnienie może być zastosowane tylko wobec administratora.
[940] Por. art. 58 ust. 2 lit. g rozporządzenia 2016/679.
[941] Por. art. 58 ust. 2 lit. j rozporządzenia 2016/679.
[942] Por. art. 58 ust. 2 lit. f rozporządzenia 2016/679.
[943] Por. art. 58 ust. 2 lit. i rozporządzenia 2016/679.
[944] Nie oznacza to jednak, że przed reformą prawo niektórych państw członkowskich UE nie przewidywało kar finansowych za naruszenia w obszarze ochrony danych osobowych – aczkolwiek ich górne limity były niższe niż określone w rozporządzeniu 2016/679, sięgały maksymalnie kilkuset tysięcy euro, więc wprowadzenie wyższych kar na mocy stosowanego bezpośrednio, unijnego rozporządzenia, ma zwiększyć zainteresowanie przedsiębiorców ochroną danych osobowych – por. S. Varotto, *The European General Data Protection Regulation and its potential impact on businesses: some critical notes on the strengthened regime of accountability and the new sanctions*, „Communications Law: Journal of Computer, Media & Telecommunications" 2015, vol. 20, nr 3, s. 82 i tam podane źródła.
[945] Por. P. Fajgielski, *Ogólne rozporządzenie…,* s. 604.

egzekwowania przepisów o ochronie danych osobowych[946]. Grupa Robocza Art. 29 postrzega administracyjne kary pieniężne jako zasadniczy element nowego systemu egzekwowania prawa przez organy nadzorcze[947]. W literaturze wskazuje się, że administracyjne kary pieniężne realizują cel prewencyjny, restytucyjny, a dodatkowo – choć nie jest to pierwszoplanowe – mogą pełnić funkcję represyjną[948]. Nałożenie administracyjnej kary pieniężnej oddziałuje prewencyjnie nie tylko na ukaranego – ma zapobiegać dopuszczaniu się naruszeń także przez inne podmioty[949].

Proceduralne aspekty nakładania przez Prezesa UODO administracyjnych kar pieniężnych określają przepisy uodo z 2018 r., a w zakresie nieuregulowanym oraz z zastrzeżeniem wyłączeń wskazanych w art. 106 uodo z 2018 r. – przepisy kpa, stosowane subsydiarnie[950]. Zgodnie z art. 101 uodo z 2018 r., Prezes UODO może nałożyć administracyjną karę pieniężną na podmiot obowiązany do przestrzegania przepisów rozporządzenia 2016/679 w drodze decyzji administracyjnej, na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679. Postępowanie przed Prezesem UODO jest jednoinstancyjne, a decyzja o nałożeniu kary podlega zaskarżeniu do sądu administracyjnego[951]. W myśl art. 104 uodo z 2018 r., środki z administracyjnej kary pieniężnej stanowią dochód budżetu państwa.

Stosownie do art. 83 ust. 1 rozporządzenia 2016/679, administracyjne kary pieniężne powinny być skuteczne, proporcjonalne i odstraszające w każdym indywidualnym przypadku – co oznacza, że w ich nakładaniu nie jest dopuszczalny automatyzm, lekceważenie okoliczności danej sprawy[952]. Znajduje to odzwierciedlenie we wskazanych w art. 83 ust. 2 rozporządzenia 2016/679 kryteriach, którymi kieruje się organ nadzorczy, po pierwsze podejmując decyzję o nałożeniu kary, a po drugie ustalając jej wysokość. Prawodawca zaliczył do nich: 1) charakter, wagę i czas trwania naruszenia biorąc pod uwagę charakter, zakres lub cel danego przetwarzania, liczbę poszkodowanych podmiotów danych oraz rozmiar poniesionej przez nich szkody; 2) charakter naruszenia – umyślny lub nieumyślny; 3) działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez podmioty danych; 4) stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32 rozporządzenia 2016/679; 5) wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego; 6)

[946] Por. motyw 148 preambuły rozporządzenia 2016/679.
[947] Por. Grupa Robocza Art. 29, *Wytyczne w sprawie stosowania*…, s. 4.
[948] Por. R. Suwaj, *Zasady nakładania administracyjnych kar pieniężnych*, Warszawa 2021, s. 51 i tam powołana literatura.
[949] Por. M. Abu Gholeh, D. Kuźnicka-Błaszkowska, *Nakładanie administracyjnych kar pieniężnych w rozporządzeniu o ochronie danych. Aspekty praktyczne*, Warszawa 2020, s. 26.
[950] Por. J. Łuczak-Tarka, *Komentarz do art. 101 uodo z 2018 r.*, [w:] D. Lubasz (red.), *Ustawa o ochronie danych…*, s. 494.
[951] Szerzej na ten temat por. P. Fajgielski, *Ogólne rozporządzenie…,* s. 800-802 i 955-956.
[952] Por. M. Górski, *Komentarz do art. 83 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 2.

stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków; 7) kategorie danych osobowych, których dotyczyło naruszenie; 8) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie; 9) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 – przestrzeganie tych środków; 10) stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 rozporządzenia 2016/679 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42 rozporządzenia 2016/679; 11) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty. Powyższe kryteria prowadzą do wniosku, że istotna jest nie tylko charakterystyka naruszenia (jego okoliczności, np. jakich kategorii danych dotyczyło), lecz także zachowanie administratora lub podmiotu przetwarzającego po jego wystąpieniu[953]. Zasługuje to na aprobatę – zwłaszcza wzięcie pod uwagę działań tych podmiotów, mających na celu zminimalizowanie szkody poniesionej przez podmioty danych, stanowi dla nich rzeczywistą zachętę do podjęcia wysiłków zmierzających do otoczenia podmiotów danych swoistą opieką po wystąpieniu naruszenia, szczególnie ważną, gdy chodzi o naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt 12 rozporządzenia 2016/679[954]. Niedosyt pozostawia jednak brak wskazania w art. 83 ust. 2 rozporządzenia 2016/679 kryterium kategorii podmiotów danych – jeśli naruszenie dotyczy danych osobowych dzieci, powinno być to istotna okoliczność dla organu nadzorczego. Na ten aspekt zwraca uwagę EROD w wytycznych w przedmiocie obliczania wysokości administracyjnych kar administracyjnych – w jej opinii, badając na podstawie art. 82 ust. 2 lit. a rozporządzenia 2016/679 charakter przetwarzania, organ nadzorczy może przypisać większą wagę temu kryterium przez wzgląd na to, że naruszenie dotyczy danych osób wymagających szczególnej opieki, takich jak dzieci[955]. Należy jednak podkreślić, że jest to dokument o charakterze *soft law*. Jeszcze bardziej rozczarowuje podejście prawodawcy do naruszeń dotyczących danych osobowych dzieci korzystających z usług społeczeństwa informacyjnego na gruncie przepisów określających maksymalną wysokość administracyjnych kar pieniężnych. W rozporządzeniu 2016/679 zróżnicowano je – określono dwa pułapy – obierając

[953] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 707.

[954] Przykładem takich działań, których stosowanie popiera Prezes UODO, jest umożliwienie podmiotom danych bezpłatnego korzystania z usługi „Alerty BIK", która pozwala monitorować, czy do Biura Informacji Kredytowej wpływają zapytania dotyczące danej osoby bądź informacje o jej nowych zobowiązaniach – por. decyzja Prezesa UODO, opublikowana na stronie internetowej dnia 7 lutego 2023 r. (brak informacji o dacie wydania), DKN.5131.31.2021, https://uodo.gov.pl/pl/314/2650 (dostęp: 15.04.2023).

[955] Por. EROD, *Guidelines 04/2022 on the calculation of administrative fines under the GDPR*, wersja 2.0, przyjęte 24 maja 2023 r., https://edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf (dostęp: 15.06.2023), s. 18.

za kryterium rodzaj naruszeń, co świadczy o ich odmiennym „ciężarze gatunkowym”[956]. Przepis art. 83 ust. 4 rozporządzenia 2016/679 przewiduje, że wskazane w nim naruszenia podlegają administracyjnej karze pieniężnej w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, natomiast surowsze kary przewiduje art. 83 ust. 5 rozporządzenia 2016/679, zgodnie z którym wskazane w nim naruszenia podlegają administracyjnej karze pieniężnej w wysokości do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego[957]. Druga „grupa” naruszeń zagrożona jest zatem maksymalną karą aż dwukrotnie wyższą niż pierwsza. Tym, co zaskakuje w świetle podkreślanego wielokrotnie w preambule i przepisach rozporządzenia 2016/679 znaczenia ochrony danych osobowych dzieci – jest przypisanie naruszenia obowiązków określonych w art. 8 rozporządzenia 2016/679, dotyczących zgody na przetwarzanie danych osobowych dziecka w związku ze świadczeniem usług społeczeństwa informacyjnego, do pierwszej „grupy” naruszeń, zagrożonych maksymalną karą w niższej wysokości[958]. Tym samym prawodawca wykazał się niekonsekwencją, skoro jednym celów reformy ochrony danych osobowych było wzmocnienie ochrony praw dzieci, a administracyjne kary pieniężne powinny odstraszać. Można argumentować, że zagrożenie karą w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa do 2% jego całkowitego rocznego światowego obrotu, i tak pozwala organowi nadzorczemu na nałożenie niebotycznej kary, uważam jednak, że nie można bagatelizować pejoratywnego wydźwięku „komunikatu” na temat wartościowania przestrzegania jedynego przepisu rozporządzenia 2016/679 *stricte* odnoszącego się do przetwarzania danych osobowych dzieci, który w powyższy sposób przekazuje prawodawca.

Ponadto warto zauważyć, że niejasna i budząca wątpliwości interpretacyjne jest relacja art. 83 ust. 4 lit. a rozporządzenia 2016/679 i art. 83 ust. 5 lit. a rozporządzenia 2016/679 – czyli odpowiednio przepisu o zagrożeniu naruszenia art. 8 rozporządzenia 2016/679 niższą karą i przepisu o zagrożeniu naruszenia podstawowych zasad przetwarzania, w tym warunków zgody, o których mowa w art. 5, 6, 7 oraz 9 rozporządzenia 2016/679, karą wyższą. Przepis art. 8 rozporządzenia 2016/679 odnosi się zasadniczo do warunków zgody w szczególnym kontekście świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dzieciom, a właściwe pozyskanie zgody oznacza legitymowanie się podstawą prawną przetwarzania danych osobowych, co jest emanacją zasady zgodności z prawem, rzetelności i przejrzystości, wyrażonej w art. 5 ust. 1 ust. 1 lit. a rozporządzenia 2016/679. Można więc postawić pytanie, czy oznacza to,

[956] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 709.
[957] W przypadku art. 83 ust. 4 rozporządzenia 2016/679 jak i art. 83 ust. 5 rozporządzenia 2016/679 zastosowanie ma kwota wyższa.
[958] Por. art. 83 ust. 4 lit. a rozporządzenia 2016/679.

że jeśli naruszenie dotyczy przestrzegania warunków zgody określonych w art. 8 rozporządzenia 2016/679 i jednocześnie stanowi naruszenie zasad wynikających z art. 5, 6, 7 rozporządzenia 2016/679, organ nadzorczy powinien nałożyć karę niższą? Odpowiedź twierdząca prowadziłaby do absurdalnych skutków – znaczącego obniżenia poziomu ochrony danych osobowych dziecka w porównaniu do ochrony danych osobowych osoby dorosłej. Prawodawca rozstrzygnął ten problem w art. 83 ust. 3 rozporządzenia 2016/679, który stanowi, że w razie umyślnego lub nieumyślnego kilku przepisów naruszenia rozporządzenia 2016/679 w ramach tych samych lub powiązanych operacji przetwarzania, całkowita wysokość administracyjnej kary pieniężnej nie przekracza wysokości kary za najpoważniejsze naruszenie. Wciąż zastanawiające jest to, czy możliwe jest naruszenie art. 8 rozporządzenia 2016/679, które jednocześnie nie stanowi nie stanowi naruszenia art. 5, 6, 7 rozporządzenia 2016/679 – tylko w takim stanie faktycznym organ nadzorczy mógłby zastosować art. 83 ust. 4 lit. a rozporządzenia 2016/679. Odpowiedź przecząca oznaczałaby, że subsumpcja jakiegokolwiek stanu faktycznego pod normę wynikającą z przepisu art. 83 ust. 4 lit. a rozporządzenia 2016/679 jest niemożliwa, to z kolei poddawałoby w wątpliwość sens wprowadzenia tego przepisu. Prawodawca nie doprecyzował, co rozumie przez naruszenie art. 8 rozporządzenia 2016/679 – z którego wynika *de facto* kilka obowiązków – czy jego intencją jest objęcie przepisem art. 83 ust. 4 lit. a rozporządzenia 2016/679 naruszenia każdego z tych obowiązków, czy też tylko niektórych z nich – jeśli tak, których? W kontekście nakładania administracyjnych kar pieniężnych P. Litwiński, P. Barta i M. Kawecki uważają, że przez naruszenie art. 8 rozporządzenia 2016/679 należy rozumieć naruszenie obowiązku: 1) uzyskania zgody przedstawiciela ustawowego lub jego aprobaty zgody udzielonej przez dziecko, które nie ukończyło 16. roku życia; 2) przetwarzania danych osobowych dziecka zgodnie z zakresem udzielonej zgody; 3) podjęcia rozsądnych działań w kierunku zweryfikowania, czy przedstawiciel ustawowy wyraził lub zaaprobował zgodę[959]. Odmienny pogląd prezentuje M. Zadrożny, zawężając naruszenie art. 8 rozporządzenia 2016/679 do uchybienia obowiązkowi uzyskania zgody przedstawiciela ustawowego dziecka poniżej 16. roku życia[960]. Wydaje się, że każda z wymienionych wyżej nieprawidłowości godziłaby, przynajmniej w pewnym stopniu, w naczelne zasady, o których mowa w art. 5 rozporządzenia 2016/679. Warto zasygnalizować, że reprezentanci obydwu stanowisk wydają się pomijać fundamentalną, z perspektywy stosowania art. 8 rozporządzenia 2016/679, kwestię podjęcia przez administratora rozsądnych działań w celu ustalenia wieku dziecka. Analizowany problem związany z miarkowaniem administracyjnej kary pieniężnej za naruszenie danych osobowych dzieci nie został do tej pory poruszony w

[959] Por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 83 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 8.
[960] Por. M. Zadrożny, *Warunki nakładania przez GIODO administracyjnych kar pieniężnych*, [w:] A. Dmochowska, M. Zadrożny, *Unijna reforma ochrony danych osobowych - analiza zmian*, Warszawa 2016, Legalis.

orzecznictwie Prezesa UODO – z informacji znajdujących się w rocznych sprawozdaniach wynika, że polski organ nadzorczy nie nałożył jeszcze żadnej administracyjnej kary pieniężnej w związku z przetwarzaniem danych osobowych dzieci w kontekście świadczenia usług społeczeństwa informacyjnego. Ze względu na ważkość zagadnienia uważam, że wskazana jest interwencja prawodawcy i rozstrzygnięcie relacji art. 83 ust. 4 lit. a rozporządzenia 2016/679 i art. 83 ust. 5 lit. a rozporządzenia 2016/679 – moim zdaniem najlepszym rozwiązaniem byłoby usunięcie tej niejasności poprzez usytuowanie naruszenia art. 8 rozporządzenia 2016/679 obok naruszeń dotyczących art. 5, 6, 7 oraz 9 rozporządzenia 2016/679, czyli w art. 83 ust. 5 lit. a rozporządzenia 2016/679. Oprócz rozwiania niektórych wątpliwości interpretacyjnych, zapewniłoby to większą, wewnętrzną spójność art. 83 ust. 5 lit. a rozporządzenia 2016/679 oraz – dzięki zmianie kwalifikacji naruszenia art. 8 rozporządzenia 2016/679 – spójność z założeniami i celami unijnej reformy ochrony danych osobowych.

1.3 Prawo wniesienia skargi do organu nadzorczego

1.3.1 Proceduralne ramy postępowania w sprawie ze skargi

Rozdział VII rozporządzenia 2016/679 nosi tytuł „Środki ochrony prawnej, odpowiedzialność i sankcje" i otwiera go przepis art. 77 ust. 1, zgodnie z którym każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, jeżeli sądzi, że dotyczące jej przetwarzanie danych osobowych narusza rozporządzenie 2016/679. W literaturze podkreśla się istotne znaczenie instytucji skargi, która z perspektywy podmiotu danych „służy więc przede wszystkim wykonaniu prawa do ochrony danych osobowych poprzez działanie organu nadzorczego, jeżeli do realizacji uprawnień w tym względzie nie doszło wcześniej poprzez działania adresatów obowiązków (przede wszystkim administratora)"[961]. Umiejscowienie tego przepisu na początku rozdziału traktującego m.in. o środkach ochrony prawnej wydaje się celowym zabiegiem prawodawcy, który potwierdza tezę o doniosłości prawa do wniesienia skargi. Warto także zauważyć, że stosownie do art. 13 ust. 2 lit. d rozporządzenia 2016/679 i art. 14 ust. 2 lit. e rozporządzenia 2016/679 administrator ma obowiązek informować osobę, które dane dotyczą, o prawie wniesienia skargi do organu nadzorczego. Skorzystanie z prawa do wniesienia skargi nie wpływa na możliwość skorzystania przez podmiot danych z innych środków ochrony prawnej natury administracyjnej lub cywilnej[962].

[961] G. Sibiga, *Skarga do organu nadzorczego oraz jej rozpatrzenie według ogólnego rozporządzenia o ochronie danych. Postępowanie w przedmiocie skargi osoby, której dane dotyczą*, „Prawo Mediów Elektronicznych" 2017, nr 4, s. 7.

[962] Jak zauważono w literaturze, przepis art. 77 ust. 1 rozporządzenia 2016/679 zawiera usterkę redakcyjną („Bez uszczerbku dla innych administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego…"), jednak nie ulega wątpliwości, że intencją prawodawcy

Zgodnie z art. 57 ust. 1 lit. f rozporządzenia 2016/679, organ nadzorczy rozpatruje skargi wniesione przez osobę, której dane dotyczą, prowadzi postępowania w przedmiocie tych skarg i w rozsądnym terminie informuje skarżącego o postępach i wynikach tych postępowań, w szczególności jeżeli niezbędne jest dalsze prowadzenie postępowań lub koordynacja działań z innym organem nadzorczym. Przepis art. 57 ust. 2 rozporządzenia 2016/679 stanowi, że organ nadzorczy ułatwia wnoszenie skarg za pomocą środków takich jak gotowy formularz skargi, który można również wypełnić elektronicznie, co nie wyklucza innych sposobów komunikacji. Ciążący na ogranie nadzorczym obowiązek, polegający na ułatwianiu wnoszenia skarg, może konkretyzować się poprzez różne środki, zmierzające do osiągnięcia tego celu[963].

Przedmiotem skargi może być naruszenie każdego z przepisów rozporządzenia 2016/679, o ile dotyczy przetwarzania danych osobowych skarżącego – podmiotu danych[964], a ponadto naruszenia aktów delegowanych i wykonawczych przyjętych na mocy rozporządzenia 2016/679 oraz prawa krajowego doprecyzowującego rozporządzenie 2016/679[965].

Rozporządzenie 2016/679 jako akt prawa UE nie reguluje proceduralnych aspektów ze względu na zasadę autonomii państw członkowskich w tym zakresie, zatem tryb postępowania określają przepisy rozdziału 7. uodo z 2018 r. i kpa. Skarga powinna spełniać wymogi podania, czyli zgodnie z art. 63 §2 kpa zawierać co najmniej wskazanie osoby, od której pochodzi, jej adres oraz żądanie[966]. Podanie wnoszone na piśmie powinno być podpisane własnoręcznie (art. 63 §3 kpa), zaś wnoszone w postaci elektronicznej powinno być przesłane na adres do doręczeń elektronicznych lub za pośrednictwem konta w systemie teleinformatycznym organu administracji publicznej (art. 63 §1 kpa) i opatrzone kwalifikowanym podpisem elektronicznym, podpisem

było wyraźne wskazanie, iż wniesienie skargi nie zamyka drogi do sięgnięcia po inne instrumenty, np. wytoczenie powództwa o naruszenie dóbr osobistych – por. M. Górski, *Komentarz do art. 77 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 6.

963 Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 601. Prezes UODO nie opracował formularza skargi. Na swojej stronie internetowej wyjaśnia, w jaki sposób można złożyć skargę i jakie są jej obligatoryjne elementy (https://www.uodo.gov.pl/pl/526/2464, dostęp: 15.04.2023). Prezes UODO zachęca, by w pierwszej kolejności podmiot danych skierował swoje żądanie bezpośrednio do administratora lub podmiotu przetwarzającego, co może pozwolić na sprawne spełnienie żądania przez jego adresata. 20 czerwca 2023 r. EROD przyjęła wzór formularza skargi oraz potwierdzenia wpłynięcia skargi do organu, który może być stosowany fakultatywnie w sprawach transgranicznych (https://edpb.europa.eu/system/files/2023-06/edpb_20230620_templatecomplaintform_0.pdf, https://edpb.europa.eu/system/files/2023-06/edpb_20230620_template_acknowledgement_of_receipt_0.pdf, dostęp: 04.07.2023).

964 Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 679.

965 Por. motyw 146 preambuły do rozporządzenia 2016/679. Należy zgodzić się z J. Łuczak, że zasadne jest przyjęcie zaprezentowanego w tym motywie szerokiego rozumienia pojęcia naruszenia rozporządzenia 2016/679 także w kontekście wnoszenia skarg do organu nadzorczego – por. J. Łuczak, *Komentarz do art. 77 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 1024. Będzie to miało szczególne znaczenie w przypadku przetwarzania danych osobowych w myśl art. 6 ust. 1 lit. c oraz e rozporządzenia 2016/679, gdy podstawa prawna została określona w prawie państwa członkowskiego (por. art. 6 ust. 3 lit. b rozporządzenia 2016/679).

966 Jak wyjaśnia Prezes UODO, żądanie powinno być sformułowane jednoznacznie (np. skarżący powinien wskazać, że chodzi o usunięcie danych, wypełnienie obowiązku informacyjnego), a w przypadku kilku żądań zawartych w jednej skardze, nie mogą być one ze sobą sprzeczne – por. UODO, *Składanie skargi w formie tradycyjnej, w tym do protokołu w siedzibie Prezesa Urzędu*, https://uodo.gov.pl/pl/489/2247 (dostęp: 04.07.2023).

zaufanym[967] albo podpisem osobistym[968] lub kwalifikowaną pieczęcią elektroniczną[969] (art. 14 §1d kpa w związku z art. 14 §1a kpa). Kwalifikowany podpis elektroniczny może być wydany osobie fizycznej przez dostawcę usług zaufania. Uzyskanie takiego podpisu wiąże się z pewnym wydatkiem[970] i wymaga poświęcenia czasu w sytuacji, gdy konieczne jest osobiste stawiennictwo u dostawcy usług zaufania w celu sprawdzenia tożsamości. Do składania podpisu osobistego może służyć dowód osobisty[971]. W warstwie elektronicznej dowodu osobistego zamieszcza się certyfikat podpisu osobistego, jeśli osoba posiadająca pełną zdolność do czynności prawnych wyraziła na to zgodę przy składaniu wniosku o wydanie dowodu osobistego, a w przypadku osoby posiadającej ograniczoną zdolność do czynności prawnych – jeśli zgodę wyraził jeden z rodziców, opiekun lub kurator tej osoby (art. 12a ust. 3 pkt 2 i 3 ustawy o dowodach osobistych). Najłatwiejsze – z perspektywy wnoszącego skargę w postaci elektronicznej – wydaje się opatrzenie jej podpisem zaufanym, dostępnym z poziomu konta profilu zaufanego w systemie teleinformatycznym, za który odpowiada minister właściwy do spraw informatyzacji (art. 20aa ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[972]), ponieważ mimo obowiązku złożenia wniosku o utworzenie profilu, istnieją różne, przystępne sposoby potwierdzenia tożsamości[973], a korzystanie z usługi jest bezpłatne. Z profilu zaufanego może

[967] Podpis zaufany został zdefiniowany w art. 3 pkt 14a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz. U. z 2023 r. poz. 57 z późn. zm.) jako podpis elektroniczny, którego autentyczność i integralność są zapewniane przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji, zawierający określone w tym przepisie dane identyfikujące osobę, identyfikator środka identyfikacji elektronicznej, przy użyciu którego został złożony oraz czas jego złożenia.

[968] Podpis osobisty to według art. 2 ust. 1 pkt 9 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (t.j. Dz. U. z 2022 r. poz. 671 z późn. zm.) zaawansowany podpis elektroniczny, o którym mowa w art. 3 pkt 11 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.8.2014, s. 73), czyli podpis elektroniczny, który spełnia wymogi określone w art. 26 tego rozporządzenia (jest unikalnie przyporządkowany podpisującemu, umożliwia ustalenie tożsamości podpisującego, jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą, jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna).

[969] Kwalifikowany podpis elektroniczny i kwalifikowana pieczęć elektroniczna zostały zdefiniowane odpowiednio w art. 3 pkt 12 oraz pkt 27 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE. W myśl tych przepisów, kwalifikowany podpis elektroniczny to zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego, zaś kwalifikowaną pieczęcią elektroniczną jest zaawansowana pieczęć elektroniczna, która została złożona za pomocą kwalifikowanego urządzenia do składania pieczęci elektronicznej i która opiera się na kwalifikowanym certyfikacie pieczęci elektronicznej.

[970] Przykładowo, koszt rocznego korzystania z podpisu wydawanego przez Polską Wytwórnię Papierów Wartościowych wynosi ok. 320 zł (https://sklep.sigillum.pl/#/product/information?id=15, dostęp: 04.07.2023), natomiast przez Krajową Izbę Rozliczeniową – ok. 350 zł (https://www.elektronicznypodpis.pl/oferta/cennik/, dostęp: 04.07.2023).

[971] Por. art. 10a ust. 3 pkt 3 ustawy o dowodach osobistych.

[972] T.j. Dz. U. z 2023 r. poz. 57 z późn. zm.

[973] Jako przykład można wskazać potwierdzenie tożsamości poprzez uwierzytelnienie w systemie teleinformatycznym banku, który uzyskał zgodę ministra właściwego do spraw informatyzacji (por. art. 19a ust. 2a ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne), dzięki czemu nie jest konieczne osobiste stawiennictwo w punkcie potwierdzającym.

korzystać osoba posiadająca pełną lub ograniczoną zdolność do czynności prawnych (por. art. 3 pkt 14 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne), a zatem także dziecko, które ukończyło 13 lat.

W myśl art. 77 §1 kpa organ ma obowiązek w sposób wyczerpujący zebrać i rozpatrzyć cały materiał dowodowy. Dowodem mogą być w szczególności dokumenty, zeznania świadków, opinie biegłych i oględziny (art. 75 §1 kpa). Przepis art. 68 ust. 1 uodo z 2018 r. umożliwia Prezesowi UODO przeprowadzenie postępowania kontrolnego, także w związku z rozpatrywaniem skargi, jeżeli w toku postępowania zajdzie konieczność uzupełnienia dowodów, co sprzyja realizacji zasady prawdy obiektywnej (art. 7 kpa) i jest postrzegane jako dodatkowa ochrona wnoszącego skargę[974]. Warto także zwrócić uwagę na specyficzne postanowienie, jakie może wydać Prezes UODO stosownie do art. 70 ust. 1 uodo z 2018 r. – zobowiązujące do ograniczenia przetwarzania danych osobowych i wskazujące dopuszczalny zakres przetwarzania, jeżeli „w toku postępowania zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki". Wydanie postanowienia ma na celu zapobieżenie tym skutkom. Postanowienie ma charakter zabezpieczający, tymczasowy, a jego wydanie nie przesądza o sposobie rozstrzygnięcia sprawy[975]. W myśl art. 70 ust. 2 uodo z 2018 r., wskazany w postanowieniu termin obowiązywania ograniczenia przetwarzania nie może być dłuższy niż do dnia wydania decyzji kończącej postępowanie w sprawie. Źródła wprowadzenia w uodo z 2018 r. instytucji postanowienia zabezpieczającego można upatrywać w art. 58 ust. 2 lit. f rozporządzenia 2016/679, który do naprawczych uprawnień organu nadzorczego zalicza „wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania", dlatego zasadne jest skorzystanie ze wskazówek interpretacyjnych zawartych w motywie 67 preambuły do rozporządzenia 2016/679[976]. Prawodawca wyjaśnił w nim, że do metod ograniczenia przetwarzania można zaliczyć „czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania, uniemożliwienie użytkownikom dostępu do wybranych danych, lub czasowe usunięcie opublikowanych danych ze strony internetowej". Wprowadzenie do uodo 2018 r. omawianego postanowienia zasługuje na aprobatę, gdyż czas potrzebny na rozstrzygnięcie skomplikowanej sprawy co do meritum może się wydłużać, a sytuacja podmiotu danych nie powinna się przez to pogarszać – kluczowe jest przerwanie uprawdopodobnionego stanu

[974] Por. J. Behr, *Prawo do wniesienia skargi do organu nadzorczego*, [w:] J. Behr, M. Błażewski, *Środki prawne ochrony danych osobowych*, Wrocław 2018, s. 188.
[975] Por. P. Litwiński, *Komentarz do art. 70 uodo z 2018 r.*, [w:] P. Litwiński (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, Legalis, teza 3. Zgodnie z art. 70 ust. 3 uodo z 2018 r., na postanowienie przysługuje skarga do sądu administracyjnego.
[976] Por. M. Sakowska-Baryła, *Komentarz do art. 58 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 15.

naruszenia. W kontekście świadczenia usług społeczeństwa informacyjnego szczególnie znacząca wydaje się możliwość nakazania ograniczenia przetwarzania w sprawach związanych z upublicznieniem danych osobowych dziecka.

Postępowanie prowadzone w wyniku złożenia skargi kończy się wydaniem przez Prezesa UODO decyzji administracyjnej, na mocy której może m.in. nakazać przywrócenie stanu zgodnego z prawem[977]. Poprzez decyzję administracyjną organ kształtuje prawa i obowiązki jej adresata w konkretnej sytuacji[978]. Na kanwie rozważań o adekwatności wydawania decyzji administracyjnej do realizacji zadań organu nadzorczego ds. ochrony danych osobowych, w literaturze zaprezentowano stanowisko, że władczy charakter można przypisać w szczególności zadaniom organu nadzorczego wymienionym w art. 58 ust. 2 rozporządzenia 2016/679, do których zalicza się m.in. nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienie żądania podmiotu danych wynikającego z praw przysługujących mu na mocy rozporządzenia 2016/679 (art. 58 ust. 2 lit. c rozporządzenia 2016/679), zatem w konsekwencji wykonywanie tych kompetencji następuje w drodze decyzji administracyjnej[979]. Sprawa ze skargi podmiotu danych kwalifikowana jest jako indywidualna sprawa administracyjna, ponieważ rozstrzygnięcie organu nadzorczego konkretyzuje uprawnienia i obowiązki stron stosunku administracyjnoprawnego, którym przysługuje – w myśl art. 78 ust. 1 rozporządzenia 2016/679 – prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego[980] – wniesienia skargi do sądu administracyjnego.

1.3.2 Reprezentowanie dziecka przez przedstawiciela ustawowego i samodzielny udział dziecka w postępowaniu

Po nakreśleniu ogólnych proceduralnych ram postępowania należy postawić pytanie, w jaki sposób prawo do wniesienia skargi do organu nadzorczego może być wykonywane w przypadku, gdy podmiotem danych jest dziecko? Przepis art. 28 kpa stanowi, że stroną jest każdy, czyjego interesu prawnego lub obowiązku dotyczy postępowanie albo kto żąda czynności organu ze względu na swój interes prawny lub obowiązek. Interes prawny istnieje zawsze wtedy, gdy norma prawna wynikająca z materialnego prawa powszechnie obowiązującego przewiduje konkretne uprawnienie[981]. Źródłem takiej normy może być m.in. Konstytucja, o ile z jej przepisów możliwe

[977] Por. Sprawozdanie z działalności Prezesa UODO w 2021 r., https://uodo.gov.pl/pl/487/2279 (dostęp: 04.07.2023), s. 35.
[978] Por. J. Izdebski, hasło „decyzja administracyjna", [w:] M. Domagała, A. Haładyj, S. Wrzosek (red.), *Encyklopedia prawa administracyjnego*, Warszawa 2010, s. 64.
[979] Por. M. Sakowska-Baryła, Joanna Wyporska-Frankiewicz, *Zadania i decyzje Prezesa Urzędu Ochrony Danych Osobowych*, „Roczniki Nauk Prawnych" 2022, nr 1, s. 69 i s. 72.
[980] Por. G. Sibiga, *Skarga do organu nadzorczego…*, s. 8.
[981] Por. Z. Kmieciak, J. Wegner, *Komentarz do art. 28 kpa*, [w:] Z. Kmieciak, J. Wegner, M. Wojtuń, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2023, s. 211-213 i tam powołana literatura.

jest wyinterpretowanie normy kreującej konkretne uprawnienie, a także regulacje służące ochronie podstawowych praw i wolności[982]. W świetle art. 51 Konstytucji, art. 8 KPP i przepisów rozporządzenia 2016/679 nie ulega wątpliwości, że osobie, której dane dotyczą, przysługują – w ujęciu ogólnym – prawo do ochrony danych osobowych, zaś w ujęciu szczegółowym – konkretne uprawnienia, przewidziane zwłaszcza w art. 12-22 rozporządzenia 2016/679, i ma ona interes prawny w tym, by były one respektowane. W przypadku sprawy ze skargi na przetwarzanie danych osobowych, przymiot strony przysługuje podmiotowi danych, a zatem – w omawianym przypadku – dziecku. Osoba fizyczna może być stroną bez względu na swój wiek – co do zasady od urodzenia (przymiot strony przysługuje także dziecku poczętemu, jeśli urodzi się żywe) do śmierci[983]. Jak zauważa R. Suwaj, „nie każda jednak osoba fizyczna, która może występować w postępowaniu administracyjnym jako strona, ma możliwość samodzielnego podejmowania prawnie wiążących czynności procesowych. Nie każda osoba fizyczna posiada więc tzw. zdolność procesową, pomimo posiadania interesu prawnego lub obowiązku w konkretnej sprawie administracyjnej"[984]. Stosownie do art. 30 §1 i §2 kpa, osoby fizyczne, które nie posiadają zdolności do czynności prawnych, działają przez swoich ustawowych przedstawicieli, zaś zdolność do czynności prawnych stron ocenia się według przepisów prawa cywilnego. Nie ulega zatem wątpliwości, że skargę do Prezesa UODO może wnieść przedstawiciel ustawowy dziecka, które nie posiada zdolności do czynności prawnych. Gdyby takie dziecko samodzielnie wniosło skargę, co jest mało prawdopodobne szczególnie w przypadku najmłodszych, żądanie wszczęcia postępowania należałoby uznać za bezskuteczne, a organ powinien wydać postanowienie o odmowie wszczęcia postępowania przy założeniu, że bezskuteczność żądania ma charakter bezwzględny[985]. Natomiast w świetle powyższych przepisów kpa w przypadku dziecka posiadającego ograniczoną zdolność do czynności prawnych nie istnieje wymóg reprezentowania go przez przedstawiciela ustawowego[986]. Należy zatem uznać, że w związku z poczuciem zaistnienia naruszenia dotyczącego przetwarzania danych osobowych dziecka, które ukończyło 13 lat, skargę do Prezesa UODO może skutecznie wnieść samo dziecko lub jego przedstawiciel ustawowy – brak wymogu zastępowania przez niego dziecka nie wydaje się wykluczać takiej możliwości. Udział przedstawiciela ustawowego, działającego w imię dobra dziecka i posiadającego większe

[982] Tamże, s. 214.
[983] Por. E. Szewczyk, M. Szewczyk, *Strona w postępowaniu administracyjnym*, [w:], G. Łaszczyca, A. Matan (red.), *System Prawa Administracyjnego Procesowego*: W. Chróścielewski (red.), tom II część 1. *Zakres przedmiotowy i podmiotowy postępowania administracyjnego ogólnego*, Warszawa 2018, s. 303-304.
[984] R. Suwaj, *Wiek uczestników postępowania administracyjnego a skuteczność podejmowanych przez nich czynności prawnych*, „Białostockie Studia Prawnicze" 2010, nr 7, s. 198.
[985] Por. Z. R. Kmiecik, *Etap wszczęcia postępowania administracyjnego ogólnego*, [w:] G. Łaszczyca, A. Matan (red.), *System Prawa Administracyjnego Procesowego*: C. Martysz (red.), tom II część 4. *Dynamika postępowania administracyjnego ogólnego*, Warszawa 2021, s. 78-79.
[986] Tamże, s. 73.

doświadczenie życiowe, pozwalające na umiejętne załatwianie spraw „urzędowych", z pewnością miałby korzystny wpływ na przebieg postępowania. Należy jednak przewidzieć, że nie każdy przedstawiciel ustawowy kieruje się dobrem dziecka – o czym świadczy przykładowo zjawisko publikowania na portalach społecznościowych zdjęć kompromitujących dziecko (*sharenting*), świadczące o lekceważeniu jego prawa do ochrony danych osobowych i prawa do prywatności, a potencjalnie także eksponujące je na zagrożenia o trudnych do przewidzenia skutkach. Dziecko może mieć obawy przed podzieleniem się swoimi problemami z rodzicem, zwłaszcza jeśli korzysta z usług profilaktycznych lub doradczych – które z powodu potrzeby zapewnienia dziecku ochrony i poufności, niekiedy także wobec przedstawiciela ustawowego, nie powinny być świadczone za jego zgodą[987] – a poczucie naruszenia zasad ochrony danych osobowych związane jest z korzystaniem z tego rodzaju usług społeczeństwa informacyjnego. Pomijając skrajne przykłady, konieczne jest także wzięcie pod uwagę, że przedstawiciel ustawowy może nie dysponować odpowiednią wiedzą, np. nie znać lub nie rozumieć warunków świadczenia usługi, z której korzysta dziecko[988], a w dobie ogromnej popularności dzielenia się szczegółami z życia prywatnego w internecie, bagatelizować negatywne odczucia dziecka związane z korzystaniem z usług społeczeństwa informacyjnego. Mając na uwadze, że dzieckiem-użytkownikiem takich usług jest nastolatek, w grę mogą wchodzić charakterystyczne dla okresu dojrzewania bariery w komunikacji z rodzicem-przedstawicielem ustawowym. Identyfikacja i analiza przyczyn, z których dostrzeżenie przez przedstawiciela ustawowego potrzeby, a w następstwie podjęcie działań w celu ochrony praw dziecka w drodze wniesienia skargi do Prezesa UODO jest niemożliwe lub trudne, wykracza poza przedmiot niniejszej rozprawy. Niemniej nie ulega wątpliwości, że takie problemy mogą występować.

Dopuszczalność samodzielnego wniesienia skargi do Prezesa UODO przez dziecko korzystające z usług społeczeństwa informacyjnego, które ukończyło 13 lat, nie powinna być kwestionowana ze względu na wskazane wyżej przepisy kpa. Ponadto mając w pamięci jeden z celów reformy ochrony danych osobowych – objęcie szczególną ochroną praw dziecka związanych z przetwarzaniem jego danych osobowych – interpretacja przepisów proceduralnych i praktyka organu nadzorczego powinny być ukierunkowane na umożliwienie dziecku wykonywania jego uprawnień w jak najszerszym zakresie, bez stosowania ograniczeń, które nie byłyby wyraźnie uzasadnione okolicznościami danej sprawy. Warto także przywołać art. 12 ust. 1 KPD, zgodnie z którym dziecko zdolne do kształtowania swych własnych poglądów ma prawo do ich swobodnego wyrażania we wszystkich dotyczących go sprawach. Przepis art. 12 ust. 2 KPD

[987] Por. motyw 38 preambuły rozporządzenia 2016/679.
[988] Por. S. van der Hof, *I Agree. . . Or Do I? — A Rights-Based Analysis of the Law On Children's Consent in the Digital World*, „Wisconsin International Law Journal" 2017, vol. 34, s. 129.

stanowi, że w celu realizacji powyższego prawa „dziecko będzie miało w szczególności zapewnioną możliwość wypowiadania się w każdym postępowaniu sądowym i administracyjnym, dotyczącym dziecka, bezpośrednio lub za pośrednictwem przedstawiciela bądź odpowiedniego organu, zgodnie z zasadami proceduralnymi prawa wewnętrznego". Ciążący na organie nadzorczym na podstawie art. 57 ust. 2 rozporządzenia 2016/679 obowiązek ułatwiania wnoszenia skarg, w związku z wynikającym z art. 57 ust. 1 lit. a rozporządzenia 2016/679 zadaniem polegającym na upowszechnianiu w społeczności wiedzy m.in. o prawach związanych z przetwarzaniem danych osobowych i poświęcaniu szczególnej uwagi takim działaniom skierowanym do dzieci, mógłby być realizowany poprzez kampanie edukacyjne popularyzujące wiedzę o możliwości i sposobach wniesienia skargi, rozpowszechnianie materiałów informacyjnych o charakterze poradnikowym, skierowanych nie tylko do przedstawicieli ustawowych dzieci, ale także do nich bezpośrednio jako do podmiotów danych. Za przykład dobrej praktyki można uznać opublikowanie przez irlandzki organ nadzorczy ds. ochrony danych osobowych wytycznych w sprawie składania skarg przez dzieci lub ich przedstawicieli ustawowych, dotyczących przetwarzania danych osobowych dzieci[989]. Jak wyjaśniono w tym dokumencie, irlandzkie prawo nie określa, od którego roku życia dziecko może wykonywać swoje uprawnienia, zatem organ nadzorczy nie widzi przeszkód, by działało samodzielnie, o ile to potrafi i służy to jego dobru. Zaangażowanie przedstawiciela ustawowego w złożenie skargi do organu nadzorczego powinno być dopuszczalne, jeśli tego chce dziecko i nie wolno uniemożliwiać mu wykonywania swoich uprawnień z powodu wieku ani dojrzałości. Irlandzki organ nadzorczy trafnie zwraca uwagę, że im starsze jest dziecko – zwłaszcza gdy zbliża się do ukończenia 18. roku życia – tym bardziej prawdopodobne jest, że samo będzie korzystało z praw przysługujących mu w związku z przetwarzaniem danych osobowych[990].

Procedura rozpatrywania skarg przez Prezesa UODO jest dość sformalizowana – nie bez znaczenia wydaje się fakt, że kodeks postępowania administracyjnego został uchwalony ponad 60 lat temu, w zupełnie innych realiach społeczno-gospodarczych[991], gdy w Polsce nie występował fenomen usług społeczeństwa informacyjnego ani nie obowiązywały przepisy w dziedzinie ochrony danych osobowych. Można ubolewać, że szczególne regulacje dotyczące postępowania przed Prezesem UODO, zawarte w uodo z 2018 r., milczą na temat procedury rozpatrywania skarg w przedmiocie przetwarzania danych osobowych dzieci. Warte rozważenia byłoby wprowadzenie

[989] Data Protection Commission, *Children, Parents…,* s. 1-8.
[990] Tamże, s. 3-4.
[991] Próby uwspółcześnienia przepisów kpa odnoszą się przede wszystkim do kwestii doręczeń elektronicznych i bywają przedmiotem krytyki – szerzej na ten temat por. G. Sibiga, *Jak nie informatyzować administracji*, „Rzeczpospolita" 18.07.2022 r., https://www.rp.pl/opinie-prawne/art36713481-grzegorz-sibiga-jak-nie-informatyzowac-administracji (dostęp: 15.04.2023); A. Cebera, *Nowa procedura doręczeń elektronicznych w postępowaniu administracyjnym*, „Ius Novum" 2023, nr 2, s. 158-180.

rozwiązań mających na celu ułatwienie im korzystania z prawa do wniesienia skargi do organu nadzorczego, szczególnie w kontekście korzystania z usług społeczeństwa informacyjnego oferowanych bezpośrednio dzieciom, co przyczyniłoby się do osiągnięcia celu reformy ochrony danych osobowych.

1.3.3 Reprezentowanie dziecka przez organizację działającą na rzecz ochrony danych osobowych

Przepis art. 57 ust. 1 lit. f rozporządzenia 2016/679 przewiduje, że organ nadzorczy, oprócz skarg podmiotów danych, rozpatruje skargi wniesione przez podmiot, organizację lub zrzeszenie zgodnie z art. 80 rozporządzenia 2016/679 – czyli przez działający w imieniu osoby, które dane dotyczą, podmiot niemający charakteru zarobkowego, który został należycie ustanowiony zgodnie z prawem państwa członkowskiego, ma cele statutowe leżące w interesie publicznym i działa w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych[992]. Stosownie do art. 61 uodo z 2018 r., organizacja społeczna może występować w postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych „za zgodą osoby, której dane dotyczą, w jej imieniu i na jej rzecz". Ponadto w tym przepisie ustawodawca wskazał, że chodzi o organizację społeczną, o której mowa w art. 31 §1 kpa – tzn. podmiot, który w sprawie innej osoby może m.in. żądać wszczęcia postępowania, „jeżeli jest to uzasadnione celami statutowymi tej organizacji i gdy przemawia za tym interes społeczny".

Ratio legis art. 57 ust. 1 lit. f i art. 80 rozporządzenia 2016/679 należy upatrywać w dążeniu do ułatwienia wykonywania uprawnień osobie, która napotyka na trudności – związane przykładowo z niemożnością skorzystania z pomocy profesjonalnego pełnomocnika z uwagi na koszty – dzięki nieodpłatnemu wsparciu ze strony organizacji wyspecjalizowanej w dziedzinie ochrony danych osobowych[993]. Instytucja reprezentowania podmiotu danych przez organizację działającą na rzecz ochrony danych osobowych może mieć szczególnie doniosłe znaczenie w przypadku wykonywania uprawnień przez dziecko korzystające z usług społeczeństwa informacyjnego. Niewątpliwie działanie na rzecz podmiotu danych w takim kontekście przetwarzania danych osobowych wymaga nie tylko znajomości prawnych regulacji, ale i nierzadko orientowania się w technicznych aspektach działania tego typu usług. Bezpłatny dostęp do eksperckiego poradnictwa – co naturalnie poprzedza sposobność działania w czyimś imieniu i przykładowo sporządzenia skargi do organu nadzorczego[994] – może przyczyniać się do wzmocnienia poziomu ochrony danych osobowych dzieci. Ponadto w literaturze zauważa się, że

[992] Dalej jako: „organizacja działająca na rzecz ochrony danych osobowych".
[993] Por. P. Fajgielski, *Ogólne rozporządzenie…,* s. 690.
[994] Por. I. Bogucka, *Komentarz do art. 61 uodo z 2018 r*., [w:]. D. Lubasz (red.), *Ustawa o ochronie danych…*, s. 336.

przewidziana w art. 80 rozporządzenia 2016/679 możliwość zwrócenia się do organizacji działającej na rzecz ochrony danych osobowych toruje dziecku drogę do realizacji swoich uprawnień w sytuacji, gdy nie może polegać na działaniu przedstawiciela ustawowego lub gdy wręcz to on dopuszcza się czynów godzących w prawa dziecka[995]. Zwrócenie się przez dziecko do organizacji działającej na rzecz ochrony danych osobowych o pomoc nie powinno zatem być warunkowane aprobatą, a w skrajnych przypadkach nawet wiedzą przedstawiciela ustawowego. Z perspektywy legalności przetwarzania danych osobowych dziecka, realizacja statutowych zadań takiej organizacji, polegających na świadczeniu pomocy w sprawach dotyczących wykonywania uprawnień związanych z przetwarzaniem danych osobowych, mogłaby być traktowana podobnie jak usługa doradcza oferowana bezpośrednio dziecku, o której mowa w motywie 38 preambuły do rozporządzenia 2016/679 – do korzystania z której nie jest wymagana zgoda na przetwarzanie udzielona przez przedstawiciela ustawowego.

Wątpliwości może wzbudzać to, w jaki sposób przedstawiciel ustawowy lub dziecko mogą skutecznie umocować organizację działającą na rzecz ochrony danych osobowych do działania w imieniu dziecka. Przepisy uodo z 2018 r. nie odnoszą się do tej kwestii, a tym bardziej rozporządzenia 2016/679 z racji autonomii proceduralnej państw członkowskich UE. W sprawach nieuregulowanych w uodo z 2018 r. stosuje się subsydiarnie kpa, co mogłoby wskazywać, że właściwe byłoby odwołanie się do art. 32 i 33 kpa dotyczących możliwości i trybu ustanowienia pełnomocnika strony. Z kolei z powodu dużej ogólności tych przepisów uważa się, że niezbędne jest sięgnięcie do regulacji z zakresu prawa cywilnego i stosowanie ich na zasadzie analogii w celu „sprecyzowania możliwych zakresów umocowania"[996]. Stosownie do art. 88 §1 ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego[997], pełnomocnictwo może być ogólne, do prowadzenia poszczególnych spraw albo do niektórych czynności. W razie wątpliwości co do zakresu pełnomocnictwa, organ prowadzący postępowanie winien na podstawie art. 64 §2 kpa wezwać stronę do jego doprecyzowania[998]. Mimo, że w orzecznictwie zaprezentowano pogląd, że zwięzłość przepisów kpa dotyczących ustanowienia pełnomocnika świadczy o tym, że ustawodawca nie zamierzał sformalizować związanych z tym wymogów[999], istnieją podstawy do polemizowania z tym stanowiskiem[1000] i obaw, że umocowanie organizacji działającej na rzecz

[995] Por. E. Lievens, C. Vander Maelen, *A Child's Right to be Forgotten: Letting Go of the Past and Embracing the Future?*, „Latin American Law Review" 2019, nr 2, s. 71-72; J. Maniszewska-Ejsmont, *Sharenting a prawa dziecka – rozważania nad władzą rodzicielską w dobie mediów społecznościowych*, „Palestra" 2022, nr 4, s. 82.
[996] J. Chmielewski, *Pełnomocnik i pełnomocnictwo w ogólnym postępowaniu administracyjnym*, „Monitor Prawniczy" 2016, nr 11, s. 590 i tam powołane orzecznictwo.
[997] T.j. Dz. U. z 2023 r. poz. 1550 z późn. zm., dalej jako: „kpc".
[998] J. Chmielewski, *Pełnomocnik i pełnomocnictwo…*, s. 590.
[999] Por. wyrok NSA z 04.07.2004 r., sygn. II OSK 941/05.
[1000] Por. A. Wróbel, *Komentarz do art. 32 kpa*, [w:] M. Jaśkowska, M. Wilbrandt-Gotowicz, A. Wróbel, *Komentarz aktualizowany do Kodeksu postępowania administracyjnego*, LEX 2023.

ochrony danych osobowych nie będzie trywialne dla niedoświadczonej osoby. Należy jednak dostrzec także kontrargument, iż skoro w postępowaniu ma brać udział wyspecjalizowany podmiot, wszystkie sporządzone przez niego pisma – przygotowane także na etapie poprzedzającym wniesienie skargi do organu nadzorczego – będą odpowiadały wymogom przewidzianym w kpa.

O ile możliwość umocowania przez przedstawiciela ustawowego organizacji działającej na rzecz ochrony danych osobowych (lub innego pełnomocnika) do reprezentowania dziecka nie wzbudza wątpliwości[1001], o tyle może je wywoływać skuteczność ustanowienia takiego pełnomocnika przez samo dziecko. Zgodnie z art. 30 §2 kpa, zasadą jest działanie osoby nieposiadającej zdolności do czynności prawnych przez przedstawiciela ustawowego. Natomiast przy założeniu, że osoba posiadająca ograniczoną zdolność do czynności prawnych ma zdolność procesową, w konsekwencji należy także przyjąć, że może ustanowić pełnomocnika. Biorąc pod uwagę, że intencją unijnego prawodawcy jest jak najdalej idące ułatwienie podmiotowi danych wykonywanie jego uprawnień, w tym także z pomocą organizacji działającej na rzecz ochrony danych osobowych, kwestia jej umocowania przez dziecko – w zasadzie wyrażenia zgody, nawiązując do brzmienia art. 61 uodo z 2018 r. – nie powinna być kwestionowana, gdyż mogłoby to skutkować ograniczaniem praw dziecka.

Wydaje się, że nie ma przeszkód by organ nadzorczy – w ramach wykonywania swojego zadania, o którym mowa w art. 57 ust. 1 lit. b rozporządzenia 2016/679 – upowszechniał wiedzę o rozwiązaniach ułatwiających podmiotom danych wykonywanie ich uprawnień poprzez skorzystanie z pomocy organizacji działających na rzecz ochrony danych osobowych, w tym o możliwości wnoszenia przez nie skarg w imieniu osób, których dane dotyczą[1002], a także zachęcał same organizacje do wzmożonej aktywności w sferze ochrony danych osobowych dzieci. Warto postulować publikowanie na stronie internetowej organu nadzorczego wykazu organizacji działających na rzecz ochrony danych osobowych, gotowych do reprezentowania dzieci w myśl art. 80 rozporządzenia 2016/679.

1.3.4 Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego

W motywie 141 preambuły do rozporządzenia 2016/679 prawodawca uwypuklił, że każdy ma prawo do wniesienia skargi do organu nadzorczego oraz prawo do skutecznego środka ochrony

[1001] Por. J. Wegner, *Komentarz do art. 32 kpa*, [w:] Z. Kmieciak, J. Wegner, M. Wojtuń, *Kodeks postępowania administracyjnego…*, s. 273.
[1002] Takie informacje zamieścił na swojej stronie internetowej brytyjski organ nadzorczy (ICO, *What rights do children have?*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-rights-do-children-have/#a5, dostęp: 15.04.2023).

prawnej przed sądem, także wobec działań tego organu. Ten postulat znalazł odzwierciedlenie w części normatywnej – art. 78 rozporządzenia 2016/679. W przypadku decyzji administracyjnej wydanej przez Prezesa UODO, za taki środek ochrony prawnej można uznać prawo jej zaskarżenia do sądu administracyjnego[1003]. Przepis art. 26 §1 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi[1004] przyznaje – w przypadku osób fizycznych – zdolność do czynności w postępowaniu w sprawach sądowoadministracyjnych osobom posiadającym pełną zdolność do czynności prawnych. Z kolei art. 26 §2 ppsa przewiduje, że „osoba fizyczna ograniczona w zdolności do czynności prawnych ma zdolność do czynności w postępowaniu w sprawach wynikających z czynności prawnych, których może dokonywać samodzielnie". Wątpliwości może budzić to, czy dziecko posiadające ograniczoną zdolność do czynności prawnych może samodzielnie zaskarżyć decyzję Prezesa UODO do sądu administracyjnego.

W orzecznictwie znane są przypadki – w innych sprawach niż z zakresu ochrony danych osobowych[1005] – wniesienia skargi do sądu administracyjnego przez nastolatka posiadającego ograniczoną zdolność do czynności prawnych, któremu organy, a następnie sądy administracyjne odmawiały podjęcia czynności bez uzyskania potwierdzenia ze strony przedstawicieli ustawowych. W wyniku wniesionej w jednej z tych spraw skargi kasacyjnej NSA orzekł, że zdolność procesowa przysługująca osobie z ograniczoną zdolnością do czynności prawnych na podstawie art. 26 §2 ppsa polega „na posiadaniu zdolności procesowej w pełnym zakresie, ale jedynie w sprawach wynikających z czynności prawnych, których taka osoba może dokonywać samodzielnie", zaś „dopuszczalność zastosowania w konkretnej sprawie sądowoadministracyjnej art. 26 § 2 p.p.s.a. musi podlegać szczegółowej analizie w kontekście możliwości dokonania samodzielnie danej czynności prawnej przez osobę o ograniczonej zdolności prawnej"[1006]. Z kolei w postanowieniu wydanym w drugiej sprawie, również w związku z rozpatrywaniem skargi kasacyjnej – wniesionej m.in. przez Rzecznika Praw Obywatelskich i Rzecznika Praw Dziecka – NSA rozwinął kluczowe dla oceny dopuszczalności zastosowania art. 26 §2 ppsa zagadnienie czynności prawnych, których osoba posiadająca ograniczoną zdolność do czynności prawnych może dokonywać samodzielnie, poprzez podanie przykładów[1007] regulacji o charakterze

[1003] Por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 78 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 2.
[1004] T.j. Dz. U. z 2023 r. poz. 259 z późn. zm., dalej jako: „ppsa".
[1005] Por. postanowienie WSA w Szczecinie z dnia 28.06.2016 r., sygn. II SAB/Sz 64/16; postanowienie WSA w Warszawie z dnia 21.03.2017 r., sygn. II SAB/Wa 155/16. Dotyczyły odpowiednio samodzielnego działania przez nastolatka, posiadającego ograniczoną zdolność do czynności prawnych, w kontekście uzyskania fotokopii aktu zgonu swojego dziadka i uzyskania dostępu do informacji publicznej.
[1006] Postanowienie NSA z dnia 11.10.2016 r., sygn. II OSK 2238/16.
[1007] Te same przykłady zostały przedstawione w literaturze – por. B. Adamiak, *Skarga i skarga kasacyjna w postępowaniu sądowoadministracyjnym. Komentarz*, Warszawa 2014, s. 211.

administracyjnoprawnym przewidujących dokonywanie czynności prawnych przez osoby niepełnoletnie i uznał, że w sprawach takich kategorii posiadają one zdolność do czynności w postępowaniu sądowoadministracyjnym. NSA podał mianowicie jako przykłady art. 6 ust. 2, art. 7 ust. 1 i 2, art. 8 ustawy z dnia 2 kwietnia 2009 r. o obywatelstwie polskim[1008], zgodnie z którymi działania wpływające na obywatelstwo małoletniego, który ukończył 16 lat, wymagają jego zgody, a także art. 8 ust. 2, 3, 4 ustawy z dnia 17 października 2008 r. o zmianie imienia i nazwiska[1009], dotyczące wyrażenia zgody przez małoletniego, który ukończył 13 lat, na zmianę swojego nazwiska wskutek zmiany nazwiska jednego z rodziców. NSA sformułował wniosek, że „zdolność procesową w danej sprawie sądowoadministracyjnej należy wyprowadzić ze zdolności do dokonania konkretnej czynności prawnej, której sprawa ta dotyczy, czy z której się wywodzi, a więc ustalić ją w oparciu o uprawnienia do samodzielnego działania na gruncie materialnoprawnym. (…) analizując zakres samodzielności procesowej skarżącego konieczne jest odwołanie się do przedmiotu jego żądania na gruncie materialnoprawnym”[1010]. Na gruncie rozporządzenia 2016/679 – w kontekście świadczenia usług społeczeństwa informacyjnego – za takie uprawnienie należy uznać przewidzianą w przypadkach określonych w art. 8 ust. 1 rozporządzenia 2016/679 możliwość wyrażenia przez dziecko zgody na przetwarzanie danych osobowych bez udziału przedstawiciela ustawowego. Opowiedzenie się przez Rzecznika Praw Dziecka i Rzecznika Praw Obywatelskich w swoich skargach kasacyjnych, wniesionych w sprawie o sygn. I OSK 2500/16, za możliwie jak najszerszym umożliwieniu dziecku samodzielnego działania w ramach postępowań[1011] świadczy o tym, że zbyt rygorystyczna interpretacja przepisów ogranicza prawa dziecka, co jest rzecz jasna niepożądanym zjawiskiem. Na kanwie przepisów o dostępie do informacji publicznej i art. 13 KPD Rzecznik Praw Dziecka zauważył, że państwo powinno unikać „arbitralnych i zbyt rygorystycznych ograniczeń”[1012]. Arbitralność rozstrzygnięć jest realnym zagrożeniem[1013]. Uznając uniwersalność powyższego stanowiska Rzecznika Praw Dziecka, uprawnione jest przeniesienie go także na grunt regulacji mających na celu ochronę innych praw dziecka – w tym także prawa do ochrony danych osobowych i wykonywania uprawnień wywodzących się z art. 8 ust. 1 rozporządzenia 2016/679.

[1008] T.j. Dz. U. z 2022 r. poz. 465 z późn. zm.
[1009] T.j. Dz. U. z 2021 r. poz. 1988.
[1010] Postanowienie NSA z dnia 21.03.2021 r., sygn. I OSK 2500/16.
[1011] Należy odnotować, że NSA nie podzielił przedstawionych przez Rzeczników argumentów i interpretacji przepisów.
[1012] Cytat pochodzi z uzasadnienia do postanowienia NSA z dnia 21.03.2021 r., sygn. I OSK 2500/16 – fragmentu, w którym NSA sparafrazował główne motywy skargi kasacyjnej Rzecznika Praw Dziecka.
[1013] W sprawie o sygn. II OSK 2238/16 NSA stwierdził, że sąd I instancji nie przeprowadził szczegółowej analizy dopuszczalności zastosowania art. 26 § 2 ppsa w przypadku wniesienia skargi przez małoletniego, przez co nie miał możliwości odniesienia się do zarzutów skarg kasacyjnych – nie mógł podjąć się przeprowadzenia kontroli instancyjnej.

Ze względu na poziom skomplikowania procedury sądowoadministracyjnej, należy zauważyć, że rozważania o dopuszczalności samodzielnego złożenia przez dziecko skargi do sądu administracyjnego i podejmowania czynności w toku postępowania mają bardziej teoretyczny charakter – trudno bowiem spodziewać się, że przeciętne dziecko wie o takiej instytucji i umiałoby z niej skorzystać. Zakładając jednak, że potencjalnie może się to wydarzyć, rutynowe negowanie zdolności procesowej podmiotu danych posiadającego ograniczoną zdolność do czynności prawnych budziłoby duże wątpliwości i mogłoby skutkować utrudnieniem realizacji jednego z celów unijnej reformy ochrony danych osobowych – wzmocnienia praw dziecka. Wniesienie do sądu administracyjnego skargi na decyzję Prezesa UODO przez dziecko posiadające ograniczoną zdolność do czynności prawnych nie powinno być kwestionowane bez uprzedniego, drobiazgowego zbadania możliwości zastosowania art. 26 § 2 ppsa w konkretnej sprawie.

1.4 Wszczęcie postępowania przez organ nadzorczy z urzędu

Przez wszczęcie postępowania z urzędu w ogólnym ujęciu rozumie się sytuację, w której organ działa z własnej inicjatywy, bez żądania strony, realizując w ten sposób swój obowiązek lub uprawnienie „w zależności od tego, czy przepis prawa materialnego obliguje czy upoważnia go do uregulowania sytuacji prawnej poprzez podjęcie określonej decyzji”[1014] – działając zgodnie z wyrażoną w art. 6 kpa zasadą legalizmu.

W przypadku Prezesa UODO przepisem zobowiązującym go do niezwłocznego wszczęcia postępowania w sprawie naruszenia przepisów o ochronie danych osobowych jest art. 90 uodo z 2018 r., który materializuje się, jeśli organ powziął takie podejrzenie na podstawie informacji zgromadzonych w postępowaniu kontrolnym. Wszczęcie przez Prezesa UODO postępowania z urzędu może być także przykładowo wynikiem otrzymania zgłoszenia naruszenia ochrony danych osobowych, pozyskania informacji od innych organów nadzorczych ds. ochrony danych osobowych (art. 57 ust. 2 lit. f rozporządzenia 2016/679), od „podmiotów trzecich”[1015], jak i z innych źródeł, których katalog wydaje się otwarty[1016]. Do podjęcia działań przez Prezesa UODO, takich jak przeprowadzenie postępowania kontrolnego lub wszczęcie postępowania administracyjnego, mogą skłaniać doniesienia medialne. Pożądane byłoby monitorowanie

[1014] Z. R. Kmiecik, *Etap wszczęcia postępowania…*, s. 135.
[1015] Prezes UODO wszczął postępowanie w następstwie otrzymania informacji wskazującej na podejrzenie naruszenia ochrony danych osobowych od „podmiotu trzeciego”. W treści decyzji nie doprecyzowano, co organ rozumie przez to pojęcie. Wydaje się, że może chodzić o podmiot, który nie jest administratorem, podmiotem przetwarzającym ani podmiotem danych. Por. decyzja Prezesa UODO z 31.03.2023 r., sygn. DKN.5131.8.2021, https://www.uodo.gov.pl/decyzje/DKN.5131.8.2021 (dostęp: 11.07.2023).
[1016] Prezes UODO wszczął postępowanie z urzędu z uwagi na „sygnały na temat ewentualnych nieprawidłowości w procesie przetwarzania danych osobowych”, jednak w decyzji nie wskazał, w jaki sposób ani od kogo owe sygnały do niego dotarły – por. decyzja Prezesa UODO z 15.09.2019 r., sygn. ZSPU.440.200.2019, https://uodo.gov.pl/decyzje/ZSPU.440.200.2019 (dostęp: 11.07.2023).

mediów przez organ nadzorczy i sprawne podejmowanie zdecydowanych działań w wymagających tego sprawach, zwłaszcza dotyczących ochrony danych osobowych dzieci.

Prezes UODO stoi na stanowisku, że praktyki administratora w zakresie stosowanych zabezpieczeń, ich skuteczności oraz adekwatności do zagrożeń mogą być wyłącznie przedmiotem oceny w ramach postępowania wszczętego z urzędu, a nie ze skargi, ponieważ jej celem nie jest kontrola zabezpieczeń na wniosek podmiotu danych. Organ motywuje swój pogląd tym, że po pierwsze „funkcją skargi jest egzekwowanie przestrzegania przepisów o ochronie danych osobowych w operacjach przetwarzania danych, które bezpośrednio wpływają na osobę, której przetwarzane dane dotyczą" a po drugie „przyjęcie przeciwnego stanowiska oznaczałoby *de facto* możliwość zapoznania się przez wnioskodawcę, w ramach postępowania przed organem, ze sposobem zabezpieczenia danych (w tym danych innych osób) przez administratora danych osobowych, co samo w sobie zmniejsza poziom ochrony danych oraz może zwiększyć ryzyko ich naruszenia"[1017]. Mimo, że z pierwszym uzasadnieniem można byłoby polemizować, konkluzje Prezesa UODO, w tym drugi z argumentów, zasługują na aprobatę. Do obowiązków informacyjnych administratora nie należy w świetle art. 13 i 14 rozporządzenia 2016/679 wtajemniczanie podmiotu danych w kwestie związane z zabezpieczeniem danych.

Najczęstsze zagadnienia, które były przedmiotem postępowań wszczętych przez Prezesa UODO z urzędu w 2021 r., dotyczyły ocen ryzyka naruszenia praw i wolności podmiotów danych, wdrożenia środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa, doboru zabezpieczeń oraz metod testowania, mierzenia i oceniania ich skuteczności, wykonywania umowy powierzenia przetwarzania, informowania podmiotów danych o naruszeniu ochrony danych osobowych[1018].

2. Odpowiedzialność cywilna

Zgodnie z art. 82 ust. 1 rozporządzenia 2016/679, każdej osobie, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów rozporządzenia 2016/679, przysługuje prawo do uzyskania od administratora lub podmiotu przetwarzającego odszkodowania za poniesioną szkodę. Przepisy rozporządzenia 2016/679 uważa się – z uwagi na jego bezpośrednie stosowanie w państwach członkowskich UE – za samodzielną podstawę

[1017] Sprawozdanie z działalności Prezesa UODO w 2020 r., https://uodo.gov.pl/pl/487/2279 (dostęp: 04.07.2023), s. 76.
[1018] Sprawozdanie z działalności Prezesa UODO w 2021 r., https://uodo.gov.pl/pl/487/2279 (dostęp: 04.07.2023), s. 185-186. W sprawozdaniu nie podano, czy te postępowania dotyczyły przetwarzania danych osobowych dzieci w związku ze świadczeniem usług społeczeństwa informacyjnego.

odpowiedzialności odszkodowawczej[1019]. Jak wyjaśnił prawodawca w motywie 146 do preambuły rozporządzenia 2016/679, „pojęcie szkody należy interpretować szeroko, w świetle orzecznictwa Trybunału Sprawiedliwości, w sposób w pełni odzwierciedlający cele niniejszego rozporządzenia". Pojęcie szkody ma więc charakter autonomiczny, zaś z analizy orzecznictwa TSUE w sprawach z innych dziedzin niż ochrona danych osobowych można wyprowadzić wniosek, że jest ono pojmowane podobnie jak na gruncie polskiego prawa cywilnego[1020]. Teza o autonomii pojęcia szkody została potwierdzona w wyroku TSUE zapadłym już na kanwie art. 82 rozporządzenia 2016/679. Trybunał orzekł w nim także, że sam fakt naruszenia przepisów rozporządzenia 2016/679 nie wystarczy do przyznania odszkodowania, bowiem muszą zostać spełnione kumulatywnie przesłanki: 1) naruszenia przepisów rozporządzenia 2016/679; 2) poniesienia szkody przez osobę, której dane dotyczą; 3) istnienia związku przyczynowo-skutkowego między naruszeniem rozporządzenia 2016/679 a szkodą[1021]. W literaturze wskazuje się, że art. 82 rozporządzenia 2016/679 ma charakter prywatnoprawny i odnosi się do horyzontalnej relacji administratora (lub podmiotu przetwarzającego) z podmiotem danych[1022]. M. Gumularz porównuje art. 82 rozporządzenia 2016/679 „do konstrukcji odpowiedzialności odszkodowawczej z tytułu czynów niedozwolonych"[1023]. W zakresie nieuregulowanym w rozporządzeniu 2016/679 do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych stosuje się przepisy kc (art. 92 uodo z 2018 r.), zaś do postępowania w tych sprawach – w tym przypadku w zakresie nieuregulowanym w uodo z 2018 r. – stosuje się przepisy kpc (art. 100 uodo z 2018 r.).

Administrator ponosi odpowiedzialność w szerszym zakresie niż podmiot przetwarzający, bowiem ciąży na nim „znacznie więcej obowiązków, gdyż to on decyduje o celach i sposobach przetwarzania danych, co pociąga za sobą szeroki zakres odpowiedzialności odszkodowawczej za naruszenie przepisów rozporządzenia"[1024]. Przepis art. 82 ust. 1 rozporządzenia 2016/679 stanowi, że podmiot przetwarzający odpowiada wyłącznie za szkody spowodowane przetwarzaniem, gdy nie dopełnił obowiązków, które są bezpośrednio nałożone na podmioty przetwarzające lub gdy działał poza zgodnymi z prawem poleceniami administratora lub wbrew takim poleceniom. Za

[1019] Por. R. Strugała, *RODO a odpowiedzialność odszkodowawcza. Podstawowe problemy odpowiedzialności za szkodę spowodowaną nieprawidłowym przetwarzaniem danych osobowych*, „Monitor Prawniczy" 2018, nr 17, s. 915 i tam powołana literatura.
[1020] Por. A. Pązik, *Szkoda wynikająca z naruszenia przepisów RODO. Wybrane problemy*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2020, nr 3, s. 133-137 i tam powołane orzecznictwo.
[1021] Por. wyrok TSUE z dnia 04.05.2023 r. w sprawie C-300/21, UI przeciwko Österreichische Post AG.
[1022] Por. N. Zawadzka, *Komentarz do art. 82 rozporządzenia 2016/679*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 1049.
[1023] M. Gumularz, *Wpływ regulacji odpowiedzialności odszkodowawczej w ogólnym rozporządzeniu o ochronie danych osobowych na systemy prawa prywatnego państw członkowskich*, „Europejski Przegląd Sądowy" 2017, nr 5, s. 33-34.
[1024] P. Fajgielski, *Ogólne rozporządzenie…*, s. 697.

przykład takiego postępowania można uznać działanie niezgodnie z warunkami przewidzianymi w umowie, na mocy której administrator powierzył mu przetwarzanie[1025]. Należy jednak zaznaczyć, że nieuprawnione wejście przez podmiot przetwarzający w rolę administratora – tzn. własnowolne decydowanie o celach i sposobach przetwarzania danych osobowych, które zostały mu powierzone – powoduje, że będzie odpowiadał za to przetwarzanie jak administrator (por. art. 28 ust. 10 rozporządzenia 2016/679). Jeśli w przetwarzaniu bierze udział więcej niż jeden podmiot (np. administrator i podmiot przetwarzający, administratorzy działający jako współadministratorzy), odpowiadają one solidarnie za całą szkodę (por. art. 82 ust. 4 rozporządzenia 2016/679), zaś podmiot, który zapłacił odszkodowanie za całą wyrządzoną szkodę, może żądać od pozostałych zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność (por. art. 82 ust. 5 rozporządzenia 2016/679).

Według art. 82 ust. 3 rozporządzenia 2016/679, administrator lub podmiot przetwarzający są zwolnieni z odpowiedzialności, jeśli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody. Dla przykładu, mogą oni dążyć do wykazania, że wdrożyli adekwatne do zagrożeń techniczne i organizacyjne środki bezpieczeństwa, przeprowadzili ocenę skutków i zastosowali się do zaleceń organu nadzorczego, przekazywali dane osobowe wyłącznie do państw trzecich, które zapewniają odpowiedni poziom ochrony danych osobowych[1026]. Z perspektywy obrony przed roszczeniami kluczowe dla tych podmiotów jest więc przestrzeganie zasady rozliczalności. W praktyce obrona przed roszczeniami, a także ich dochodzenie przez podmiot danych, może powodować duże trudności, zwłaszcza gdy chodzi o kwestie bezpieczeństwa danych. W tej materii przepisy rozporządzenia 2016/679 ogólnie zarysowują obowiązki podmiotów odpowiedzialnych za ochronę danych osobowych, które zgodnie z podejściem *risk based approach* konkretyzują się dopiero poprzez analizę ryzyka i samodzielną ocenę skuteczności stosowanych rozwiązań. Sporne może być przykładowo to, czy wdrożone zabezpieczenia są odpowiednie w świetle aktualnego stanu wiedzy technicznej (por. art. 32 ust. 1 rozporządzenia 2016/679). Należy podkreślić, że na gruncie postępowania cywilnego, zgodnie z charakterystyczną dla niego zasadą kontradyktoryjności[1027], ciężar dowodowy spoczywa na stronach. W myśl art. 232 kpc, są one obowiązane wskazywać dowody dla stwierdzenia faktów, z których wywodzą skutki prawne. Może to nastręczać dużych trudności powodowi-podmiotowi danych, jeśli nie jest reprezentowany przez profesjonalnego pełnomocnika.

[1025] Por. M. Górski, *Komentarz do art. 82 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 4.
[1026] Por. O. Legat, *Komentarz do art. 92 uodo z 2018 r.*, [w:] B. Marcinkowski (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 229.
[1027] Por. J. Paszkowski, *Komentarz do art. 232 kpc*, [w:] T. Szanciło (red.), *Kodeks postępowania cywilnego. Komentarz. Komentarz. Art. 1–458[16]. Tom I. Wyd. 2*, Warszawa 2023, Legalis, teza 3.

Jeżeli chodzi o wysokość odszkodowania, jakie może być przyznane podmiotowi danych na podstawie art. 82 rozporządzenia 2016/679, TSUE podkreślił, że wobec nieuregulowania w tym akcie prawnym zasad ustalania kwoty odszkodowania, konieczne jest sięgnięcie do prawa krajowego i zaznaczył, że przewidziane w nim instrumenty muszą umożliwiać „pełne i skuteczne odszkodowanie za poniesione szkody" w myśl zasad równoważności i skuteczności prawa UE. Prawo państwa członkowskiego nie może uzależniać przyznania odszkodowania od osiągnięcia pewnego stopnia wagi, gdyż stałoby to w sprzeczności z art. 82 rozporządzenia 2016/679, który takiego warunku nie przewiduje[1028]. Praktyka polskich sądów w sprawach o podobnym charakterze – o naruszenie dóbr osobistych – pokazuje, że kwoty zasądzanych zadośćuczynień są niskie[1029]. Wysokość odszkodowania za szkodę spowodowaną naruszeniem rozporządzenia 2016/679 może być uzależniona od indywidualnych cech osoby fizycznej. Sąd Okręgowy w Warszawie w sprawie o sygn. III C 280/22, orzekając w przedmiocie wysokości odszkodowania za szkodę niemajątkową – stres i obawy o wykorzystanie danych osobowych przez nieuprawnione osoby, których powód doświadczył w związku z „wyciekiem" danych osobowych z portalu internetowego – wziął pod uwagę pełnoletniość powoda i pełnione przez niego role społeczne (męża i ojca), co doprowadziło sąd do przekonania, że to zdarzenie nie powinno wywoływać w przypadku dojrzałego człowieka skutków tak poważnych, jak wskazywał powód[1030]. Gdyby natomiast ujemne przeżycia psychiczne, będące następstwem naruszenia przepisów rozporządzenia 2016/679, dotknęły dziecka, powinny być istotnym czynnikiem w ustalaniu wysokości odszkodowania.

Trudności związane z dochodzeniem roszczeń na ścieżce cywilnoprawnej – m.in. spoczywanie ciężaru dowodowego na stronach, nikła perspektywa uzyskania odszkodowania w znaczącej wysokości – mogą sprawiać wrażenie nie do przezwyciężenia i zniechęcać podmiot danych do skorzystania z tego środka. W przypadku, gdy w wyniku naruszenia rozporządzenia 2016/679 szkodę poniosło dziecko, będzie ono stroną w procesie – zdolność sądowa przysługuje każdej osobie fizycznej (por. art. 64 §1 kpc). Należy ponadto zauważyć, że warunkową zdolność sądową posiada *nasciturus* pod warunkiem, że urodzi się żywy – co jest skorelowane z jego warunkową zdolnością prawną[1031]. Stosownie do art. 65 §1 kpc, zdolność procesową mają osoby fizyczne posiadające pełną zdolność do czynności prawnych, zaś osoby niemające zdolności procesowej mogą – zgodnie z art. 66 kpc – podejmować czynności procesowe tylko przez swoich

[1028] Por. wyrok TSUE z dnia 04.05.2023 r. w sprawie C-300/21, UI przeciwko Österreichische Post AG.
[1029] Por. A. Pązik, *Szkoda wynikająca z naruszenia…*, s. 133-137 i tam powołane orzecznictwo.
[1030] Por. wyrok Sądu Okręgowego w Warszawie z dnia 7 lutego 2023 r., sygn. akt. III C 280/22. Powód domagał się m.in. zasądzenia 30000 zł z tytułu odszkodowania za poniesioną szkodę niemajątkową. Sąd zasądził natomiast kwotę 1500 zł wraz z odsetkami ustawowymi za opóźnienie.
[1031] Por. P. Grzegorczyk, *Komentarz do art. 64 kpc*, [w:] T. Ereciński (red.), *Kodeks postępowania cywilnego. Komentarz. Tom I. Postępowanie rozpoznawcze, wyd. V*, Warszawa 2016, s. 423; wyrok SN z

przedstawicieli ustawowych. Tymczasem według art. 65 §2 kpc, osoba fizyczna ograniczona w zdolności do czynności prawnych ma zdolność procesową w sprawach wynikających z czynności prawnych, których może dokonywać samodzielnie. Nawet gdyby przyjąć, że art. 65 §2 kpc ma zastosowanie w przypadku roszczeń z tytułu naruszenia przepisów rozporządzenia 2016/679 w związku z przetwarzaniem danych osobowych dziecka korzystającego z usług społeczeństwa informacyjnego na podstawie zgody, której w myśl art. 8 ust. 1 rozporządzenia 2016/679 mogło ono udzielić samodzielnie, trudno wyobrazić sobie, żeby dysponowało odpowiednią wiedzą do podejmowania czynności w postępowaniu cywilnym. Trudności może sprawiać już spełnienie podstawowego warunku podjęcia przez sąd czynności na skutek wniesienia pisma, tzn. uiszczenia opłaty. Domaganie się zwolnienia od kosztów sądowych również wymaga orientowania się w tej procedurze.

Przepisy uodo z 2018 r. zawierają szczególne regulacje, sprzyjające wzmocnieniu pozycji podmiotu danych i realizacji jego interesów w postępowaniu. Przewidują one uprawnienie Prezesa UODO do wytaczania powództwa na rzecz podmiotu danych oraz wstępowania do postępowania w każdym stadium za jego zgodą (art. 98 ust. 1 uodo z 2018 r.). W razie wytoczenia powództwa przez Prezesa UODO, osoba, na której rzecz to nastąpiło, może wstąpić do sprawy w charakterze powoda, czego konsekwencją będzie odpowiednie stosowanie przepisów o współuczestnictwie jednolitym[1032]. Niezależnie od tego, Prezes UODO jest uprawniony do przedstawienia sądowi istotnego dla sprawy poglądu, jeżeli uzna, że przemawia za tym interes publiczny (art. 99 uodo z 2018 r.). Warto zastanowić się, w jakich stanach faktycznych zaistnieje sposobność stosowania tych przepisów przez Prezesa UODO. Na zasadzie art. 94 ust. 1 uodo z 2018 r., sąd ma obowiązek niezwłocznego zawiadomienia Prezesa UODO o wniesieniu pozwu oraz prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych. W ten sposób organ nadzorczy dowiaduje się o tym, że wniesiono pozew, co umożliwia mu wstąpienie do postępowania (pod warunkiem wyrażenia na to zgody przez powoda) lub przedstawienie poglądu. Z kolei, żeby wytoczyć powództwo na czyjąś rzecz, Prezes UODO musi wcześniej znać okoliczności sprawy i naturalnie tożsamość tej osoby (por. art. 55 kpc). Wydaje się, że asumpt do skorzystania przez Prezesa UODO z powyższego uprawnienia może dać wniesiona do niego skarga. Warto odnotować, że w sprawozdaniach z działalności Prezesa UODO w latach 2018-2021 nie ma wzmianek o podejmowaniu przez niego działań określonych w art. 98 ust. 1 uodo z 2018 r., co z dużą dozą prawdopodobieństwa świadczy o tym, że organ nie korzysta z tych uprawnień. Aktywność Prezesa UODO w postępowaniach cywilnych o roszczenia z tytułu szkód poniesionych przez dzieci w związku z korzystaniem z usług

[1032] Por. art. 98 ust. 3 uodo z 2018 r. w związku z art. 56 §1 kpc – P. Barta, *Komentarz do art. 98 uodo z 2018 r.*, [w:] P. Litwiński (red.), *Ustawa o ochronie danych…*, Legalis, teza 3.

społeczeństwa informacyjnego byłaby pożądana, gdyż przyczyniałaby się do urzeczywistnienia celów reformy ochrony danych osobowych, czyli wzmocnienia ochrony praw dzieci i uskutecznienia prawa do uzyskania odszkodowania.

Istotnym czynnikiem wspierającym osiągnięcie powyższych założeń mogłoby być również wsparcie podmiotu danych przez organizację działającą na rzecz ochrony danych osobowych. Stosownie do art. 80 ust. 1 *in fine* rozporządzenia 2016/679, może ona żądać w imieniu podmiotu danych odszkodowania, o którym mowa w art. 82 rozporządzenia 2016/679, pod warunkiem, że przewiduje to prawo państwa członkowskiego. Ustawodawca nie zdecydował się na wprowadzenie w uodo z 2018 r. takiego przepisu, poprzestając na uregulowaniu w niej udziału organizacji działającej na rzecz ochrony danych osobowych w postępowaniu administracyjnym w sprawie naruszenia przepisów o ochronie danych osobowych, prowadzonym przez Prezesa UODO. W zakresie nieuregulowanym w uodo z 2018 r. stosuje się przepisy kpc, który przewiduje wprawdzie wytaczanie powództw na rzecz osoby fizycznej (za jej pisemną zgodą) przez organizacje pozarządowe w zakresie swoich zadań statutowych, jednak w zamkniętym katalogu spraw, których to dotyczy, nie znajdują się sprawy z zakresu ochrony danych osobowych (por. art. 61 §1 kpc). Ustawodawca przewidział taką możliwość m.in. w sprawach z zakresu ochrony konsumentów, w których zgodnie z art. 87 §5 kpc, pełnomocnikiem może być przedstawiciel organizacji, do której zadań statutowych należy ochrona konsumentów[1033]. Należy postulować wprowadzenie analogicznej regulacji odnoszącej się do spraw z zakresu ochrony danych osobowych, by umożliwić podmiotom danych – zwłaszcza dzieciom, a także ich przedstawicielom ustawowym – szerszy dostęp do wsparcia ze strony organizacji wyspecjalizowanych w ochronie danych osobowych. Choć w świetle art. 80 ust. 1 rozporządzenia 2016/679 wprowadzenie takiej regulacji nie jest obowiązkiem państwa członkowskiego, można argumentować, że pozwoliłoby to na pełniejsze osiągnięcie celów unijnej reformy ochrony danych osobowych, zwłaszcza że instytucja jest już znana polskiemu prawu cywilnemu.

3. Odpowiedzialność karna

Zgodnie z art. 84 ust. 1 rozporządzenia 2016/679, państwa członkowskie przyjmują przepisy określające inne niż przewidziane przez samo rozporządzenia 2016/679 sankcje za jego naruszenia, które powinny być skuteczne, proporcjonalne i odstraszające. Jak podkreślono w motywie 149 preambuły do rozporządzenia 2016/679, państwa członkowskie powinny mieć

[1033] Szerzej na ten temat por. M. Maciejewska-Szałas, *Organizacje pozarządowe i formy ich uczestnictwa w postępowaniu cywilnym*, „Gdańskie Studia Prawnicze" 2017, nr 2, s. 121-136; M. Dziurda, *Legitymacja do wytaczania powództw na rzecz konsumentów*, „Przegląd Sądowy" 2022, nr 11-12, s. 54-74.

możliwość ustanawiania przepisów przewidujących sankcje karne. Ustawodawca skorzystał z tej możliwości wprowadzając w uodo z 2018 r. przepisy karne[1034].

Na mocy art. 107 ust. 1 uodo z 2018 r. ustawodawca penalizuje przetwarzanie danych osobowych przez tego, kto je przetwarza choć nie jest to dopuszczalne albo do ich przetwarzania nie jest uprawniony, co jest zagrożone grzywną, karą ograniczenia wolności albo pozbawienia wolności do lat dwóch. W myśl art. 107 ust. 2 uodo z 2018 r., jeżeli ten czyn dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech. Przepis art. 107 ust. 2 uodo z 2018 r. przewiduje surowszą karę co wynika z tego, że czyn dotyczy przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, co do zasady objętych zakazem przetwarzania[1035].

Przez niedopuszczalność przetwarzania komentatorzy rozumieją brak spełnienia przesłanek zgodności z prawem, o których mowa w art. 6, 9, 10 rozporządzenia 2016/679, zaś przez nieuprawnione przetwarzanie – dokonywanie tego z naruszeniem obowiązku działania z upoważnienia administratora lub podmiotu przetwarzającego w rozumieniu art. 29 rozporządzenia 2016/679[1036]. W przypadku oceny dopuszczalności przetwarzania danych osobowych na podstawie zgody osoby, której dane dotyczą, znaczenie powinny mieć przepisy rozporządzenia 2016/679 określające warunki jej ważności – przede wszystkim art. 7 rozporządzenia 2016/679, a w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku dodatkowo art. 8 rozporządzenia 2016/679. P. Poniatowski wskazuje, że za przykład niedopuszczalnego przetwarzania można postrzegać naruszenie przez administratora obowiązku wynikającego z art. 17 ust. 1 lit. f rozporządzenia 2016/679 – tzn. niespełnienie żądania usunięcia danych i dalsze ich przetwarzanie w sytuacji, gdy dane osobowe zostały zebrane na podstawie zgody w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku[1037]. Podobny przykład niedopuszczalnego przetwarzania podaje M. Zimna – jest nim przetwarzanie danych osobowych mimo skutecznego wniesienia przez podmiot danych sprzeciwu na mocy art. 21 rozporządzenia

[1034] Por. M. Pawlicka, *Komentarz do art. 107 uodo z 2018 r.,* [w:] M. Kawecki, M. Czerniawski (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2019, Legalis, teza 5.
[1035] Por. J. Łuczak-Tarka, *Komentarz do art. 107 uodo z 2018 r*., [w:] D. Lubasz (red.), *Ustawa o ochronie danych…*, s. 532.
[1036] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 966; M. Pawlicka, *Komentarz do art. 107 uodo z 2018 r*., [w:] M. Kawecki, M. Czerniawski (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2019, Legalis; P. Barta, *Komentarz do art. 107 uodo z 2018 r.*, [w:] P. Litwiński (red.), *Ustawa o ochronie danych…*, Legalis, teza 12.
[1037] Por. P. Poniatowski, *Niedopuszczalne lub nieuprawnione przetwarzanie danych osobowych – aspekty prawnokarne*, „Prokuratura i Prawo" 2021, nr 11, s. 77

2016/679[1038]. Wydaje się jednak, że gdy dochodzi do naruszenia przepisów rozporządzenia 2016/679 nakładających na administratora obowiązek realizowania uprawnień podmiotów danych, rozwiązaniem bardziej adekwatnym do stanu faktycznego jest egzekwowanie wykonania tych obowiązków na ścieżce administracyjnoprawnej, tzn. przez wniesienie skargi do Prezesa UODO. Jest to rozwiązanie, które z perspektywy podmiotów danych może być postrzegane jako bardziej pożądane i skuteczne, ponieważ organ nadzorczy dzięki swoim uprawnieniom władczym jest w stanie przywrócić stan zgodności z prawem – przykładowo doprowadzić do spełnienia żądania osoby, której dane dotyczą i zaprzestania przetwarzania – a także, o ile zaistnieją ku temu przesłanki, nałożyć administracyjną karę pieniężną. Mając na względzie zasadę subsydiarności prawa karnego należy zgodzić się z tezą, że „zasadniczą rolę w przeciwdziałaniu zachowaniom stanowiącym naruszenie przepisów dotyczących ochrony danych osobowych odgrywać mają przepisy statuujące odpowiedzialność administracyjną i cywilną. Środkiem reakcji na naruszenie tych przepisów mają być przede wszystkim obowiązki wynikające z prawa administracyjnego oraz administracyjne kary pieniężne”[1039].

Nie oznacza to jednak, że należy zgodzić się z przedstawioną w literaturze krytyką penalizacji naruszeń przepisów o ochronie danych osobowych. Zdaniem B. Sołtysa, „zważywszy na okoliczność, że naruszenie przepisów o ochronie danych osobowych jest obecnie w Polsce sankcjonowane odpowiedzialnością cywilną, administracyjną, karno-administracyjną oraz karną trzeba zastanowić się, czy sankcje te nie są nadmierne, zwłaszcza wobec bardzo szerokiego ujęcia strony przedmiotowej czynów karalnych oraz jednoczesnego zagrożenia takich czynów wysokimi karami pieniężnymi w ramach odpowiedzialności administracyjno-karnej przewidzianej w RODO”[1040]. W wyniku swoich rozważań B. Sołtys stawia m.in. tezę, że nadmierność sankcji karnych potęguje jednoczesne zagrożenie objętych nimi naruszeń odpowiedzialnością karnoadministracyjną[1041]. Autor pominął natomiast kluczową okoliczność, że administracyjna kara pieniężna za naruszenie przepisów o ochronie danych osobowych może zostać nałożona przez organ nadzorczy na administratora lub podmiot przetwarzający, działający w imieniu administratora[1042]. Może się wydawać, że skoro pierwszorzędnym kryterium pozwalającym na

[1038] Por. M. Zimna, *Odpowiedzialność karna za naruszenie ochrony danych osobowych*, „Prokuratura i Prawo” 2020, nr 1, s. 64.
[1039] A. Błachnio-Parzych, *Przepisy karne w ustawie z 10.5.2018 r. o ochronie danych osobowych*, [w:] G. Sibiga (red.), *Przepisy prawa uzupełniające RODO. Aktualne problemy prawnej ochrony danych osobowych 2018* (dodatek do „Monitora Prawniczego” 2018, nr 22), Warszawa 2018, s.19.
[1040] B. Sołtys, *Wątpliwości wokół konstytucyjności sankcji karnych i administracyjno-karnych za naruszenie przepisów o ochronie danych osobowych*, „Przegląd Sejmowy” 2019, nr 5, s. 38-39.
[1041] Tamże, s. 40.
[1042] Administracyjna kara pieniężna może być także nałożona na podmiot certyfikujący i podmiot monitorujący w związku z naruszeniem ich obowiązków, co nie ma jednak związku z przetwarzaniem danych osobowych – szerzej na ten temat por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 83 rozporządzenia 2016/679*, [w:] P. Litwiński (red.), *Rozporządzenie UE…*, Legalis, teza 8.

uznanie danego podmiotu za administratora jest fakt decydowania o celach i sposobach przetwarzania danych osobowych, administratorem staje się każdy podmiot, który uzyskuje dostęp do danych i samowolnie dokonuje na nich operacji – bez względu na okoliczności, w jakich to następuje i czy istnieje ku temu podstawa prawna. Bardziej właściwe wydaje się przyjęcie – zwłaszcza jeśli dopuszczalność przetwarzania danych osobowych przez inny podmiot wzbudza uzasadnione wątpliwości – że powinien być on postrzegany jako strona trzecia[1043], która w zależności od okoliczności faktycznych i prawnych nie musi stać się automatycznie nowym, odrębnym administratorem, ze wszystkimi wiążącymi się z tym konsekwencjami[1044]. Prowadzi to do wniosku, że nie każdy podmiot, który faktycznie przetwarza dane osobowe, jest jednocześnie podmiotem podlegającym odpowiedzialności administracyjnej – krąg tych podmiotów zdaje się zawężony. Z kolei przestępstwo, o którym mowa w art. 107 uodo z 2018 r., jest przestępstwem powszechnym, tzn. „może się go dopuścić każdy, kto bezprawnie przetwarza dane osobowe, natomiast w zakresie przetwarzania danych przez osobę nieuprawnioną – podmiotem mogącym ponieść odpowiedzialność będzie każdy, kto nie jest uprawniony do przetwarzania danych”[1045].

Uznanie przez ustawodawcę w art. 107 ust. 2 uodo z 2018 r., że przestępstwo dotyczące przetwarzania szczególnych kategorii danych osobowych powinno być zagrożone surowszą karą, zasługuje na aprobatę. Do tego rodzaju danych zaliczają się m.in. dane biometryczne, których przetwarzanie znajduje coraz szersze zastosowanie. Rodzi to obawy o legalność i proporcjonalność przetwarzania w stosunku do jego celów, co jest spowodowane m.in. specyficznymi zagrożeniami wynikającymi z niezmienności danych biometrycznych – w przeciwieństwie do innych informacji o osobie fizycznej, np. danych teleadresowych. W literaturze podkreśla się, że „ogólny zakaz wykorzystywania danych biometrycznych to istotne zabezpieczenie dla nas wszystkich – użytkowników nowych technologii. Warto bowiem pamiętać, że dane biometryczne to dane szczególnie wartościowe”[1046]. Przykładem przetwarzania danych biometrycznych w ramach świadczenia usług społeczeństwa informacyjnego (czy szerzej – w internecie) jest zautomatyzowane rozpoznawanie twarzy w celu oznaczania osób na zdjęciach i wyszukiwania zdjęć, na których utrwalony jest ich wizerunek – co może powodować ryzyko wykorzystywania takich informacji w celach wykraczających poza pierwotnie zdefiniowane[1047].

[1043] Zgodnie z art. 4 pkt 10 rozporządzenia 2016/679, strona trzecia oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

[1044] Por. B. Fischer, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda, *Komentarz do art. 4 pkt 10 rozporządzenia 2016/679*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, Legalis, teza 3.

[1045] Por. P. Fajgielski, *Ogólne rozporządzenie…*, s. 966.

[1046] M. Miernik, *Wizerunek a nowe technologie. Wizerunek jako dana biometryczna*, „Prawo Nowych Technologii” 2022, nr 3, s. 14.

[1047] Por. P. Fajgielski, *Automatyczne rozpoznawanie twarzy – wybrane zagadnienia prawne*, [w:] B. Fischer, A. Pązik, M. Świerczyński (red.), *Prawo sztucznej inteligencji i nowych technologii*, Warszawa 2021, s. 81-82.

Ilustruje to zjawisko stosowania technologii *deepfake*, która polega na tym, że zdjęcia lub nagrania przedstawiające wizerunek są automatycznie przetwarzane z wykorzystaniem algorytmów sztucznej inteligencji w celu stworzenia nowej treści, a następnie rozpowszechniania jej w internecie przykładowo by zdyskredytować, ośmieszyć daną osobę[1048]. M. Czapska i R. Nożykowski podkreślają, że kolebką *deepfake* była branża pornograficzna i taki charakter wciąż ma wiele treści kreowanych z wykorzystaniem tej technologii. Autorzy ci, analizując prawnokarne konsekwencje naruszenia w ten sposób wizerunku, proponują rozpatrywać je pod kątem zniewagi lub zniesławienia, a nawet tworzenia fałszywych dowodów (odpowiednio art. 212 kk, art. 216 kk, art. 235 kk)[1049]. Zastosowanie technologii *deepfake* bez wiedzy i zgody podmiotu danych może być moim zdaniem rozpatrywane pod kątem wypełnienia znamion przestępstwa określonego w art. 107 uodo z 2018 r.

Przepis art. 107 uodo z 2018 r. nie jest jedynym przepisem prawa karnego, który ma znaczenie w kontekście przetwarzania danych osobowych w związku ze świadczeniem usług społeczeństwa informacyjnego. Charakterystycznym zagrożeniem dla tej sfery jest tzw. kradzież tożsamości. Unijny prawodawca wymienia ją w motywach 75 i 85 preambuły do rozporządzenia 2016/679 jako jeden z czynników prowadzących do zaistnienia ryzyka naruszenia praw i wolności osób, których dane dotyczą. W literaturze zauważa się, że „media społecznościowe umożliwiają popełnianie przestępstw charakterystycznych dla przestrzeni internetowej (np. kradzież tożsamości w sieci); tworzą przestrzenie lub środki do popełnienia czynu zabronionego (znieważenie na portalu społecznościowym)”[1050]. Jedną z głównych przyczyn takiego stanu rzeczy trafnie identyfikuje A. Lach wskazując, że usługi społeczeństwa informacyjnego wykorzystują nowe sposoby identyfikacji, zasadzające się przeważnie na tym, co użytkownik wie lub posiada (autor podaje jako przykłady login, hasło, kartę dostępu). Brak bezpośredniego kontaktu z osobą podającą dane czy też dodatkowych metod potwierdzenia tożsamości stwarza więc sposobność do nadużyć[1051]. Założenie konta w usłudze społeczeństwa informacyjnego z wykorzystaniem cudzych danych osobowych jest nieskomplikowane – wystarczy znać podstawowe informacje identyfikujące tę osobę. Login, którym często jest adres poczty elektronicznej, może być abstrakcyjny, a nawet jeśli zawiera w sobie imię i nazwisko nie przesądza to o tożsamości korzystającego z takiego adresu, ponieważ jego utworzenie nie jest poprzedzone weryfikacją prawdziwości danych. W dobie popularności publikowania zdjęć dokumentujących niemal

[1048] Por. O. Bodanka, *Naruszenie wizerunku przy wykorzystaniu technologii deepfake – analiza prawna i praktyczna*, „Opolskie Studia Administracyjno-Prawne” 2022, nr 2, s. 13-14.
[1049] Por. M. Czapska, R. Nożykowski, *Wizerunek a nowe technologie – wybrane problemy prawne*, „Prawo Nowych Technologii” 2021, nr 1, s. 59.
[1050] K. Skraba, I. Strzałkowski, *Media społecznościowe jako źródło dowodu w polskim procesie karnym. Badanie orzecznictwa sądów apelacyjnych i Sądu Najwyższego*, [w:] P. Waszkiewicz (red.), *Media społecznościowe w pracy organów ścigania*, Warszawa 2021, s. 130.
[1051] Por. A. Lach, *Kradzież tożsamości*, „Prokuratura i Prawo” 2012, nr 3, s. 29-30.

wszystkie aspekty życia, nietrudno także pozyskać zdjęcie przedstawiające wizerunek innej osoby i wykorzystać je w celu utworzenia profilu na portalu społecznościowego, zwiększając w ten sposób jego wiarygodność w oczach innych użytkowników. Innym przykładowym sposobem wykorzystania cudzych danych osobowych w celu podszycia się pod kogoś na portalu społecznościowym (lub w innej usłudze społeczeństwa informacyjnego), jest posłużenie się danymi do logowania do „prawdziwego" konta tej osoby, dzięki ich niefrasobliwemu ujawnieniu przez samego użytkownika lub pozyskaniu dzięki zastosowaniu socjotechnik. Zjawisko wyłudzania poufnych informacji, takich jakich jak hasło, nazywane jest phishingiem[1052]. Znane są przypadki zastosowania tej metody lub posłużenia się złośliwym oprogramowaniem w celu wyłudzenia danych potrzebnych do zalogowania na konto na platformie gier w celu przejęcia „wirtualnej postaci" wykreowanej przez użytkownika, co nierzadko wymaga poniesienia nakładów finansowych (gdy np. wyposażenie tzw. awatara w broń jest odpłatne), a więc może skutkować szkodą majątkową[1053].

Choć w polskim prawie karnym nie występuje pojęcie kradzieży tożsamości – które jest natomiast używane powszechnie w języku potocznym i prawniczym[1054] – czyn tego typu, związany bezpośrednio z zagadnieniem ochrony danych osobowych, penalizuje art. 190a §2 kk[1055]. W myśl tego przepisu, przestępstwo to polega na tym, że sprawca podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej. Zgodnie z art. 190a §1 kk, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8. Zauważyć należy także, że stosownie do art. 190a §3 kk, jeżeli następstwem czynu jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od lat 2 do 12. Nie jest istotna okoliczność czy próba samobójcza była skuteczna – sprawca podlega odpowiedzialności karnej także wtedy, gdy pokrzywdzony usiłował odebrać sobie życie[1056]. W literaturze kwestionowana jest zasadność ustanowienia kwalifikowanego typu tego przestępstwa ze względu na wątpliwości, czy istotnie skutkiem kradzieży tożsamości może być podjęcie próby samobójczej[1057]. Ten sceptycyzm nie wydaje się zasadny, szczególnie jeśli pokrzywdzonym jest dziecko. Jak dowodzą badania, „przyczyną podjęcia próby samobójczej przez młode osoby może być każdy, nawet najbardziej prozaiczny problem, który według ofiary jest nie do rozwiązania w

[1052] Por. K. Chałubińska-Jentkiewicz, *Zagrożenia związane z nowymi technologiami. Cyberprzestępczość a bezpieczeństwo w sieci*, [w:] K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015, s. 377.
[1053] Por. P. Siemkowicz, *Zakres skuteczności regulacji art. 190a § 2 KK dla zwalczania działań sprawczych związanych z tzw. kradzieżą tożsamości w sieci Internet*, „Prawo Mediów Elektronicznych" 2018, nr 1, s. 33.
[1054] Por. A. Lach, *Kradzież…*, s. 29.
[1055] Por. K. Chałubińska-Jentkiewicz, *Zagrożenia związane z nowymi technologiami…*, s. 381.
[1056] Por. S. Hypś, *Komentarz do art. 190a kk*, [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny…,* Legalis, teza 16.
[1057] Por. A. Lach, *Kradzież…*, s. 38.

inny sposób”[1058]. Powodami myśli samobójczych u nastolatków są m.in. niepowodzenia w szkole – trudności w nauce, konflikty z nauczycielami lub rówieśnikami[1059]. Nie można więc wykluczyć, że dziecko pokrzywdzone w wyniku kradzieży tożsamości, dla przykładu ośmieszone i poniżone w swoim środowisku, nie będzie odczuwać wstydu oraz cierpienia, którego skutki mogą być bardzo dotkliwe i trudne do przewidzenia. Słusznie więc prawodawca dostrzegł istnienie zagrożenia targnięcia się przez pokrzywdzonego na własne życie i przewidział kwalifikowany typ przestępstwa kradzieży tożsamości, gdyż jego oddziaływanie na dziecko korzystające z usług społeczeństwa informacyjnego może mieć tragiczne skutki.

Warto zauważyć, że jeśli wskutek przestępstwa pokrzywdzony poniósł szkodę majątkową lub niemajątkową (krzywda), w ramach postępowania karnego może na podstawie art. 46 §1 kk wnioskować o zasądzenie obowiązku naprawienia szkody lub zadośćuczynienia, co uważane jest za dużo łatwiejsze niż wytoczenie odrębnego powództwa cywilnego – przede wszystkim z uwagi na to, że wniosek nie podlega opłacie, nie istnieją szczególne wymogi dotyczące jego treści, a na pokrzywdzonym nie ciążą obowiązki dowodowe[1060]. Ponadto, w myśl art. 49a kpk, wniosek można złożyć aż do zamknięcia przewodu sądowego na rozprawie głównej. Stosownie do art. 46 §1 kk, sąd może także orzec obowiązek naprawienia wyrządzonej przestępstwem szkody lub zadośćuczynienia za doznaną krzywdę z urzędu[1061].

[1058] A. Bąbik, D. Olejniczak, *Uwarunkowania i profilaktyka samobójstw wśród dzieci i młodzieży w Polsce*, „Dziecko krzywdzone. Teoria, badania, praktyka” 2014, nr 2, s. 105.
[1059] Por. A. Kielan, I. Cieślak, J. Skonieczna, D. Olejniczak, K. Jabłkowska-Górecka, M. Panczyk, J. Gotlib, B. Zalewska-Zielecka, *Analysis of the opinions of adolescents on the risk factors of suicide*, „Psychiatria Polska” 2018, nr 4, s. 700.
[1060] Por. P. Bróżek, *Wniosek o orzeczenie obowiązku naprawienia szkody lub zadośćuczynienia za doznaną krzywdę jako skuteczna alternatywa dla pozwu cywilnego*, „Monitor Prawniczy” 2022, nr 22, s. 1107-1112 i tam powołana literatura.
[1061] D. Szeleszczuk, *Komentarz do art. 46 kk*, [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny...*, Legalis teza 4.

ZAKOŃCZENIE

W rezultacie przeprowadzonej w niniejszej rozprawie analizy zawartych w rozporządzeniu 2016/679 przepisów odnoszących się do przetwarzania danych osobowych dziecka udowodniona została teza, iż regulacja przetwarzania danych osobowych dziecka jest fragmentaryczna, zbyt ogólna i rodzi liczne wątpliwości interpretacyjne, a w konsekwencji reforma ochrony danych osobowych nie realizuje w pełni jednego z jej założeń, jakim jest wzmocnienie ochrony danych osobowych dziecka w związku ze świadczeniem usług społeczeństwa informacyjnego.

Zaprezentowane w rozprawie aksjologiczne uzasadnienie potrzeby objęcia dziecka szczególną ochroną w celu urzeczywistnienia zasady dobra dziecka w kontekście ochrony danych osobowych podnoszone było już w 2010 r. na wstępnym etapie prac legislacyjnych nad rozporządzeniem 2016/679, a następnie zostało zaakcentowane w licznych motywach jego preambuły. Pełnią one zasadniczą rolę w wykładni prawa Unii Europejskiej, w której prym wiedzie wykładnia celowościowa. Motywy wyznaczają kierunki interpretacji, którymi posiłkują się w praktyce orzeczniczej Trybunał Sprawiedliwości Unii Europejskiej, a także właściwe organy nadzorcze – w Polsce Prezes Urzędu Ochrony Danych Osobowych. Wielokrotne podkreślanie w motywach potrzeby wyjątkowego podejścia do przetwarzania danych osobowych dziecka, które jest mniej świadome konsekwencji korzystania z usług społeczeństwa informacyjnego – zwłaszcza gdy przetwarzanie służy celom marketingowym, tworzeniu profili osobowych – wskazuje jasno na intencje prawodawcy.

W rozprawie przedstawione zostały w sposób przekrojowy rozwiązania, które wprowadzono w celu osiągnięcia powyższych założeń. Na aprobatę zasługuje przede wszystkim dostrzeżenie przez prawodawcę konieczności przyjęcia rozwiązań uwzględniających specyfikę przetwarzania danych osobowych dzieci na mocy rozporządzenia, czyli aktu prawa Unii Europejskiej obowiązującego bezpośrednio we wszystkich państwach członkowskich. Daje to szansę na ujednolicenie prawa, co jest warunkiem jego skuteczności mając na względzie charakter usług społeczeństwa informacyjnego, świadczonych na odległość, przez internet, co oznacza brak barier w postaci granic państw. Analiza przepisów rozporządzenia 2016/679 pozwala na wniosek, że prawodawca wykorzystał tę szansę częściowo, pozostawiając kluczowe kwestie do rozstrzygnięcia przez prawo krajowe państw członkowskich. Dotyczy to ustalenia granicy wieku dziecka, od którego może ono samodzielnie wyrazić zgodę na przetwarzanie danych osobowych w związku z korzystaniem z usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku i polega na pozostawieniu pewnego marginesu swobody dzięki zawarciu w art. 8 ust. 1 rozporządzenia 2016/679 klauzuli kompetencyjnej, wskutek czego w Unii Europejskiej funkcjonują aż cztery różne granice wieku. Ponadto na krytykę zasługuje nieprzeprowadzenie na

etapie prac legislacyjnych wnikliwych, interdyscyplinarnych badań, dzięki którym określenie właściwej granicy wieku, od którego dziecko może samodzielnie decydować o przetwarzaniu dotyczących go danych, byłoby uzasadnione obiektywnymi przesłankami odnoszącymi się do możliwości poznawczych dziecka na różnych etapach rozwoju. Ponadto poziom ochrony danych osobowych dziecka może być obniżony z powodu zbyt ogólnie zarysowanej kwestii wyrażenia zgody przez przedstawiciela ustawowego lub zaaprobowania przez niego zgody wyrażonej wcześniej przez dziecko. Ocena, jakie środki są odpowiednie do zastosowania się do norm wynikających z art. 8 ust. 1 rozporządzenia 2016/679, leży w gestii administratora, co wydaje się istotnie uderzać w dyrektywę pewności prawa. Dla porównania, amerykański prawodawca określił w przepisach COPPA katalog możliwych rozwiązań służących pozyskaniu zgody przedstawiciela ustawowego, co należy ocenić pozytywnie z perspektywy wszystkich zainteresowanych podmiotów – dziecka, jego przedstawiciela ustawowego i przedsiębiorcy świadczącego usługę społeczeństwa informacyjnego.

Powyższe, nierozwiązane przez prawodawcę problemy wyrastające na gruncie art. 8 ust. 1 rozporządzenia 2016/679 nie są jedynymi dylematami związanymi ze zgodą dziecka na przetwarzanie danych osobowych. Przesłanka zgody uprawniająca administratora do przetwarzania może być bowiem stosowana przez niego w innych okolicznościach niż świadczenie usług społeczeństwa informacyjnego z wykorzystaniem podstawowych danych i w celu dokonywania niewielu operacji przetwarzania, takich jak zbieranie, przechowywanie, usuwanie danych. Świadczenie takich usług jest często bardzo skomplikowanym procesem, wykorzystującym innowacyjne techniki przetwarzania – opierające się przykładowo na tzw. sztucznej inteligencji i uczeniu maszynowym – w który zaangażowane są inne podmioty działające w różnych rolach. Ze względu na powszechność występowania tego zjawiska w obrocie gospodarczym wskazać należy na powierzenie przetwarzania danych osobowych innemu podmiotowi, świadczącemu usługi na rzecz administratora-dostawcy usługi społeczeństwa informacyjnego. Szeroko pojęte usługi informatyczne, polegające np. na przetwarzaniu danych w chmurze obliczeniowej, asyście technicznej, wdrażaniu i utrzymywaniu systemów służących do przetwarzania, świadczone są przez przedsiębiorców z różnych państw, przede wszystkim azjatyckich. Powoduje to potrzebę przekazywania danych osobowych do państw trzecich, co w wyjątkowych przypadkach może odbyć się na podstawie zgody osoby, której dane dotyczą (por. art. 49 ust. 1 lit. a rozporządzenia 2016/679). Przepisy rozporządzenia 2016/679 nie regulują jednak tego, czy – a jeśli tak pod jakimi warunkami – zgodę na taką operację przetwarzania może wyrazić dziecko. Innym, rodzącym podobne wątpliwości przykładem jest dopuszczalność przetwarzania szczególnych kategorii danych osobowych dotyczących dziecka na podstawie zgody w myśl art. 9 ust. 1 lit. a rozporządzenia 2016/679. W tym przypadku prawodawca również

pominął ten problem. Kontrowersje i niepewność budzi również możliwość powołania się przez administratora na zgodę w przypadku, gdy uchyla ona ogólny zakaz podejmowania wobec podmiotu danych decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec niego istotne skutki (por. art. 22 ust. 2 lit. c rozporządzenia 2016/679). Ponownie zostało to pozostawione do interpretacji, której podjęła się – z kuriozalnym skutkiem – Grupa Robocza Art. 29. Mianowicie stanęła ona na stanowisku, że nie istnieje bezwzględny zakaz dokonywania tego rodzaju przetwarzania danych osobowych dzieci, jednocześnie postulując, by administratorzy unikali go i nie powoływali się na wyjątki ustanowione w art. 22 ust. 2 rozporządzenia 2016/679, czyli także na fakt wyrażenia zgody. Świadczy to o podjęciu przez organy nadzorcze próby dokonania wykładni zgodnej z założeniami i duchem reformy, jednak ich wytyczne niewątpliwie nie są narzędziem korygującym niedoskonałości rozporządzenia 2016/679 i nie rozwiązują problemu.

Zasadne jest wysunięcie postulatów *de le ferenda* – ujednolicenia w rozporządzeniu 2016/679 – po przeprowadzeniu odpowiednich badań – granicy wieku dziecka, od którego może ono skutecznie, samodzielnie wyrazić zgodę na przetwarzanie danych osobowych, wprowadzenie regulacji odnoszących się do sposobu pozyskania zgody lub aprobaty przedstawiciela ustawowego, które mogłyby być inspirowane COPPA, doprecyzowanie zasad przetwarzania danych osobowych dziecka na podstawie zgody – tj. wyjaśnienie relacji między art. 8 ust. 1 rozporządzenia 2016/679 a przepisami odwołującymi się do wyrażenia zgody na transfer danych do państwa trzeciego, przetwarzania danych należących do szczególnych kategorii, przetwarzania danych do celów podejmowania decyzji w sposób zautomatyzowany.

Wśród niedociągnięć rozporządzenia 2016/679 w zakresie zasad pozyskiwania zgody dziecka na przetwarzanie danych osobowych wskazać należy także materię świadczenia profilaktycznych lub doradczych usług oferowanych bezpośrednio dziecku. Jedynie w motywie 38 preambuły do rozporządzenia 2016/679 zaznaczono, że w takim przypadku zgoda przedstawiciela ustawowego nie powinna być wymagana. Przyczynkiem do tego było poczynione na etapie prac legislacyjnych spostrzeżenie, że dziecko powinno mieć dostęp do pomocy w trudnych sytuacjach – takich jak przemoc – bez zgody czy wręcz nawet wiedzy przedstawiciela ustawowego. Wziąwszy pod uwagę ten szczególny kontekst, lakoniczne zasygnalizowanie problemu w nienormatywnej części rozporządzenia 2016/679 zasługuje na krytykę i daje podstawę do sformułowania postulatu *de le ferenda*, że pożądane jest dookreślenie warunków przetwarzania danych osobowych do celów świadczenia usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku. Warte rozważenia jest zawężenie kręgu podmiotów, które mogą to czynić wyłącznie za zgodą dziecka i bez wiedzy przedstawiciela ustawowego, opierając się na kryterium charakteru działalności (np. prowadzenie działalności na rzecz ochrony praw dziecka przez

organizację społeczną) i kompetencji osób, które miałyby udzielać dziecku wsparcia (np. wymóg posiadania wykształcenia z zakresu psychologii, pedagogiki itp.).

Na mocy rozporządzenia 2016/679 podmiotowi danych – dziecku – przysługuje wiele uprawnień związanych z przetwarzaniem. Analiza art. 12 ust. 1 rozporządzenia 2016/679, motywów rozporządzenia 2016/679 i wytycznych wybranych organów nadzorczych ds. ochrony danych osobowych z innych państw członkowskich Unii Europejskiej prowadzi do wniosku, że dziecko może samodzielne wykonywać swoje uprawnienia w relacji z administratorem. Takie podejście jest godne aprobaty. Niemniej, w przypadku dwóch uprawnień, tzn. prawa do uzyskania kopii danych i prawa do przenoszenia danych (odpowiednio art. 15 ust. 3 i art. 20 ust. 1 rozporządzenia 2016/679), ze względu na potencjalne zagrożenia związane z niefrasobliwym postępowaniem z otrzymanym zestawem danych w szerokim zakresie lub przekazaniem ich innemu administratorowi w celu dalszego przetwarzania, wydaje się, że udział przedstawiciela ustawowego dziecka w procesie realizacji powyższych uprawnień służyłby dobru dziecka. Należałoby w szczególności rozważyć zasady wykonania żądania przesłania danych osobowych innemu administratorowi w sytuacji, gdy podstawą prawną przetwarzania jest zgoda przedstawiciela ustawowego lub wyrażona przez niego aprobata zgody udzielonej przez dziecko. Nadto warto byłoby przeanalizować możliwość wprowadzenia wyjątków od pobierania przez administratora opłat związanych z obsługą żądania o wydanie kopii danych (por. art. 15 ust. 3 rozporządzenia 2016/679) i doprecyzowanie okoliczności, kiedy może być pobrana opłata w przypadku pozostałych uprawnień (por. art. 12 ust. 5 rozporządzenia 2016/679), gdy wykonuje je dziecko.

W materii bezpieczeństwa danych osobowych, szczególna uwaga została w rozprawie poświęcona obowiązkowi uwzględniania ochrony danych osobowych w fazie projektowania i funkcjonowania przedsięwzięć związanych z ich przetwarzaniem, a także obowiązkowi przestrzegania zasady domyślnej ochrony danych (por. art. 25 rozporządzenia 2016/679). Jak wykazano w rozprawie, rzetelne wywiązywanie się przez administratora z tych powinności stanowi ważny element budowania bezpieczeństwa danych osobowych dzieci, a także skutkowałoby wyeliminowaniem (lub przynajmniej ograniczeniem) stosowania wobec nich technik typu *deceptive pattern*, których rozpoznanie może być trudne zwłaszcza dla najmłodszych użytkowników. Przepis art. 25 rozporządzenia 2016/679 jest jednak lakoniczny i niedosyt pozostawia pominięcie zagadnienia przetwarzania danych osobowych dzieci i ich potrzeb w kontekście korzystania z usług społeczeństwa informacyjnego. Z powyższego przepisu można wprawdzie w drodze wykładni wywieść wiele obowiązków, które powinny być spełnione przy przetwarzaniu danych osobowych dzieci, wymaga to jednak pogłębionej analizy wszystkich zasad przetwarzania określonych w art. 5 rozporządzenia 2016/679 i prawdopodobieństwa oraz wagi

ryzyka naruszenia praw lub wolności dzieci. Z tych względów, również jako postulat *de lege ferenda*, podnieść można potrzebę doprecyzowania sposobu zadośćuczynienia obowiązkom wynikającym z art. 25 rozporządzenia 2016/679 w odniesieniu do przetwarzania danych osobowych dzieci-użytkowników usług społeczeństwa informacyjnego.

Na kanwie zagadnienia bezpieczeństwa danych w rozprawie poddano rozważaniom obowiązek przeprowadzenia oceny skutków dla ochrony danych, gdy przetwarzanie, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności podmiotów danych (por. art. 35 rozporządzenia 2016/679). Prawodawca ustanowił kryteria, których spełnienie powoduje po stronie administratora powstanie obowiązku dokonania takiej oceny, a ponadto przyznał organom nadzorczym kompetencję do opracowania własnych wykazów. Wskutek przeprowadzonej analizy wyprowadzono wniosek, że przetwarzanie danych osobowych dzieci może potencjalnie mieścić się w jednym z tych kryteriów, jednak przesłanka przetwarzania danych dzieci – przykładowo na dużą skalę lub w związku z korzystaniem z *IoT* – nie została ujęta w tym katalogu. W świetle celów reformy, dążenia do zapewnienia dzieciom większej ochrony w kontekście stosowania nowych technik przetwarzania, korzystania z usług świadczonych w internecie, w tym usług społeczeństwa informacyjnego, należy postulować rozszerzenie przesłanek dokonania oceny skutków dla ochrony danych, wymienionych w art. 35 ust. 3 rozporządzenia 2016/679, o okoliczność przetwarzania danych osobowych dzieci. Godne pochwały jest uwzględnienie przez Prezesa Urzędu Ochrony Danych Osobowych w swoim wykazie operacji przetwarzania danych osobowych dzieci związku z oferowaniem im interaktywnych zabawek i usług, jednak dowodzi to, że istnieje uzasadniona obawa o niejednolitość podejścia do tej kwestii, prowadząca do zróżnicowania poziomu ochrony dzieci w Unii Europejskiej. Problemy związane z przetwarzaniem danych osobowych dzieci przez dostawców interaktywnych zabawek i usług winny być rozwiązane na poziomie rozporządzenia 2016/679.

W niniejszej rozprawie skupiono się również na analizie obowiązków materializujących się w przypadku naruszenia ochrony danych osobowych dzieci, o którym mowa art. 4 pkt 12 rozporządzenia 2016/679, tzn. naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. W razie wystąpienia naruszenia ochrony danych osobowych, które powoduje wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, na administratorze co do zasady ciąży obowiązek zawiadomienia ich o tym zdarzeniu (por. z art. 34 ust. 1 rozporządzenia 2016/679). Przeanalizowano, czy takie zawiadomienie powinno być

skierowane bezpośrednio do dziecka, czy do jego przedstawiciela ustawowego. Wzięto pod uwagę ważkie argumenty zarówno za, jak i przeciw informowaniu bezpośrednio dziecka, w tym racje przedstawione przez Prezesa Urzędu Ochrony Danych Osobowych w materiale informacyjnym opublikowanym na stronie internetowej urzędu. Należy zgodzić się z organem nadzorczym, że działania administratora, w tym komunikaty o naruszeniu, winny być dostosowane do wieku dziecka. Akcentując podmiotowość dziecka i nieograniczanie jego uprawnień ze względu na wiek i z pominięciem prawa do zajmowania stanowiska w dotyczących go sprawach, zauważyć należy, że bezpośrednie poinformowanie dziecka o naruszeniu może narazić je na duży stres. Jednocześnie, w przypadku przetwarzania danych osobowych na podstawie zgody dziecka, której mogło ono udzielić samodzielnie, skierowanie zawiadomienia do przedstawiciela ustawowego może być obiektywnie niemożliwe z powodu nieposiadania jego danych kontaktowych. Podkreślić zatem należy, traktując to jako wniosek *de lege ferenda*, że po przeprowadzeniu nieodzownych interdyscyplinarnych badań, w szczególności z udziałem psychologów i pedagogów, konieczne jest uzupełnienie rozporządzenia 2016/679 o przepisy doprecyzowujące zasady zawiadamiania podmiotów danych o naruszeniu w przypadku, gdy dotyczy ono danych osobowych dzieci korzystających z usług społeczeństwa informacyjnego.

Zagadnieniem o fundamentalnym znaczeniu z perspektywy skuteczności rozporządzenia 2016/679 i egzekwowania praw przysługujących dzieciom jako podmiotom danych jest kwestia odpowiedzialności za naruszenia powyższych przepisów. W rozprawie przestawiono i przeanalizowano rozwiązania przyjęte w ramach trzech reżimów odpowiedzialności – administracyjnej, cywilnej i karnej. Skoncentrowano się szczególnie na możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdyż celem tej instytucji jest przywrócenie stanu zgodności z prawem, np. spowodowanie, że administrator zrealizuje żądanie dziecka. Organ nadzorczy dysponuje szerokim wachlarzem uprawnień naprawczych. W wyniku analizy przepisów ustawy o ochronie danych osobowych i kodeksu postępowania administracyjnego w zakresie zdolności procesowej dziecka wyprowadzono wniosek, że dziecko posiadające ograniczoną zdolność do czynności prawnych może skutecznie wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych. Możliwość samodzielnego wniesienia skargi ma ważkie znaczenie, zwłaszcza gdy asumpt do jej złożenia dało poczucie naruszenia zasad ochrony danych osobowych w związku z korzystaniem przez dziecko z usług profilaktycznych lub doradczych, które jak wskazano wyżej nie powinny być świadczone za zgodą przedstawiciela ustawowego z powodu potrzeby zapewnienia dziecku ochrony i poufności.

W dysertacji przeanalizowano kompetencje Prezesa Urzędu Ochrony Danych Osobowych w zakresie nakładania administracyjnych kar pieniężnych. Stanowi to *novum*, najbardziej nowatorską instytucję rozporządzenia 2016/679. Wprowadzenie administracyjnych kar

pieniężnych zasługuje na aprobatę, jednak niezrozumiałe na tle celów reformy jest zakwalifikowanie naruszenia obowiązków określonych w art. 8 rozporządzenia 2016/679, dotyczących zgody na przetwarzanie danych osobowych dziecka w związku ze świadczeniem usług społeczeństwa informacyjnego, do naruszeń zagrożonych maksymalną karą w niższej wysokości (por. art. 83 ust. 4 lit. a rozporządzenia 2016/679). Prawodawca wykazał się w ten sposób niekonsekwencją, skoro administracyjne kary pieniężne powinny odstraszać – pełnić m.in. funkcję prewencyjną. EROD słusznie stanęła na stanowisku, że okoliczność, iż naruszenie dotyczy danych osobowych dzieci, może przesądzać o przypisaniu przez organ nadzorczy większej wagi temu naruszeniu w procesie miarkowania kary i badania kryterium „charakteru przetwarzania". Warta rozważenia jest zatem zmiana kwalifikacji naruszenia art. 8 rozporządzenia 2016/679, a nadto uszczegółowienie, co należy rozumieć przez uchybienie mu, mając w pamięci że w istocie wynika z niego kilka obowiązków.

Przedmiotem analiz poczynionych w niniejszej rozprawie były także zagadnienia odpowiedzialności cywilnej za szkody niemajątkowe i majątkowe spowodowane naruszeniem przepisów rozporządzenia 2016/679. Pozytywnie należy ocenić przyjęte przez unijnego prawodawcę rozwiązanie, które ma w założeniach ułatwić podmiotom danych dochodzenie roszczeń na ścieżce sądowej, polegające na możliwości żądania w imieniu podmiotu danych odszkodowania, o którym mowa w art. 82 rozporządzenia 2016/679, pod warunkiem, że przewiduje to prawo państwa członkowskiego, przez podmiot niemający charakteru zarobkowego, który został należycie ustanowiony zgodnie z prawem państwa członkowskiego, ma cele statutowe leżące w interesie publicznym i działa w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych (por. art. 80 rozporządzenia 2016/679). Polski ustawodawca nie zdecydował się jednak na wprowadzenie przepisu, który by to umożliwiał. Należy więc postulować *de lege ferenda* wprowadzenie regulacji zapewniającej podmiotom danych – zwłaszcza dzieciom, a także ich przedstawicielom ustawowym – szerszy dostęp do wsparcia ze strony organizacji wyspecjalizowanych w ochronie danych osobowych.

Pochylając się nad problematyką odpowiedzialności karnej, w rozprawie przenalizowano przepisy karne zawarte w ustawie o ochronie danych osobowych z 2018 r. oraz kodeksie karnym. Przepis art. 107 ustawy o ochronie danych osobowych z 2018 r. penalizuje przetwarzanie danych osobowych przez tego, kto je przetwarza choć nie jest to dopuszczalne albo do ich przetwarzania nie jest uprawniony. Jaskrawym, mogącym wyjątkowo dotkliwie godzić w prawa dziecko przykładem przetwarzania danych osobowych bez podstawy prawnej jest posługiwanie się technologią *deepfake*, która polega m.in. na tym, że zdjęcia przedstawiające wizerunek są automatycznie przetwarzane z wykorzystaniem algorytmów sztucznej inteligencji w celu stworzenia nowej treści, a następnie rozpowszechniania jej w internecie przykładowo w celu

ośmieszenia osoby, której dane dotyczą. W przypadku kodeksu karnego, kierując się koniecznością uchwycenia specyfiki zagrożeń związanych ze świadczeniem dziecku usług społeczeństwa informacyjnego, skupiono się na art. 190a §2 kk, penalizującym tzw. kradzież tożsamości. W rozprawie wykazano, że popełnienie tego przestępstwa jest nieskomplikowane zwłaszcza w celu podszycia się pod kogoś na portalu społecznościowym, co wynika z zasad funkcjonowania tego typu usług społeczeństwa informacyjnego. Słusznie postąpił ustawodawca dostrzegając istnienie zagrożenia targnięcia się przez pokrzywdzonego na własne życie i przewidując w art. 190a §3 kodeksu karnego kwalifikowany typ przestępstwa kradzieży tożsamości, gdyż jego oddziaływanie na dziecko korzystające z usług społeczeństwa informacyjnego może mieć tragiczne skutki. Wykazano w rozprawie, że istnienie trzech reżimów odpowiedzialności jest uzasadnione wziąwszy pod uwagę zróżnicowany charakter i potencjalne skutki naruszeń dotyczących ochrony danych osobowych dzieci.

Reasumując, przeprowadzone badania pozwoliły na osiągnięcie postawionych celów badawczych oraz udowodnienie tezy rozprawy. Przedstawione wnioski z wnikliwej analizy przepisów rozporządzenia 2016/679 świadczą tylko o częściowym osiągnięciu celów unijnej reformy ochrony danych osobowych w kontekście ochrony danych osobowych dziecka korzystającego z usług społeczeństwa informacyjnego. Z pewnością na pozytywną ocenę zasługuje dostrzeżenie przez prawodawcę tej problematyki, ponieważ regulacje obowiązujące w Unii Europejskiej przed reformą jej nie poruszały. Za czynnik wpływający korzystnie na poziom ochrony danych osobowych w przypadku wszystkich osób, których dane dotyczą, można niewątpliwie uznać uregulowanie tej materii aktem prawnym stosowanym bezpośrednio we wszystkich państwach Unii Europejskiej oraz wprowadzenie administracyjnych kar pieniężnych. Potrzeba objęcia dziecka szczególną ochroną jest podkreślana w niektórych motywach i przepisach rozporządzenia 2016/679, jednak traktują one te zagadnienia wybiórczo wywołując liczne wątpliwości interpretacyjne. Pozostawienie państwom członkowskim marginesu swobody w ustaleniu granicy wieku dziecka, od którego może ono samodzielnie wyrazić zgodę na przetwarzanie danych osobowych w związku z korzystaniem z usług społeczeństwa informacyjnego powoduje, że na tej płaszczyźnie nie udało się osiągnąć podstawowego celu reformy ochrony danych osobowych – zniwelowania różnic w poziomie ochrony w poszczególnych państwach członkowskich. W dysertacji przedstawiono i umotywowano postulaty *de lege ferenda*, sformułowane z myślą o pełniejszym zrealizowaniu jednego z kluczowych celów reformy i z troską o dobro dziecka.

WYKAZ ŹRÓDEŁ

1. Akty normatywne

1.1 Unijne akty normatywne

Traktat o Unii Europejskiej i Traktat o Funkcjonowaniu Unii Europejskiej, wersje skonsolidowane (Dz. Urz. UE C 326 z 26.10.2012, s. 1).

Karta Praw Podstawowych Unii Europejskiej, załącznik do Traktatu z Lizbony zmieniającego Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską z 13.12.2007 r. (Dz.U. z 2009 r., Nr 203, poz. 1569).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.8.2014, s. 73).

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.U. L 119 z 04.05.2016, s. 1).

Rozporządzenie 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 dnia 21.11.2018, s. 39).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz. Urz. UE L 277 z 27.10.2022, s. 1).

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 dnia 23.11.1995 r., s. 31).

Dyrektywa 2000/31/WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego na rynku wewnętrznym (dyrektywa o handlu elektronicznym) (Dz. Urz. UE L 178 z dnia 17.07.2000 r., s. 1).

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. UE L 201 z dnia z 31.07.2002 r., s. 37).

Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz. Urz. UE L 2011 Nr 88, str. 45).

Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającą procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. Urz. UE L 241 z dnia 17.09.2015 r., s. 1).

Dyrektywa 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 uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, s. 89).

Decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (Dz. Urz. UE L 199 z dnia 07.06.2021, s. 31).

Commission implementing decision of 10.07.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, C (2023) 4745 final.

1.2 Międzynarodowe akty normatywne

Powszechna Deklaracja Praw Człowieka z 10 grudnia 1948 r., http://libr.sejm.gov.pl/tek01/txt/onz/1948.html (dostęp:15.03.2023).

Konwencja o ochronie praw człowieka i podstawowych wolności z dnia 4 listopada 1950 r. (Dz.U. z 1993 r., Nr 61, poz. 284).

Międzynarodowy Pakt Praw Gospodarczych, Społecznych i Kulturalnych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz. U. z 1977 r., nr 38 poz. 169).

Konwencja Rady Europy 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz. U. z 2003 r. nr 3, poz. 25).

Konwencja o Prawach Dziecka przyjęta przez Zgromadzenie Ogólne ONZ dnia 20 listopada 1989 r. (Dz.U. z 1991 r., Nr 120, poz. 526).

1.3 Polskie akty normatywne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r., Nr 78, poz. 483 ze zm.).

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2023 r. poz. 775 ze zm.).

Ustawa z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy (T.j. Dz. U. z 2020 r. poz. 1359 z późn. zm.).

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz.U. z 2023 r. poz. 1610).

Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (T.j. Dz. U. z 2023 r. poz. 1550 z późn. zm.).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (T.j. Dz.U. z 2023 r. poz. 171 z późn zm.).

Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2019 r. poz. 351 z późn. zm.).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (T.j. Dz.U. z 2022 r. poz. 1138 z późn. zm.).

Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (T.j. Dz. U. z 2022 r. poz. 1375 z późn. zm.).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 ze zm.).

Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz.U. z 2022 r. poz. 2324 z późn zm.).

Ustawa z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni Przeciwko Narodowi Polskiemu (T.j. Dz.U. z 2023 r. poz. 102).

Ustawa z dnia 6 stycznia 2000 r. o Rzeczniku Praw Dziecka (T.j. Dz. U. z 2023 r., poz. 292).

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t. j. Dz. U. z 2020 r. poz. 344).

Ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (T.j. Dz. U. z 2023 r. poz. 259 z późn. zm.).

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t. j. Dz.U. z 2022 r. poz. 1648 z późn. zm.).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (T.j. Dz. U. z 2023 r. poz. 57 z późn. zm.).

Ustawa z dnia 17 października 2008 r. o zmianie imienia i nazwiska (T.j. Dz. U. z 2021 r. poz. 1988).

Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (T.j. Dz.U. z 2020 r. poz. 849).

Ustawa z dnia 2 kwietnia 2009 r. o obywatelstwie polskim (T.j. Dz. U. z 2022 r. poz. 465 z późn. zm.).

Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (t.j. Dz. U. z 2022 r. poz. 671 z późn. zm.).

Ustawa z dnia 30 maja 2014 r. o prawach konsumenta (T.j. Dz.U. z 2020 r. poz. 287 z późn. zm).

Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. z 2016 r. poz. 147).

Ustawa z dnia 6 marca 2018 r. Prawo przedsiębiorców (t.j. Dz. U. z 2023 r. poz. 221 z późn. zm.).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (T.j. Dz. U. z 2019 r. poz. 1781).

Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 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. U. z 2019 r. poz. 730).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i

organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024).

Komunikat Prezesa UODO z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. z 2019 r. poz. 666).

1.4 Regulacje prawne innych państw

Amerykańska ustawa w dziedzinie ochrony praw dzieci
Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505.

2. Projekty aktów normatywnych i dokumenty związane z procesem legislacyjnym

Komunikat KE z dnia 4.11.2010 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej*, KOM(2010) 609, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A52010DC0609.

Council conclusions on the Communication from the Commission to the European Parliament and the Council -A comprehensive approach on personal data protection in the European Union, 3071st Justice and Home Affairs Council meeting Brussels, 24-25.02.2011 r., https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf.

Opinia EIOD z dnia 22.06.2011 r. dotycząca komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej* (Dz. Urz. UE C 181/1).

Rezolucja Parlamentu Europejskiego z dnia 06.07. 2011 r. w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej, https://www.europarl.europa.eu/doceo/document/TA-7-2011-0323_PL.html?redirect#def_1_5.

Wniosek Komisji Europejskiej z dnia 25 stycznia 2012 r. „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)", COM/2012/011 final.

Wniosek Komisji Europejskiej z dnia 10.01.2017 r. „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)", COM/2017/010 final - 2017/03.

EIOD, *Opinion 8/2018 on the legislative package "A New Deal for Consumers",* https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf.

Komunikat KE z dnia 11.04.2018 r. do Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego „Nowy ład dla konsumentów", COM(2018) 183 final.

Projekt ustawy o ochronie danych osobowych z dnia 12 września 2017 r., https://legislacja.rcl.gov.pl/docs//2/12302950/12457652/12457653/dokument308351.pdf.

Projekt ustawy o ochronie danych osobowych z dnia 8 lutego 2018 r, https://legislacja.rcl.gov.pl/docs//2/12302950/12457684/12457685/dokument334781.pdf.

Projekt ustawy o ochronie danych osobowych z dnia 16 marca 2018 r., https://legislacja.rcl.gov.pl/docs//2/12302950/12457690/12457691/dokument334233.pdf.

Uzasadnienie do projektu ustawy o ochronie danych osobowych z dnia 12 września 2017 r., https://legislacja.rcl.gov.pl/docs//2/12302950/12457652/12457653/dokument308352.pdf.

Uzasadnienie do projektu ustawy o ochronie danych osobowych z dnia 8 lutego 2018 r, https://legislacja.rcl.gov.pl/docs//2/12302950/12457684/12457685/dokument334783.pdf.

Uwagi Generalnego Inspektora Ochrony Danych Osobowych z dnia 20 października 2017 r. do projektu ustawy o ochronie danych osobowych z dnia 12 września 2017 r., https://legislacja.rcl.gov.pl/docs//2/12302950/12457664/12457667/dokument319357.pdf.

Uwagi Generalnego Inspektora Ochrony Danych Osobowych z dnia 27 lutego 2018 r. do projektu ustawy o ochronie danych osobowych z dnia 8 lutego 2018 r., https://legislacja.rcl.gov.pl/docs//2/12302950/12457684/12457686/dokument336356.pdf.

Stenogram z 60. posiedzenia Senatu RP IX kadencji, 4 dzień, https://www.senat.gov.pl/prace/senat/posiedzenia/przebieg,506,4.html#h1_171.

GIODO, Konieczne zmiany legislacyjne przepisów o ochronie danych osobowych - wstępna analiza ekspertów Biura GIODO, https://archiwum.giodo.gov.pl/pl/1520281/9747.

GIODO, Analiza opinii uczestników VII edycji Programu „Twoje dane – Twoja sprawa" na temat wieku dziecka w kwestii wyrażania przez nie zgody na przetwarzanie danych osobowych w świetle ogólnego rozporządzenia o ochronie danych, https://archiwum.giodo.gov.pl/pl/file/12018.

3. Literatura

Abu Gholeh M., Kuźnicka-Błaszkowska D., *Nakładanie administracyjnych kar pieniężnych w rozporządzeniu o ochronie danych. Aspekty praktyczne*, Warszawa 2020.

Adamiak B., *Skarga i skarga kasacyjna w postępowaniu sądowoadministracyjnym. Komentarz*, Warszawa 2014.

Adamus R., *Zgoda na przetwarzanie danych osobowych osoby nieposiadającej pełnej zdolności do czynności prawnych*, „Gazeta Sądowa" 2005, nr 2.

M. Amarikwa, *Social Media Platforms' Reckoning: The Harmful Impact of TikTok's Algorithm on People of Color*, „Richmond Journal of Law & Technology" 2023, nr 3

Andres K., Bielak-Jomaa E., Jagielski M., Kawczyński P., Krasińska M., Litwiński P., Sieradzka A., Wojsyk K., *Ochrona danych osobowych medycznych*, wyd. 2, Warszawa 2018.

Anrig B., Browne W., Gasson M., *The Role of Algorithms in Profiling*, [w:] Hildebrandt M., Gutwirth S. (red.), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Dordrecht 2008.

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Wyd. 2*, Warszawa 2012, Legalis.

Bârsan M. M., *A partial overview of the data subjects' control over their personal data under the General Data Protection Regulation*, „Bulletin of the Transilvania University of Brasov. Series VII: Social Sciences. Law" 2018, nr 2.

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, wyd. VI, Warszawa 2015, Lex.

Barta J., Markiewicz R., *Prawo do prywatności w społeczeństwie informatycznym*, „Ethos" 1999, nr 1/2 (45/46).

Bartoli E., *Children's data protection vs marketing companies*, „International Review of Law, Computers & Technology" 2009, nr 23.

Batorski D. (red.), *Cyfrowa gospodarka. Kluczowe trendy rewolucji cyfrowej. Diagnoza, prognozy, strategie reakcji*, Warszawa 2012.

Bąba M., *Próba wyznaczenia zakresu pojęcia danych biometrycznych*, „Prawo Mediów Elektronicznych" 2016, nr 2.

Bąbik A., Olejniczak D., *Uwarunkowania i profilaktyka samobójstw wśród dzieci i młodzieży w Polsce*, „Dziecko krzywdzone. Teoria, badania, praktyka" 2014, nr 2.

Behr J., *Prawo do wniesienia skargi do organu nadzorczego*, [w:] Behr J., Błażewski M., *Środki prawne ochrony danych osobowych*, Wrocław 2018.

Będźmirowski T., Zalewska A., *Modalność obowiązku informacyjnego* [w:] Wiewiórowski W. R., Wolska H. (red.), *Rok RODO*, Warszawa 2019, Legalis.

Bielak-Jomaa E., Lubasz D. (red.), *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016.

Bielak-Jomaa E., Lubasz D. (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2017.

Bienias M., *Ochrona danych w fazie projektowania oraz domyślna ochrona danych (privacy by design oraz privacy by default) w ogólnym rozporządzeniu o ochronie danych*, „Monitor Prawniczy" dodatek: *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, Sibiga G. (red.), 2016, nr 20.

Bienias M., *Zasada czasowego ograniczenia przechowywania danych osobowych na gruncie RODO*, „Prawo Mediów Elektronicznych" 2017, nr 4, Legalis.

Bieszczad M., *Dobro dziecka jako klauzula generalna – ustalenie znaczenia pojęcia dobra dziecka w XXI w.*, „Monitor Prawniczy" 2019, nr 17.

Bietti E., *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, „Pace Law Review" 2020, vol. 40, issue 1.

Blecher-Prigat A., *Children's Right to Privacy*, [w:] Dwyer J. G. (red.), *The Oxford Handbook of Children and the Law*, Oksford 2019.

Błachnio-Parzych A., *Przepisy karne w ustawie z 10.5.2018 r. o ochronie danych osobowych*, [w:] Sibiga G. (red.), *Przepisy prawa uzupełniające RODO. Aktualne problemy prawnej ochrony danych osobowych 2018* (dodatek do „Monitora Prawniczego" 2018, nr 22), Warszawa 2018.

Bodanka O., *Naruszenie wizerunku przy wykorzystaniu technologii deepfake – analiza prawna i praktyczna*, „Opolskie Studia Administracyjno-Prawne" 2022, nr 2.

Borkowska A., Witkowska M., *Sharenting i wizerunek dziecka w sieci. Poradnik dla rodziców*, Warszawa 2020.

Bróżek P., *Wniosek o orzeczenie obowiązku naprawienia szkody lub zadośćuczynienia za doznaną krzywdę jako skuteczna alternatywa dla pozwu cywilnego*, „Monitor Prawniczy" 2022, nr 22.

Brzozowska M., *Ochrona danych osobowych w sieci*, Wrocław 2012.

Buczma K., *Konstytucyjne podstawy prawa do ochrony danych osobowych*, [w:] Misztal-Konecka J., Tylec G. (red.), *Wizja europejskiego społeczeństwa informacyjnego i jej realizacji w prawie polskim*, Lublin 2012.

Budrewicz P., *Postanowienia dotyczące dziedziczenia profilu zawarte w regulaminie portalu Facebook a prawo polskie*, „Prawo mediów elektronicznych" 2018, nr 3.

Byczkowski M., *Znaczenie norm ISO we wdrażaniu bezpieczeństwa technicznego i organizacyjnego wymaganego w RODO*, [w:] „Monitor Prawniczy" dodatek: *Wdrażanie ogólnego rozporządzenia o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2017,* G. Sibiga (red.), 2017, nr 20.

Byrski J., *Odwołanie zgody na przetwarzanie danych osobowych. Wybrane zagadnienia*, „Monitor Prawniczy" dodatek: *Nowelizacja ustawy o ochronie danych osobowych 2010*, Sibiga G. (red.), 2011, nr 3.

Byrski J., *Przetwarzanie danych osobowych przez pośredników ubezpieczeniowych,* „Wiadomości Ubezpieczeniowe" 2019, nr 3.

Cebera A., *Nowa procedura doręczeń elektronicznych w postępowaniu administracyjnym*, „Ius Novum" 2023, nr 2.

Chałubińska-Jentkiewicz K., Taczkowska-Olszewska J., *Świadczenie usług drogą elektroniczną. Komentarz*, Warszawa 2019, Legalis.

Chałubińska-Jentkiewicz K., *Zagrożenia związane z nowymi technologiami. Cyberprzestępczość a bezpieczeństwo w sieci*, [w:] Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.

Chmielewski J., *Pełnomocnik i pełnomocnictwo w ogólnym postępowaniu administracyjnym*, „Monitor Prawniczy" 2016, nr 11.

Ciechomska M., *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy" 2017, nr 5.

Ciechomska M., *Zmiana Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych szansą na powstanie globalnego instrumentu ochrony danych*, [w:] Sibiga G. (red.), *Wdrażanie ogólnego rozporządzenia o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2017*, Warszawa 2017.

Cieniak K., *Obowiązek wyznaczenia inspektora ochrony danych osobowych*, „Monitor Prawniczy" 2018, nr 16.

Cieniak K., *Wybrane zagadnienia związane z obowiązkiem prowadzenia rejestru czynności przetwarzania*, „Monitor Prawniczy" 2018, nr 3.

Ciszewski J. (red.), *Kodeks cywilny. Komentarz*, Warszawa 2019.

Czapska M., Nożykowski R., *Wizerunek a nowe technologie – wybrane problemy prawne*, „Prawo Nowych Technologii" 2021, nr 1.

Czech T., *Prawa konsumenta. Komentarz, wyd. II*, Warszawa 2020.

Czerniawski M., *Instytucja współadministrowania a pojęcie „ustalania" celów i sposobów przetwarzania danych osobowych – zarys problemu*, [w:] Wiewiórowski W. R., Wolska H. (red.), *Rok RODO*, Warszawa 2019.

Czerniawski M., *Interes publiczny w ogólnym rozporządzeniu o ochronie danych. Wybrane zagadnienia*, „Informacja w administracji publicznej" 2019, nr 1.

Czerniawski M., *Obowiązki administratora danych wynikające z prawa do przenoszenia danych*, [w:] „Monitor Prawniczy" dodatek: *Wdrażanie ogólnego rozporządzenia o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2017*, Sibiga G. (red.), 2017, nr 20.

Czerniawski M., *Prawnie uzasadnione interesy jako podstawa przetwarzania danych online*, „Prawo Mediów Elektronicznych" 2018, nr 3, Legalis.

Czerniawski M., *Zakres terytorialny a pojęcie „jednostki organizacyjnej" w przepisach ogólnego rozporządzenia o ochronie danych – zarys problemu*, [w:] Sibiga G. (red.), *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, Warszawa 2016, Legalis.

Dmochowska A., Piotrowska A., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Dobek-Rak M., Mierzejewski P., Trzcińska D., Biernat K., *Ustawa o ewidencji ludności*, Warszawa 2013.

Dove E. S., Chens J., *What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e)*, „International Data Privacy Law" 2021, nr 2.

Drobek P., *Zasada celowości w dobie wielkich zbiorów danych (big data)*, [w:] „Monitor Prawniczy" dodatek: *Aktualne problemy prawnej ochrony danych osobowych 2014,* Sibiga G. (red.), 2014, nr 9.

Drozd A., *Pojęcie danych osobowych – uwagi wstępne*, [w:] Fajgielski P. (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008.

Duminică R., Drăghici A., *The processing of personal data regarding children, according to Regulation (EU) 2016/679*, „Valahia University Law Study" Supplement 2018.

Dziurda M., *Legitymacja do wytaczania powództw na rzecz konsumentów*, „Przegląd Sądowy" 2022, nr 11-12.

K. Eichhorn, *Why an internet that never forgets is especially bad for young people*, „MIT Technology Review" 27.12.2019.

Ereciński T. (red.), *Kodeks postępowania cywilnego. Komentarz. Tom I. Postępowanie rozpoznawcze, wyd. V*, Warszawa 2016.

Fajgielski, P. *Automatyczne rozpoznawanie twarzy – wybrane zagadnienia prawne*, [w:] Fischer B., Pązik A., Świerczyński M. (red.), *Prawo sztucznej inteligencji i nowych technologii*, Warszawa 2021.

Fajgielski P., *Funkcjonowanie portali społecznościowych – wybrane problemy prawne*, [w:] Szpor G., Wiewiórowski W. R. (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, Warszawa 2012.

Fajgielski P., *Informowanie o naruszeniu ochrony danych osobowych w świetle przepisów ogólnego rozporządzenia o ochronie danych*, „Monitor Prawniczy" dodatek: *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, Sibiga G. (red.), 2016, nr 20.

Fajgielski P., *Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno-prawne*, Lublin 2008.

Fajgielski P., *Rzetelność jako ogólna zasada przetwarzania danych osobowych*, „Gdańskie Studia Prawnicze" 2021, nr 4.

Fajgielski P., *Obowiązek informacyjny z perspektywy dwóch lat stosowania nowych przepisów o ochronie danych osobowych*, „Monitor Prawniczy" dodatek: *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020*, Sibiga G. (red.), 2020, nr 23.

Fajgielski P., *Ochrona danych osobowych przedsiębiorcy będącego osobą fizyczną*, [w:] Zdyb M., Kruk E., Lubeńczuk G. (red.), *Dysfunkcje publicznego prawa gospodarczego*, Warszawa 2018, Legalis.

Fajgielski P., *Odwoływalność zgody na przetwarzanie danych osobowych – znaczenie dla praktyki gospodarczej*, [w:] Mednis A. (red.), *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, Warszawa 2013.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. 2, Warszawa 2022.

Fajgielski P., *Prawo do przenoszenia danych*, „Informacja w administracji publicznej" 2017, nr 4.

Fajgielski P., *Przetwarzanie szczególnych kategorii danych w świetle ogólnego rozporządzenia o ochronie danych*, [w:] Czaplicki K., Szpor G. (red.), *Internet. Przetwarzanie danych osobowych. Processing of personal data*, Warszawa 2019, Legalis.

Fajgielski P., Rejestry czynności przetwarzania danych osobowych, [w:] „Monitor Prawniczy" dodatek: *Wdrażanie ogólnego rozporządzenia o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2017*, Sibiga G. (red.), 2017, nr 20.

Fajgielski P., *Upoważnienie do przetwarzania danych osobowych*, „Studia Prawnicze KUL" 2020, nr 1.

Fajgielski P., *Zasady ogólne przetwarzania i ochrony danych osobowych*, [w:] Goździewicz G., Szabłowska M. (red.), *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów*, Toruń 2008.

Fajgielski P., *Zgoda na przetwarzanie danych osobowych w przepisach ogólnego rozporządzenia o ochronie danych*, „Informacja w administracji publicznej" 2016, nr 4, Legalis.

Fajgielski P., *Zgoda udzielana na przetwarzanie danych osobowych udzielana w Internecie*, [w:] Szpor G. (red.), *Internet. Ochrona wolności, własności i bezpieczeństwa*, Warszawa 2011.

Fischer B., Pązik A., Świerczyński M. (red.), *Prawo sztucznej inteligencji i nowych technologii*, Warszawa 2021.

Ferenc-Szydełko E., *Wizerunek dziecka jako dobro prawnie chronione. Wybrane zagadnienia*, [w:] Andrzejewski M. (red.), *Księga jubileuszowa prof. dr hab. Tadeusza Smyczyńskiego*, Toruń 2008.

Fischer B., *Pojęcie analizy ryzyka przy przetwarzaniu danych osobowych,* [w:] Szpor G., Czaplicki K. (red.), *Internet. Analityka danych. Data Analytics*, Warszawa 2019.

Fleszer D., *Dokumentacja przetwarzania danych osobowych,* „Roczniki Administracji i Prawa" 2017, nr XVII.

Fras M., Habdas M. (red.), *Kodeks cywilny. Komentarz. Tom I. Część ogólna (art. 1-125)*, Warszawa 2018, LEX.

Gałęzowska K., Dokumentowanie zgodności z przepisami RODO, „Monitor Prawniczy" dodatek: *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020*, Sibiga G. (red.), 2020, nr 23.

Gałęzowska K., *Współadministrowanie danymi osobowymi – wybrane problemy prawne*, [w:] Mielczarek M. A., Wyka T. (red.), *Administrator i inspektor ochrony danych osobowych. Pozycja prawna*, Warszawa 2019.

Geburczyk F., *Prawa osób fizycznych w kontekście przetwarzania danych osobowych w procesach zautomatyzowanego podejmowania decyzji*, „Monitor Prawniczy" 2020, nr 11.

Giermak M., Sofronów M., *Zgoda na przetwarzanie danych osobowych dzieci w serwisach społecznościowych w kontekście zmian prawa europejskiego*, „Monitor Prawniczy" 2017, nr 2.

Giurgiu A., Larsens T. A., *Roles and Powers of National Data Protection Authorities. Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?*, „European Data Protection Law Review" 2016, nr 3.

Głąb P., *Transfer danych osobowych do Stanów Zjednoczonych po stwierdzeniu nieważności decyzji w sprawie tarczy prywatności UE–USA*, „Radca Prawny. Zeszyty Naukowe" 2021, nr 1.

Gniewek E., Machnikowski P. (red.), *Kodeks cywilny. Komentarz,* wyd. 9, Warszawa 2019, Legalis.

Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999.

Gołaczyński J. (red.), *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Warszawa 2009.

González Fuster G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Bruksela 2014.

González-Rodríguez M. R., Díaz-Fernández M. C., Pacheco Gómez C., *Facial-expression recognition: An emergent approach to the measurement of tourist satisfaction through emotions*, „Telematics and Informatics" 2020, nr 51.

Góral U., *Europejska Rada Ochrony Danych – proces transformacji Grupy Roboczej Art. 29*, [w:] Sibiga G. (red.), *Wdrażanie ogólnego rozporządzenia o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2017*, Warszawa 2017.

Góral U., Kwasny S., *Proces modernizacji Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych*, „Monitor Prawniczy" dodatek: *Aktualne problemy prawnej ochrony danych osobowych 2014*, Sibiga G. (red.), 2014, nr 9.

Góral U., *Rola organu ochrony danych w edukacji na temat prawa do prywatności i ochrony danych*, [w:] Fidelus A., Babicki Z. (red.), *Prawa dziecka w wybranych kontekstach opiekuńczo-wychowawczych*, Warszawa 2019.

Graef I., Husovec M., Purtova N., *Data Portability and Data Control: Lessons for an Emerging Concept in EU Laws*, „German Law Journal" 2018, nr 6.

Gregory Voss W., *The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation*, „Journal of Internet Law" 2014, vol. 18, nr 1.

Grobel S., *Treść władzy rodzicielskiej*, [w:] Łukasiewicz J. M. (red.), *Instytucje prawa rodzinnego*, Warszawa, 2014.

Gryszczyńska A., *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości – zakres przedmiotowy i podmiotowy,* [w:] Czaplicki K., Szpor G. (red.)*, Internet. Przetwarzanie danych osobowych. Processing of personal data,* Warszawa 2019, Legalis.

Grzelak A. (red.), *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz,* Warszawa 2019.

Grześkowiak A., Wiak K. (red.), *Kodeks karny. Komentarz*, wyd. 7, Warszawa 2021, Legalis.

Gumularz M., Kozik P. (red.), *Ochrona danych osobowych w marketingu i sprzedaży*, Warszawa 2019, Legalis.

Gumularz M., *Wpływ regulacji odpowiedzialności odszkodowawczej w ogólnym rozporządzeniu o ochronie danych osobowych na systemy prawa prywatnego państw członkowskich*, „Europejski Przegląd Sądowy" 2017, nr 5.

Haberko J., *Udostępnianie i publikowanie wizerunku nasciturusa, noworodka i małego dziecka w świetle zasady dobra dziecka*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2013, zeszyt 3.

Harbinja E., *Post-mortem privacy 2.0: theory, law, and technology*, „International Review of Law, Computers & Technology" 2017, nr 31.

Helios J., Jedlecka W., *Wykładnia prawa Unii Europejskiej ze stanowiska teorii prawa*, Wrocław 2018.

Hildebrandt M., *Profiling: From Data to Knowledge. The challenges of a crucial technology*, "Datenschutz und Datensicherheit" 2006, nr 30.

Hołda J., *Prawa człowieka w Unii Europejskiej*, [w:] Hołda J., Hołda Z., Ostrowska D., Rybczyńska J. A., *Prawa człowieka. Zarys wykładu*, Warszawa 2011.

Hustinx P., *Data protection and international organizations: a dialogue between EU law and international law*, „International Data Privacy Law" 2021, Vol. 11, nr 2.

Izdebski J., hasło „decyzja administracyjna", [w:] Domagała M., Haładyj A., Wrzosek S. (red.), *Encyklopedia prawa administracyjnego*, Warszawa 2010.

Izydorczyk T., *Media społecznościowe a ochrona danych osobowych*, [w:] Gumularz M., Kozik P. (red.), *Ochrona danych osobowych w marketingu i sprzedaży*, Warszawa 2019, Legalis.

Jabłoński M., Węgrzyn J., *Prawo do bycia zapomnianym,* Wrocław 2021.

Jackowski M. (red.), *Ochrona danych medycznych. RODO w ochronie zdrowia*, Warszawa 2018.

Jagielski M., *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010, s. 10.

Jakubik M., Witas K., *Systemy DLP a ochrona danych osobowych – zasada rozliczalności*, [w:] Gryszczyńska A., Szpor G., Wiewiórski W.R. (red.), *Internet Hacking*, Warszawa 2023, Legalis.

Janowski J., *Kontrakty elektroniczne w obrocie prawnym*, rozdział III pkt 1.2, Warszawa 2008, LEX.

Janssen H. J., *An approach for a fundamental rights impact assessment to automated decision-making*, „International Data Privacy Law" 2020, nr 1.

Jaros P., *Rzecznik Praw Dziecka w Polsce: ukształtowanie Rzecznika Praw Dziecka w Polsce jako organu państwowego, komentarz do ustawy o Rzeczniku Praw Dziecka*, Warszawa 2013.

Jaśkowska M., Wilbrandt-Gotowicz M., Wróbel A., *Komentarz aktualizowany do Kodeksu postępowania administracyjnego*, LEX 2023.

Kahler T., *Accountability – the gravity centre of GDPR*, [w:] Kahler T. (red.), *Turning Point in Data Protection Law*, Baden-Baden 2020.

Kalina P., *Dokumentacja ochrony danych osobowych w RODO*, „Informacja w administracji publicznej) 2018, nr 3.

Kaminski M., Malgieri G., *Algorithmic impact assessments under the GDPR: producing multi-layered explanations*, „International Data Privacy Law" 2021, Vol. 2, nr 2.

Karwala D., *Komercyjne transfery danych osobowych do państw trzecich*, Warszawa 2018.

Karwala D., *Krajobraz po wyroku Trybunału Sprawiedliwości w sprawie programu Bezpiecznej Przystani*, „Monitor Prawniczy" 2016, nr 10.

Karwala D., *Transfer Impact Assessment – nowy wymóg związany z międzynarodowym przekazywaniem danych osobowych*, [w:] Sakowska-Baryła M. (red.), *Sztuczna inteligencja, transfery, odpowiedzialność i inne wyzwania ochrony danych osobowych*, Wrocław 2022.

Karwala D., *Wpływ ogólnego rozporządzenia o ochronie danych osobowych na działalność zakładów ubezpieczeń – zagadnienia wybrane*, „Prawo Asekuracyjne" 2016, nr 4.

Karwala D., *Znaczenie soft law dla transferów danych osobowych do państw trzecich na przykładzie zaleceń EROD 01/2020,* „Monitor Prawniczy" dodatek: *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych – Aktualne problemy ochrony danych osobowych 2021*, Sibiga G. (red.), 2021, nr 23.

Kawecki M., Czerniawski M. (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2019, Legalis.

Kaźmierczak J., *Prawo do przenoszenia danych osobowych – wybrane zagadnienia na tle realizacji nowego uprawnienia przyznanego przez RODO*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2018, nr 4.

Kesa A., Kerikmäe T., *Artificial Intelligence and the GDPR: inevitable nemeses?*, „TalTech Journal of European Studies" 2020, nr 3.

Kępa L., *Bezpieczeństwo danych osobowych. Podejście oparte na ryzyku*, Warszawa 2019, Legalis.

Kidyba A. (red.), *Kodeks cywilny. Komentarz. Tom I. Część ogólna*, wyd. II, Warszawa 2012, LEX.

Kielan A., Cieślak I., Skonieczna J., Olejniczak D., Jabłkowska-Górecka K., Panczyk M., Gotlib J., Zalewska-Zielecka B., *Analysis of the opinions of adolescents on the risk factors of suicide,* „Psychiatria Polska" 2018, nr 4.

Kmieciak Z., Wegner J., Wojtuń M., *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2023.

Kmiecik Z. R., *Etap wszczęcia postępowania administracyjnego ogólnego*, [w:] Łaszczyca G., Matan A. (red.), *System Prawa Administracyjnego Procesowego*: Martysz C. (red.), tom II część 4. *Dynamika postępowania administracyjnego ogólnego*, Warszawa 2021.

Kobylańska A., Lewoszewski M., P*oland: A Brief Overview Concerning the Implementation of the GDPR,* "European Data Protection Law Review" 2017, nr 4.

Kociucki L., *Zdolność do czynności prawnych w prawie europejskim – zagadnienia wybrane*, [w:] Andrzejewski M., Kociucki L., Łączkowska M., Schulz A.N. (red.), *Rozprawy z zakresu prawa cywilnego. Księga Jubileuszowa Profesora Tadeusza Smyczyńskiego*, Toruń 2008.

Konarski X., *Dostosowanie przepisów sektorowych dotyczących usług łączności elektronicznej do wymogów RODO*, [w:] „Monitor Prawniczy" dodatek: *Polskie przepisy o ochronie danych osobowych. Aktualne problemy prawnej ochrony danych osobowych 2019*, Sibiga G. (red.), 2019, nr 22.

Konarski X., *Profilowanie danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych osobowych – dotychczasowy i przyszły stan prawny w UE oraz w Polsce*, [w:] „Monitor Prawniczy" dodatek: *Aktualne problemy prawnej ochrony danych osobowych 2016*, Sibiga G. (red.), 2016, nr 20.

Konarski X., *Rozporządzenie o e-Prywatności jako regulacja sektorowa względem ogólnego rozporządzenie o ochronie danych osobowych (RODO)*, [w:] „Monitor Prawniczy" dodatek: *Wdrażanie ogólnego rozporządzenia o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2017,* Sibiga G. (red.), 2017, nr 20.

Konarski X., *Unijny Akt o Usługach Cyfrowych – cele uchwalenia, zakres stosowania oraz najważniejsze obowiązki dostawców usług pośrednich*, „Prawo Nowych Technologii" 2022, nr 3.

Kopff A., *Koncepcja praw do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne)*, „Studia Cywilistyczne" 1972, t. 20.

Kosik J., *Komputer i prawa dziecka*, „Acta Universitatis Wratislaviensis" 1981, nr 582.

Kosinski M., Stillwell D., Graepel T., *Private traits and attributes are predictable from digital records of human behavior*, "Proceedings of the National Academy of Sciences" 2013, nr 15.

Kowalczuk-Pakuła I., Borkowski M., *Co to jest transfer danych?*, [w:] Sakowska-Baryła M. (red.), *Sztuczna inteligencja, transfery, odpowiedzialność i inne wyzwania ochrony danych osobowych*, Wrocław 2022.

Kowalczuk-Pakuła I., Chołuj M., *Przekazywanie danych do państwa trzeciego – w poszukiwaniu definicji*, „Prawo Nowych Technologii" 2021, nr 1.

Kozik P., *Zakres swobody regulacyjnej państw członkowskich przy wdrażaniu ogólnego rozporządzenia o ochronie danych osobowych do prawa krajowego, „*Europejski Przegląd Sądowy" 2017, nr 5.

Krajewska-Kekusz D., *Uprzednie konsultacje: cele, warunki i przebieg (zarys problemu)*, „Informacja w administracji publicznej" 2018, nr 2.

Krasuski A., Siembida P., Analiza ryzyka w ochronie danych osobowych, Warszawa 2022.

Krasuski A., *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018.

Krzysztofek M., *„Prawo do bycia zapomnianym" i inne aspekty prywatności w epoce Internetu w prawie UE,* „Europejski Przegląd Sądowy" 2012, nr 8.

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016, Legalis.

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej*, Warszawa 2014.

Księżak P., Pyziak-Szafnicka M. (red.), *Kodeks cywilny. Komentarz. Część ogólna*, wyd. II, Warszawa 2014.

Kulesza E., *Nowe obowiązki administratorów danych osobowych w świetle RODO*, [w:] Mielczarek M. A., Wyka T. (red.), *Administrator i inspektor ochrony danych osobowych. Pozycja prawna*, Warszawa 2019.

Kuner C., Bygrave L. A., Docksey C., Drechsler L. (red.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oksford 2020.

Kuner C., *The GDPR and International Organizations*, „American Journal of International Law Unbound" 2020, Vol. 114.

Kuner C., *The Internet and the Global Reach of EU Law*, [w:] Cremona M., Scott J. (red.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, Oxford 2019.

Kupiec M., *O potrzebie przyjęcia nowego podejścia do ochrony danych osobowych dzieci przez EROD. Uwagi w świetle Opinii nr 2/2009 Grupy Roboczej Art. 29 o ochronie danych osobowych dzieci*, [w:] „Monitor Prawniczy" dodatek: *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych. Aktualne problemy ochrony danych osobowych 2021*, Sibiga G. (red.), 2021, nr 23.

Kupiec M., *Profilowanie dzieci dla celu marketingu cyfrowego w europejskim prawie ochrony danych osobowych. Między paternalizmem a potrzebą realizacji najlepiej pojętego interesu dziecka*, [w:] Sakowska-Baryła M. (red.), *Sztuczna inteligencja, transfery, odpowiedzialność i inne wyzwania ochrony danych osobowych*, Wrocław 2022.

Kusak M., Wiliński P., *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne,* Warszawa 2020.

Kuźnicka D., *Prawo do tożsamości jako prawo dziecka – wybrane zagadnienia*, „Folia Iuridica Universitatis Wratislaviensis" 2016, nr 5.

Kuźnicka-Błaszkowska D., *Prawna ochrona życia prywatnego a ochrona informacji o sobie samym w Konstytucji RP w orzecznictwie Trybunału Konstytucyjnego – wybrane aspekty*, „Acta Universitatis Wratislaviensis" 2020, nr 121.

Kuźnicka-Błaszkowska D., *Protecting Children's Personal Data under General Data Protection Regulation and California Consumer Privacy Act in Relation to Information Society Services – European Perspective*, „Przegląd Prawa Konstytucyjnego" 2022, nr 2.

Lach A., *Kradzież tożsamości*, „Prokuratura i Prawo" 2012, nr 3.

Lai L., Świerczyński M. (red.), *Prawo sztucznej inteligencji*, Warszawa 2020.

Lievens E., Vander Maelen C., *A Child's Right to be Forgotten: Letting Go of the Past and Embracing the Future?*, „Latin American Law Review" 2019, nr 2.

Lipowicz I., *Konstytucyjne podstawy ochrony danych osobowych*, [w:] Fajgielski P. (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008.

Lis W., *Zjawisko profilowania jako przejaw naruszenia prawa do prywatności w środowisku cyfrowym*, [w:] Chałubińska-Jentkiewicz K., Kakareko K., Sobczak J. (red.), *Prawo prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017.

Litwiński P., Kaźmierczak K., *Elementarz ochrony danych osobowych*, [w:] Dörre-Kolasa D. (red.), *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2017.

Litwiński P., *Nowe rozporządzenie ogólne w sprawie ochrony danych osobowych i jego wpływ na społeczeństwo informacyjne. Wybrane zagadnienia*, [w:] Flaga-Gieruszyńska K., Gołaczyński J., Szostek D. (red.), *Media elektroniczne. Współczesne problemy prawne,* Warszawa 2016.

Litwiński P. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021, Legalis.

Litwiński P., *Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – glosa do wyroku Trybunału Sprawiedliwości z 19.10.2016 r. w sprawie C-582/14 Patrick Breyer*, „Europejski Przegląd Sądowy" 2017, nr 5.

Litwiński P. (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, Legalis.

Litwiński P. (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Litwiński P., *Zasada autonomii informacyjnej w orzecznictwie Trybunału Konstytucyjnego a stosowanie przepisów o ochronie danych osobowych*, [w:]. Fajgielski P (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008.

Longchamps de Bérier F., *The status of a bearer of rights within the European legal tradition: the tradition of Rome and Jerusalem – a case study*, "Fundamina" 2013, nr 19.

Lubasz D. (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2019.

Lubasz D., Namysłowska M. (red.), *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, Warszawa 2011, LEX.

Łętowska E., Osajda K., *Wprowadzenie do części ogólnej zobowiązań* [w:] Osajda K. (red.), *Prawo zobowiązań – część ogólna. System Prawa Prywatnego tom 5*, wyd. 3, Warszawa 2020.

Łukasiewicz R., *Dobro dziecka a interesy innych podmiotów w polskiej regulacji prawnej przysposobienia*, Warszawa 2019.

Macenaite M., Kosta E., *Consent for processing children's personal data in the EU: following in US footsteps?*, "Information & Communications Technology Law" 2017.

Maciejewska-Szałas M., *Organizacje pozarządowe i formy ich uczestnictwa w postępowaniu cywilnym*, „Gdańskie Studia Prawnicze" 2017, nr 2.

Malgieri G., *The concept of Fairness in the GDPR. A linguistic and contextual interpretation*, [w:] *FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, Nowy Jork 2020.

Małobęcka-Szwast I., *Naruszenie prawa ochrony danych osobowych jako nadużycie pozycji dominującej? Postępowanie Bundeskartellamt przeciwko Facebookowi*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2018, nr 8.

Maniszewska-Ejsmont J., *Sharenting a prawa dziecka– rozważania nad władzą rodzicielską w dobie mediów społecznościowych*, „Palestra" 2022, nr 4.

Marcinkowski B. (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Marcinkowski B., *Ochrona danych osobowych pacjenta w telemedycynie w świetle RODO*, [w:] Lipowicz I., Szpor G., Świerczyński M. (red.), *Telemedycyna i e-Zdrowie. Prawo i informatyka*, Warszawa 2019.

Marcinkowski B., *Przekazywanie danych osobowych do państw trzecich. Ramy prawne i praktyka w świetle wyroków Schrems I i Schrems II*, „Monitor Prawniczy" dodatek: *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020*, Sibiga G. (red.), 2020, nr 23.

Marcinkowski B., *Przepływy danych osobowych w międzynarodowych grupach kapitałowych*, „Monitor Prawniczy" dodatek: *Wpływ technologii i technik informatycznych na ochronę danych osobowych – Aktualne problemy ochrony danych osobowych 2022*, Sibiga G. (red.), 2022, nr 21.

Mascheroni, G. Holloway D., *Introducing the Internet of Toys,* [w:] Mascheroni G., Holloway D. (red.), *The Internet of Toys. Practices, Affordances and the Political Economy of Children's Smart Plays*, Cham 2019.

Matysiak M., *Ochrona prywatności użytkowników gier wideo – zarys problematyki prawnej*, [w:] „Monitor Prawniczy" dodatek: *Prawo nowych technologii - dane osobowe i prywatność, cyberbezpieczeństwo, handel elektroniczny, innowacje, internet i media, prawo IT*, Konarski X. (red.), 2020, nr 20.

Mądel M., *Następstwo prawne treści cyfrowych na wypadek śmierci*, Warszawa 2018, Legalis.

Mc Cullagh K., *The general data protection regulation: a partial success for children on social network sites*?, [w:] Bräutigam T., Miettinen S. (red.), *Data Protection, Privacy And European Regulation In The Digital Age*, Helsinki 2016.

Mednis A., *Analityka w bankowości*, [w:] Szpor G., Czaplicki K. (red.), *Internet. Analityka danych. Data Analytics*, Warszawa 2019.

Mednis A., *Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej*, „Państwo i Prawo" 1997, nr 6.

Mednis A., *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, Warszawa 2019.

Mednis A., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999, Lex.

Mednis A., *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych*, „Monitor Prawniczy" dodatek: *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, Sibiga G. (red.), 2016, nr 20.

Mianowana-Kubiak R., *Małoletni jako strona w umowie rachunku wspólnego – rozważania na tle ustaw: Kodeks cywilny, Kodeks rodzinny i opiekuńczy oraz Prawo bankowe*, „Monitor Prawa Bankowego" 2014, nr 5.

Miernik M., *Wizerunek a nowe technologie. Wizerunek jako dana biometryczna*, „Prawo Nowych Technologii" 2022, nr 3.

Mihăilă C. O., Mihăilă M., The *legal interest, legal basis for the processing of personal data and the right to private life,* „Fiat Iustitia" 2020, nr 1.

Milkaite I., Lievens E., *Children's Rights to Privacy and Data Protecton Around the World: Challenges in the Digital Realm*, „European Journal of Law and Technology" 2019, Vol 10, Issue 1.

Milkaite I., Lievens E., *The Internet of Toys: Playing Games with Children's Data?,* [w:] Mascheroni G., Holloway D. (red.), *The Internet of Toys. Practices, Affordances and the Political Economy of Children's Smart Plays*, Cham 2019.

Milkaite I., Verdoodt V., Martens H., Lievens E., *The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society. Roundtable Report*, Bruksela 2017.

Młotkiewicz M., *Powierzenie przetwarzania w sektorze publicznym na wybranych przykładach*, „Informacja w administracji publicznej" 2020, nr 2.

Morawska K., *Rola oraz status prawny motywów preambuły ogólnego rozporządzenia o ochronie danych – klucz do wykładni przepisów nowego prawa unijnego*, [w:] Kawecki M., Osiej T., *Ogólne rozporządzenie o ochronie danych. Wybrane zagadnienia*, Warszawa 2017.

Mostowik M., *Ochrona danych osobowych w Internecie rzeczy w prawie UE*, Warszawa 2022, Legalis.

Nierodka A., *Badanie zdolności kredytowej konsumentów*, [w:] Heropolitańska I., Nierodka A., Zdziarski T., *Kredyty, pożyczki i gwarancje bankowe*, Warszawa 2021.

Niklas J., *Problem dyskryminacji automatycznej – uwagi na tle ogólnego rozporządzenia o ochronie danych osobowych*, „Europejski Przegląd Sądowy" 2019.

Nowak J. S., *Społeczeństwo informacyjne - geneza i definicje*, [w:] Sienkiewicz P., Nowak J. S. (red.), *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz,* Katowice 2008.

Nowak W., *Specyfika zagrożeń w cyberprzestrzeni*, [w:] Banasiński C., Rojszczak M. (red)., *Cyberbezpieczeństwo*, Warszawa 2020.

Nowak-Byrtek D., *Realizacja prawa dostępu w związku z przetwarzaniem danych z plików cookies lub innych technologii śledzących – problemy wybrane*, [w:] „Monitor Prawniczy" dodatek: *Wpływ technologii i technik informatycznych na ochronę danych osobowych. Aktualne problemy prawnej ochrony danych osobowych 2022*, Sibiga G. (red.), 2022, nr 21.

O'Hara K., Tuffield M. M., Shadbolt N., *Lifelogging: Privacy and Empowerment with Memories for Life*, „Identity in the Information Society" 2009, nr 1, s. 155-172.

Olejniczak A. (red.), *Prawo cywilne - część ogólna. System Prawa Prywatnego. Tom 2*, wyd. III, Warszawa 2019.

Olszewska M., *Prawne zasady dotyczące plików cookies a ochrona danych osobowych użytkowników Internetu*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2017, nr 7.

Olszewski B., *Uniwersalna definicja dziecka*, „Przegląd Prawa i Administracji" 2011, nr 85.

Osajda K., *Prawo spadkowe (w) przyszłości. Perspektywy rozwoju prawa spadkowego*, „Monitor Prawniczy" 2019, nr 2.

Osiejewicz J., *Harmonizacja prawa państw członkowskich Unii Europejskiej*, Warszawa 2016, Legalis.

Pachulska-Smulska B., *Konsument na jednolitym rynku cyfrowym*, [w:] Królikowska-Olczak M., Pachulska-Smulska B. (red.), *Ochrona prawna konsumenta na rynku mediów elektronicznych*, Warszawa 2015, Legalis.

Pawełko A., *Autonomia woli konsumenta w kontekście praktyk typu dark patterns*, [w:] Namysłowska M., Podgórski K., Sługocka-Krupa E. (red.), *Wyzwania dla prawa konsumenckiego w wymiarze globalnym, regionalnym i lokalnym*, Warszawa 2022, Legalis.

Pazdan M., Glosa do postanowienia SN z dnia 15 grudnia 1999 r., I CKN 299/98, LEX.

Pązik A., *Szkoda wynikająca z naruszenia przepisów RODO. Wybrane problemy*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2020, nr 3.

Persano F., *GDPR and Children Rights in EU Data Protection Law*, „European Journal of Privacy Law & Technologies. Special Issue", Foglia M. (red.), 2020.

Piątek S., *Prawne warunki stosowania cookies*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2015, nr 6.

Piątek S., *Prawo telekomunikacyjne. Komentarz*, Warszawa 2019, Legalis.

Pietrzykowski K. (red.), *Kodeks cywilny tom I. Komentarz. Art. 1–449[10]*, wyd. 10, Warszawa 2020, Legalis.

Pietrzykowski K. (red.), *Kodeks rodzinny i opiekuńczy. Komentarz*, Warszawa 2020, Legalis.

Piotrowski R., Prawo do prywatności i ochrony danych osobowych jako wartości konstytucyjne, [w:] Mednis A. (red.), *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, Warszawa 2016.

Płociński M., *Dalekopis - historia teleksu*, „Rzeczpospolita” 08.02.2012.

Polański P., *Europejskie prawo handlu elektronicznego. Mechanizm regulacji usług społeczeństwa informacyjnego*, Warszawa 2014, Legalis.

Poniatowski P., *Niedopuszczalne lub nieuprawnione przetwarzanie danych osobowych – aspekty prawnokarne*, „Prokuratura i Prawo” 2021, nr 11.

Pormeister K., Drożdżowski, Ł. *Protecting the Genetic Data of Unborn Children: A Critical Analysis*, “European Data Protection Law Review” 2018, nr 1.

Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, „Law, Innovation and Technology” 2018, vol. 10, nr 1.

Recio M., *Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability*, „European Data Protection Law Review” 2017, nr 1.

Rojszczak M., *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019.

Rowiński W., *Nakaz dokonywania wykładni prounijnej jako dyrektywa wykładni systemowej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny” 2016, nr 1.

Rywczyńska A., Jaroszewski P., I*nternet zabawek. Wsparcie dla rozwoju dziecka czy zagrożenie,* Warszawa 2018.

Rzewuski M., *Definicja dziecka w Polsce. Uwagi de lege lata i de lege ferenda,* “Rejent” 2007, nr 7.

Safjan M., Bosek L., *Konstytucja RP. Tom I. Komentarz do art. 1–86*, Warszawa 2016, Legalis.

Safjan M., *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym,* „Państwo i prawo” 2002, nr 6.

Sakowska- Baryła M., Więckowska M., *Dokumentacja monitorowania zgodności z RODO – audyty wewnętrzne i weryfikacja powierzenia przetwarzania*, [w:] Jagielski M. (red.), *Dokumentacja ochrony danych osobowych ze wzorami*, wyd. 2, Warszawa 2022.

Sakowska-Baryła M., *Dostęp do informacji publicznej a ochrona danych osobowych*, Wrocław 2014.

Sakowska-Baryła M. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, Legalis.

Sakowska-Baryła M., *Przesłanki dopuszczalności przetwarzania danych osobowych w art. 23 ustawy o ochronie danyc*h, „Przegląd Prawa Handlowego" 2007, nr 10.

Sakowska-Baryła M., *Wykonywanie funkcji inspektora ochrony danych – aspekty etyczne*, „Monitor Prawa Pracy" 2020, nr 12.

Sakowska-Baryła M., Wyporska-Frankiewicz Joanna, *Zadania i decyzje Prezesa Urzędu Ochrony Danych Osobowych*, „Roczniki Nauk Prawnych" 2022, nr 1.

Sakowska-Baryła M., *Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu*, [w:] Szpor G., Czaplicki K. (red.), *Internet. Przetwarzanie danych osobowych. Processing of personal data*, Warszawa 2019, Legalis.

Scudiero L., *Bringing Your Data Everywhere: A Legal Reading Of The Right To Portability*, „European Data Protection Law Review" 2017, nr 1.

Sibiga G., *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzeni o ochronie danych – wybrane zagadnienia* [w:] Sibiga G. (red.), *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, Warszawa 2016.

Sibiga G., *Jak nie informatyzować administracji*, „Rzeczpospolita" 18.07.2022 r.

Sibiga G., *Kryterium „zadania publicznego" w ustawie z 10.5.2018 r. o ochronie danych osobowych oraz jego konsekwencje dla wykonywania obowiązków administratora oraz realizacji praw osoby, której dane dotyczą*, [w:] „Monitor Prawniczy" dodatek: *Przepisy prawa uzupełniające RODO. Aktualne problemy prawnej ochrony danych osobowych 2018,* Sibiga G. (red.), 2018, nr 22.

Sibiga G., *Skarga do organu nadzorczego oraz jej rozpatrzenie według ogólnego rozporządzenia o ochronie danych. Postępowanie w przedmiocie skargi osoby, której dane dotyczą*, „Prawo mediów elektronicznych" 2017, nr 4.

Sibiga G., *Wyłączenie zakazu zautomatyzowanego podejmowania decyzji w przepisach prawa polskiego w świetle wymagań ogólnego rozporządzenia o ochronie danych (RODO) – wybrane zagadnienia*, [w:] „Monitor Prawniczy" dodatek: *Wpływ technologii i technik informatycznych na*

ochronę danych osobowych. Aktualne problemy prawnej ochrony danych osobowych 2022, Sibiga G. (red.), 2022, nr 21.

Siemkowicz P., *Zakres skuteczności regulacji art. 190a § 2 KK dla zwalczania działań sprawczych związanych z tzw. kradzieżą tożsamości w sieci Internet*, „Prawo Mediów Elektronicznych" 2018, nr 1.

Siwicki M., *Ochrona osób fizycznych w związku z przetwarzaniem i swobodnym przepływem danych osobowych (uwagi w związku z projektem rozporządzenia Parlamentu Europejskiego i Rady*), „Państwo i Prawo" 2016, nr 3.

Skraba K., Strzałkowski I., *Media społecznościowe jako źródło dowodu w polskim procesie karnym. Badanie orzecznictwa sądów apelacyjnych i Sądu Najwyższego*, [w:] Waszkiewicz P. (red.), *Media społecznościowe w pracy organów ścigania*, Warszawa 2021.

Słocka L., *Obowiązki informacyjne przedsiębiorcy charakterystyczne dla świadczenia usług drogą elektroniczną na rzecz konsumenta a plain language i warstwowe obowiązki informacyjne jako próba rozwiązania problemu tzw. information overkill*, „Prawo Mediów Elektronicznych" 2022, nr 4.

Smyczyński T. (red.), *Konwencja o prawach dziecka. Analiza i wykładnia*, Poznań 1999.

Smyczyński T. (red.), *Prawo rodzinne i opiekuńcze. System Prawa Prywatnego. Tom 12*, wyd. II, Warszawa 2011.

Sołtys B., *Wątpliwości wokół konstytucyjności sankcji karnych i administracyjno-karnych za naruszenie przepisów o ochronie danych osobowych*, „Przegląd Sejmowy" 2019, nr 5.

Spindler G., Schmechel P., *Personal Data and Encryption in the European General Data Protection Regulation*, „Journal of Intellectual Property, Information Technology and Electronic Commerce Law" 2016, nr 2.

Stachyra K., *Ułatwienie swobodnego przepływu danych osobowych i wsparcie rozwoju gospodarki cyfrowej na rynku wewnętrznym w świetle ogólnego rozporządzenia o ochronie danych*, „Studia i Materiały Miscellanea Oeconomicae" 2018, nr 3.

Stojanowska W., *Dobro dziecka jako instrument wykładni norm konwencji o prawach dziecka oraz prawa polskiego i jako dyrektywa jego stosowania*, [w:] Smyczyński T. (red.), *Konwencja o prawach dziecka. Analiza i wykładnia*, Poznań 1999.

Strugała R., *RODO a odpowiedzialność odszkodowawcza. Podstawowe problemy odpowiedzialności za szkodę spowodowaną nieprawidłowym przetwarzaniem danych osobowych*, „Monitor Prawniczy" 2018, nr 17.

Suwaj R., *Wiek uczestników postępowania administracyjnego a skuteczność podejmowanych przez nich czynności prawnych*, „Białostockie Studia Prawnicze" 2010, nr 7.

Suwaj R., *Zasady nakładania administracyjnych kar pieniężnych*, Warszawa 2021.

Syska K., *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań*, „Monitor Prawniczy" dodatek: *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, Sibiga G. (red.), 2016, nr 20.

Syska K., *Prawo dostępu do danych a prawo przenoszalności – porównanie celu regulacji, zakresu i przesłanek stosowania*, „Prawo Mediów Elektronicznych" 2017, nr 3.

Szanciło T. (red.), *Kodeks postępowania cywilnego. Komentarz. Komentarz. Art. 1–458[16]. Tom I. Wyd. 2*, Warszawa 2023, Legalis.

Szewc T., *Zgoda na przetwarzanie danych osobowych*, „Państwo i Prawo" 2008, nr 2.

Szewczyk E., Szewczyk M., *Strona w postępowaniu administracyjnym*, [w:], Łaszczyca G., Matan A. (red.), *System Prawa Administracyjnego Procesowego*: Chróścielewski W. (red.), tom II część 1. *Zakres przedmiotowy i podmiotowy postępowania administracyjnego ogólnego*, Warszawa 2018.

Szponar-Seroka J., *Wielojęzyczność jako wyzwanie w procesie stanowienia i wykładni prawa Unii Europejskiej*, „Studenckie Zeszyty Naukowe" 2017, nr 33.

Szpor G., *Kierunki zmian w ustawodawstwie dotyczącym ochrony danych osobowych*, [w:] Mednis A. (red.), *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, Warszawa 2013.

Szpor G., *Pojęcie informacji a zakres ochrony danych osobowych*, [w:] Fajgielski P. (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008.

Szuba M., *Definicja dziecka na gruncie art. 304[5] kodeksu pracy – na tle porównawczym*, „Roczniki Administracji i Prawa" 2018, nr XVIII.

Szustakiewicz P., *Ograniczenia dostępu do informacji publicznej w świetle najnowszego orzecznictwa sądów administracyjnych*, [w:] Mednis A. (red.), *Prywatność a jawność. Bilans 25-lecia i perspektywy na przyszłość*, Warszawa 2016, Legalis.

Szymielewicz K., *Reforma europejskiego prawa o ochronie danych osobowych z perspektywy praw obywateli – więcej czy mniej ochrony?*, [w:] Sibiga G. (red.), *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, Warszawa 2016.

Szymielewicz K., Walkowiak A., *Autonomia informacyjna w kontekście usług internetowych: o znaczeniu zgody na przetwarzanie danych i ryzykach związanych z profilowaniem*, [w:] Sibiga G. (red.), *Aktualne problemy prawnej ochrony danych osobowych 2014*, Warszawa 2014, Legalis.

Śledziewska K., Włoch R., G*ospodarka cyfrowa. Jak nowe technologie zmieniają świat,* Warszawa 2020.

Tapscott D., *Gospodarka cyfrowa. Nadzieje i niepokoje Ery Świadomości Systemowej*, Warszawa 1998.

Topyła M., *Zmiana ustawy o prawach konsumenta w związku z wejściem w życie tzw. ustawy dostosowującej RODO a obowiązek informacyjny w wykonaniu mikroprzedsiębiorcy*, [w;} „Monitor Prawniczy" dodatek: *Polskie przepisy o ochronie danych osobowych. Aktualne problemy prawnej ochrony danych osobowych 2019*, Sibiga G. (red.), 2019, nr 22.

van der Hof S., Lievens E., *The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR*, referat wygłoszony 17.10.2017 r. na konferencji *Children and Digital Rights: Regulating Freedoms and Safeguards* w Londynie.

van der Hof, S. *I Agree. . . Or Do I? — A Rights-Based Analysis of the Law On Children's Consent in the Digital World*, „Wisconsin International Law Journal" 2017, vol. 34.

Varotto S., *The European General Data Protection Regulation and its potential impact on businesses: some critical notes on the strengthened regime of accountability and the new sanctions*, „Communications Law: Journal of Computer, Media & Telecommunications" 2015, vol. 20, nr 3.

Volosevici D., *Child protection under GDPR*, „Jus et Civitas" 2019, nr 2.

Warren S. D., Brandeis L. D., *The right to privacy,* "Harvard Law Review" 1890, vol. IV.

Wątor W., *Prawo do bycia zapomnianym a swoboda wypowiedzi – glosa do wyroku Europejskiego Trybunału Praw Człowieka z 28.06.2018 r., 60798/10 i 65599/10, M.L. i W.W. przeciwko Niemcom,* „Europejski Przegląd Sądowy" 2019, nr 5.

Wiewiórowski W. R., *Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy" 2017, nr 5.

Wikariak S., *Dane dzieci pod ochroną aż do 16 lat*, „Dziennik Gazeta Prawna" 28.03.2018 r.

Wiśniewski L., *Geneza Konwencji o Prawach Dziecka i stosunek jej norm do innych aktów prawa międzynarodowego*, Smyczyński T. (red.), *Konwencja o prawach dziecka. Analiza i wykładnia*, Poznań 1999.

Wong J., Henderson T., *The right to data portability in practice: exploring the implications of the technologically neutral GDPR*, „International Data Privacy Law" 2019, nr 3.

Wróbel A. (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, wyd. 2, Warszawa 2020.

Wróbel I., *Pojęcie usługi społeczeństwa informacyjnego w prawie wspólnotowym,* „e-Biuletyn Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej" 2017, nr 4.

Wróbel M., *Prawo do „bycia zapomnianym" – glosa – C-131/12*, „Monitor Prawniczy" 2017, nr 2.

Wyka T., *Granice pozyskiwania danych osobowych dotyczących zdrowia pracownika*, [w:] Nerka A., Wyka T. (red.), *Granice ochrony danych osobowych w stosunkach pracy*, Warszawa 2009.

Yordanov A., *Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation,* „European Data Protection Law Review" 2017, nr 4.

Zadrożny M., *Warunki nakładania przez GIODO administracyjnych kar pieniężnych*, [w:] Dmochowska A., Zadrożny M., *Unijna reforma ochrony danych osobowych - analiza zmian*, Warszawa 2016, Legalis.

Zalewska-Bochenko A., *Portale społecznościowe jako element społeczeństwa informacyjnego*, „Studia Informatica Pomerania" 2016, nr 2.

Załucki M. (red.), *Kodeks cywilny. Komentarz*, wyd. 2, Warszawa 2019, Legalis.

Załucki M., *Śmierć a dane w systemach teleinformatycznych – przyczynek do dyskusji*, [w:] Flaga-Gieruszyńska K., Gołaczyński J., Szostek D. (red.), *Media elektroniczne. Współczesne problemy prawne*, Warszawa 2016, Legalis.

Zimna M., *Odpowiedzialność karna za naruszenie ochrony danych osobowych*, „Prokuratura i Prawo" 2020, nr 1.

Zimny W., *Praktyczne skutki nowelizacji ustawy o ochronie danych osobowych z dnia 25 sierpnia 2001 r.*, „Ochrona danych osobowych. Biuletyn ABI" 2001, nr 21.

Żeromski B., *Weryfikacja tożsamości na odległość*, [w:] „Monitor Prawniczy" dodatek: *Wpływ technologii i technik informatycznych na ochronę danych osobowych. Aktualne problemy prawnej ochrony danych osobowych 2022*, Sibiga G. (red.), 2022, nr 21.

Żyrek S., *Prawo do bycia usuniętym z listy wyników wyszukiwarki internetowej – wprowadzenie i wyrok Trybunału Sprawiedliwości z 13.05.2014 r., C-131/12, Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi,* „Europejski Przegląd Sądowy" 2019, nr 6.

4. Orzecznictwo polskich sądów i trybunałów

4.1 Orzeczenia Trybunału Konstytucyjnego

Wyrok TK z dnia 19 maja 1998 r., sygn. U 5/97, Dz.U. z 1998 r. Nr 67 poz. 444.

Wyrok TK z dnia 19 lutego 2002 r., sygn. U 3/01.

Wyrok TK z dnia 12 listopada 2002 r., sygn. SK 40/01.

Wyrok TK z dnia 28 kwietnia 2003 r., sygn. K 18/02, Dz.U. 2003 nr 83, poz. 772.

4.2 Orzeczenia Sądu Najwyższego

Wyrok SN z dnia 18 stycznia 1984 r., sygn. I CR 400/83.

Wyrok SN z dnia 4 kwietnia 1966 r., sygn. II PR 139/66.

Wyrok SN z dnia 26 września 1996 r., sygn. III ARN 40/96.

4.3 Orzeczenia Naczelnego Sądu Administracyjnego

Wyrok NSA z dnia 4 lipca 2004 r., sygn. II OSK 941/05.

Wyrok NSA z dnia 13 lipca 2004 r., sygn. OSK 507/04.

Wyrok NSA z dnia 6 września 2011 r., sygn. I OSK 1476/10.

Wyrok NSA z dnia 25 sierpnia 2020 r., sygn. I OSK 3325/19.

Postanowienie NSA z dnia 21 marca 2021 r., sygn. I OSK 2500/16.

Postanowienie NSA z dnia 11 października 2016 r., sygn. II OSK 2238/16.

4.4 Orzeczenia wojewódzkich sądów administracyjnych

Wyrok WSA w Gliwicach z dnia 9 maja 1997 r., sygn. IV SA/Gl 284/06.

Wyrok WSA w Białymstoku z dnia 27 października 2005 r., sygn. II SA/Bk 503/05.

Wyrok WSA we Wrocławiu z dnia 08 lutego 2006 r., sygn. IV SA/Wr 798/04.

Wyrok WSA w Łodzi z dnia 12 lutego 2019 r., sygn. II SAB/Łd 181/18.

Wyrok WSA w Warszawie z dnia 11 grudnia 2019 r., sygn. II SA/Wa 1030/19.

Wyrok WSA w Warszawie z dnia 26 sierpnia 2020 r., sygn. II SA/Wa 2826/19.

Postanowienie WSA w Szczecinie z dnia 28 czerwca 2016 r., sygn. II SAB/Sz 64/16.

Postanowienie WSA w Warszawie z dnia 21 marca 2017 r., sygn. II SAB/Wa 155/16.

4.5 Orzeczenia sądów powszechnych

Wyrok SA w Warszawie z dnia 13 grudnia 2018 r., sygn.VI ACa 744/18.

Wyrok SO w Warszawie z dnia 7 lutego 2023 r., sygn. III C 280/22.

5. Orzeczenia Trybunału Sprawiedliwości Unii Europejskiej

Wyrok TSUE z dnia 04 grudnia 1974 r. w sprawie 41/74, Yvonne van Duyn przeciwko Home Office.

Wyrok TSUE z dnia 19 stycznia 1982 r. w sprawie 8/81, Ursula Becker przeciwko Finanzamt Münster-Innenstadt.

Wyrok TSUE z dnia 27 września 1988 r. w sprawie C-263/86, Państwo belgijskie przeciwko René Humbel i Marie-Thérèse Edel.

Wyrok TSUE z dnia 06 listopada 2003 r. w sprawie C-101/01, Göta hovrätt – Szwecja przeciwko Bodil Lindqvist.

Wyrok TSUE z dnia 13 maja 2014 r. w sprawie C-131/12, Google Spain SL, Google Inc. Przeciwko Agencia Española de Protección de Datos (AEPD), M. C. Gonzálezowi.

Wyrok TSUE z dnia 11 września 2014 r. w sprawie C-291/13, Sotiris Papasavvas przeciwko O Fileleftheros Dimosia Etaireia Ltd i in.

Wyrok TSUE z dnia 1 października 2015 r. w sprawie C-201/14, Smaranda Bara i in. przeciwko Președintele Casei Naționale de Asigurări de Sănătate i inni.

Wyrok TSUE z dnia 15 września 2016 r. w sprawie C-484/14, Tobias Mc Fadden przeciwko Sony Music Entertainment Germany GmbH.

Wyrok TSUE z dnia 19 października 2016 r. w sprawie C-582/14, Patrick Breyer przeciwko Bundesrepublik Deutschland.

Wyrok TSUE z dnia 20 grudnia 2017 r. w sprawie C-434/16, Peter Nowak przeciwko Data Protection Commissioner.

Wyrok TSUE z dnia 10 kwietnia 2018 r. w sprawie C-320/16, Uber France SAS przy udziale Nabila Bensalema.

Wyrok TSUE z dnia 05 czerwca 2018 r. w sprawie C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH.

Wyrok TSUE z dnia 05 czerwca 2019 r. w sprawie C-142/18, Skype Communications Sàrl przeciwko Institut belge des services postaux et des télécommunications (IBPT).

Wyrok TSUE z dnia 29 lipca 2019 r. w sprawie C-40/17, Fashion ID GmbH & Co.KG przeciwko Verbraucherzentrale NRW eV.

Wyrok TSUE z dnia 24 września 2019 r. w sprawie C-507/17, Google LLC, następca prawny Google Inc., przeciwko Commission nationale de l'informatique et des libertés (CNIL).

Wyrok TSUE z dnia 19 grudnia 2019 r. w sprawie C-390/18, X przy udziale YA, Airbnb Ireland UC, Hôtelière Turenne SAS, Association pour un hébergement et un tourisme professionnels (AHTOP), Valhotel.

Wyrok TSUE z dnia 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commissioner przeciwko Facebook Ireland Ltd, Maximillian Schrems.

Wyrok TSUE z dnia 11 listopada 2020 r. w sprawie C-61/19, Orange Romania SA przeciwko Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

Wyrok TSUE z dnia 03 grudnia 2020 r. w sprawie C-62/19, Star Taxi App SRL przeciwko Unitatea Administrativ Teritorială Municipiul Bucureşti prin Primar General i Consiliul General al Municipiului Bucureşti.

Wyrok TSUE z dnia 04 maja 2023 r. w sprawie C-300/21, UI przeciwko Österreichische Post AG.

6. Orzeczenia Europejskiego Trybunału Praw Człowieka

Wyrok ETPCZ z dnia 16 lutego 2000 r., 27798/95, Amann v. Szwajcaria.

Wyrok ETPCZ z dnia 02 września 2010 r., 35623/05, Uzun v. Niemcy.

Wyrok ETPCZ z dnia 3 kwietnia 2007 r., 62617/00, Copland v. Wielka Brytania.

7. Decyzje Prezesa UODO

Decyzja GIODO z dnia 12 września 2017 r., DIS/DEC-1110/17/68986.

Decyzja Prezesa UODO z dnia 15 marca 2019 r., ZSPR.421.3.2018.

Decyzja Prezesa UODO z dnia 22 marca 2019 r. ZSZZS.440.660.2018.

Decyzja Prezesa UODO z dnia 3 kwietnia 2019 r., ZSPU.421.8.2018.

Decyzja Prezesa UODO z dnia 12 kwietnia 2019 r., ZSZZS.440.672.2018.

Decyzja Prezesa UODO z dnia 16 października 2019 r., ZSPR.421.7.2019.

Decyzja Prezesa UODO z dnia 18 października 2019 r., ZSPU.421.3.2019.

Decyzja Prezesa UODO z dnia 18 lutego 2020 r., ZSZZS.440.768.2018.

Decyzja Prezesa UODO z dnia 21 sierpnia 2020 r., ZSOŚS.421.25.2019.

Decyzja Prezesa UODO z dnia 12 listopada 2020 r., DKN.5101.25.2020.

Decyzja Prezesa UODO z dnia 9 grudnia 2020 r., DKN.5131.5.2020.

Decyzja Prezesa UODO z dnia 9 grudnia 2021 r., DKN.5130.2559.2020.

Decyzja Prezesa UODO z dnia 6 lipca 2022 r., DKN.5131.34.2021.

Decyzja Prezesa UODO z dnia 30 listopada 2022 r., DKN.5112.5.2021.

Decyzja Prezesa UODO, opublikowana na stronie internetowej dnia 7 lutego 2023 r. (brak informacji o dacie wydania), DKN.5131.31.2021.

Decyzja Prezesa UODO opublikowana na stronie internetowej dnia 1 marca 2023 r. (brak informacji o dacie wydania), DKN.5131.49.2021.

Decyzja Prezesa UODO z 31 marca 2023 r., DKN.5131.8.2021.

8. Rozstrzygnięcia zapadłe w wybranych państwach członkowskich Unii Europejskiej

Wyrok Sądu Rejonowego Gelderland z dnia 13 maja 2020 r. w sprawie nr C/05/368427, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBGEL:2020:2521&showbutton=true&keyword=AVG.

Autorité de protection des données, decyzja z dnia 16 czerwca 2020 r., https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Beslissing_GK_31-2020_NL.pdf.

Autoriteit Persoonsgegevens, decyzja z dnia 9 kwietnia 2021 r., https://www.autoriteitpersoonsgegevens.nl/en/news/tiktok-fined-violating-children's-privacy.

Data Protection Commission, decyzja z dnia 2 września 2022 r. w sprawie IN-20-7-4, https://edpb.europa.eu/system/files/2022-09/in-20-7-4_final_decision_-_redacted.pdf.

9. Dokumenty Grupy Roboczej Art. 29 oraz Europejskiej Rady Ochrony Danych

Grupa Robocza Art. 29, *Working Document on Genetic Data*, przyjęty 17.03.2004, WP 91, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf.

Grupa Robocza Art. 29, *Opinia nr 4/2007 w sprawie pojęcia danych osobowych*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pl.pdf.

Grupa Robocza Art. 29, *Opinia w sprawie ochrony danych osobowych dzieci (Ogólne wytyczne i szczególny przypadek szkół)*, przyjęta dnia 11 lutego 2009 r., https://archiwum.giodo.gov.pl/pl/1520022/2991.

Grupa Robocza Art. 29, *Opinia nr 5/2009 w sprawie portali społecznościowych*, przyjęta w dniu 12 czerwca 2009 r., https://archiwum.giodo.gov.pl/pl/1520022/2988.

Grupa Robocza Art. 29, *Opinia 3/2010 w sprawie zasady rozliczalności*, przyjęta w dniu 13 lipca 2010 r., https://archiwum.giodo.gov.pl/pl/1520057/3732.

Grupa Robocza Art. 29, *Opinia w sprawie systemów rozpoznawania twarzy w usługach online i usługach komórkowych*, przyjęta w dniu 22 marca 2012 r., WP 192, https://archiwum.giodo.gov.pl/pl/1520111/4620.

Grupa Robocza Art. 29, *Opinia nr 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych*, przyjęta w dniu 27 kwietnia 2012 r., WP193, https://archiwum.giodo.gov.pl/pl/file/5337.

Grupa Robocza Art. 29, *Opinia nr 04/2012 w sprawie wyłączenia zapisywania plików cookie spod zasady pozyskiwania zgody*, przyjęta w dniu 7 czerwca 2012 r., https://archiwum.giodo.gov.pl/pl/1520111/4722.

Grupa Robocza Art. 29, *Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE*, przyjęta w dniu 9 kwietnia 2014 r., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_pl.pdf.

Grupa Robocza Art. 29, *Wytyczne dotyczące inspektorów ochrony danych („DPO")* przyjęte w dniu 13 grudnia 2016 r., WP243, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-officer_pl (dostęp:15.03.2023).

Grupa Robocza Art. 29, *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679*, przyjęte w dniu 4 kwietnia 2017 r., WP 248 rev.01.

Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia danych*, przyjęte w dniu 5 kwietnia 2017 r., https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

Grupa Robocza Art. 29, *Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679*, przyjęte w dniu 3 października 2017 r., https://archiwum.giodo.gov.pl/pl/1520344/10432.

Grupa Robocza Art. 29, *Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679*, przyjęte w dniu 3 października 2017 r., WP250, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-personal-data-breach-notification-under_pl.

Grupa Robocza Art. 29, *Guidelines on Transparency under Regulation 2016/679,* przyjęte w dniu 29 listopada 2017 r., https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679*, przyjęte w dniu 29 listopada 2017 r., www.uodo.gov.pl/pl/3/1343.

Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE*, przyjęte w dniu 6 lutego 2018 r., https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

EROD, *Wytyczne 3/2018 w sprawie terytorialnego zakresu stosowania RODO (art. 3)*, wersja 2.0 przyjęta 12.11.2019 r., https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_pl.pdf.

EROD, *Opinia nr 17/2018 w sprawie projektu wykazu sporządzonego przez właściwy polski organ nadzorczy dotyczącego rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych (art. 35 ust. 4 RODO)*, przyjęta 25 września 2018 r., https://edpb.europa.eu/sites/default/files/files/file1/2018-09-25-opinion_2018_art._64_pl_sas_dpia_list_pl.pdf.

EROD, *Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą*, Wersja 2.0, przyjęte w dniu 8 października 2019 r., https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.

EROD, *Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo*, wersja 2.0, przyjęte w dniu 29 stycznia 2020 r., https://edpb.europa.eu/our-work-tools/our-documents/pokyny/guidelines-32019-processing-personal-data-through-video-devices_en.

EROD, *Wytyczne 4/2019 dotyczące artykułu 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych*, przyjęte w dniu 20 października 2020 r., https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_pl.pdf.

EROD, *Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB*, przyjęte w dniu 19 listopada 2020 r., https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201119_eprivacy_regulation_en.pdf.

EROD, *Opinia 5/2019 w sprawie wzajemnej zależności między dyrektywą o prywatności i łączności elektronicznej a RODO, w szczególności w zakresie właściwości, zadań i uprawnień organów ochrony danych*, przyjęta w dniu 12 marca 2019 r., https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_pl.pdf.

EROD, *Wytyczne 5/2019 w sprawie kryteriów dotyczących prawa do bycia zapomnianym w sprawach dotyczących wyszukiwarek internetowych na podstawie RODO*, przyjęte w dniu 7 lipca 2020 r. (wersja 2.0), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_pl.

EROD, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications - version for public* consultation, przyjęte w dniu 28 stycznia 2020 r., https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

EROD, *Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych*, wersja 2.0, przyjęta w dniu 18 czerwca 2021 r., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_pl.

EROD, *Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679*, przyjęte w dniu 4 maja 2020 r., https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

EROD, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, wersja 1.0, przyjęta w dniu 2 września 2020 r., https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

EROD, *Guidelines 8/2020 on the targeting of social media users*, wersja do publicznych konsultacji, przyjęta w dniu 2 września 2020 r., https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf (dostęp: 23.09.2020).

EROD, *Wytyczne 01/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych*, przyjęte w dniu 14 grudnia 2021 r., wersja 2.0, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_pl.

EROD, *Wytyczne 04/2021 dotyczące kodeksów postępowania jako narzędzi do przekazywania danych*, wersja 2.0, przyjęte w dniu 22 lutego 2022 r., https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_pl.

EROD, *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, wersja 2.0, przyjęta w dniu 14 lutego 2023, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_pl.

EROD, *Guidelines 01/2022 on data subject rights - Right of access*, wersja 2.0, przyjęta w dniu 28 marca 2023 r.,
https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf.

EROD, *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them*, przyjęte w dniu 14 lutego 2023 r., https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_pl.

EROD, *Guidelines 04/2022 on the calculation of administrative fines under the GDPR*, wersja 2.0, przyjęte w dniu 24 maja 2023 r., https://edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf.

EROD, *Wytyczne 07/2022 dotyczące certyfikacji jako narzędzia do przekazywania danych*, wersja 2.0, przyjęte w dniu 14 lutego 2023 r., https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_pl.

EROD, *Template Complaint Form*, przyjęty w dniu 20 czerwca 2023 r., https://edpb.europa.eu/system/files/2023-06/edpb_20230620_templatecomplaintform_0.pdf.

10. Dokumenty Rady Europy

Komitet Ministrów, *Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997)*, http://hrlibrary.umn.edu/instree/coerecr97-5.html.

Komitet Ministrów, *Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment*, 04.07.2018, https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html.

Komitet Ministrów, *Rekomendacja CM/Rec (2010) 13 Komitetu Ministrów państw członkowskich w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili*, 23.11.2010 r., https://uodo.gov.pl/pl/file/1425.

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 10.10.2018 r., https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016808ac918.

Strategia Rady Europy na rzecz praw dziecka (2016-2021), https://rm.coe.int/strategia-rady-europy-na-rzecz-praw-dziecka-2016-2021-/1680931c80.

11. Dokumenty Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)

ENISA, *Guidelines for SMEs on the security of personal data processing*, https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing.

ENISA, *Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymization*, https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions.

ENISA, *Privacy and Data Protection by Design – from policy to engineering*, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

ENISA, *Privacy and data protection in mobile applications. A study on the app development ecosystem and the technical implementation of GDPR*, https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications.

ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches*, https://www.enisa.europa.eu/publications/dbn-severity.

ENISA, *Privacy, Accountability and Trust – Challenges and Opportunities*, https://www.enisa.europa.eu/publications/pat-study.

12. Wytyczne i materiały informacyjne Prezesa UODO (wcześniej GIODO)

GIODO, *Informacja Generalnego Inspektora Ochrony Danych Osobowych o zagrożeniach płynących z upowszechnienia danych biometrycznych w kontaktach obywateli z instytucjami publicznymi i prywatnymi*, przyjęta w czerwcu 2017 r., https://archiwum.giodo.gov.pl/pl/file/12478.

GIODO, *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku część 1*, https://archiwum.giodo.gov.pl/pl/1520282/10294.

GIODO, *Jak stosować podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku część 2*, https://archiwum.giodo.gov.pl/pl/1520282/10294.

GIODO, poradnik *Czy jesteś gotowy na RODO?,* https://www.giodo.gov.pl/pl/1520281/10255.

UODO, *Obowiązki administratorów związane z naruszeniami ochrony danych osobowych*, https://archiwum.uodo.gov.pl/pl/134/1029.

UODO, *Cele i Etapy Programu Twoje dane – Twoja sprawa*, https://uodo.gov.pl/pl/21/30.

UODO, *Dzieci mają prawo być informowane o naruszeniach, które ich dotyczą,* https://uodo.gov.pl/pl/138/1287.

UODO, *Składanie skargi w formie tradycyjnej, w tym do protokołu w siedzibie Prezesa Urzędu*, https://uodo.gov.pl/pl/489/2247.

UODO, *Standardowe klauzule ochrony danych*, https://uodo.gov.pl/pl/535/2506.

UODO, *Twoje dane – Twoja sprawa*, https://uodo.gov.pl/512.

UODO, *Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO*, https://uodo.gov.pl/data/filemanager_pl/708.pdf.

UODO, *Prezes UODO nałożyła pierwszą karę pieniężną*, https://uodo.gov.pl/pl/138/786.

UODO, *PESEL nie musi być publicznie ujawniany*, https://uodo.gov.pl/pl/138/1098.

UODO, *Co z obowiązkiem informacyjnym wobec członków zarządu osób prawnych?*, https://uodo.gov.pl/pl/225/1577.

Sprawozdania z działalności Prezesa UODO, https://uodo.gov.pl/pl/487/2279.

13. Wytyczne i materiały informacyjne organów nadzorczych z wybranych państw członkowskich Unii Europejskiej

Agencia Española de Protección de Datos, *A Guide to Privacy by Design*, https://www.aepd.es/es/documento/guia-privacidad-desde-diseno_en.pdf.

Autoritat Catalana de Proteccio de Dades, *Privacy by design and privacy by default. A guide for developers*,
https://apdcat.gencat.cat/web/.content/03-documentacio/documents/guiaDesenvolupadors/GUIA-PDDD_EN.pdf.

Commission Nationale de l'Informatique et des Libertés, *GDPR developer's guide*, https://www.cnil.fr/en/gdpr-developers-guide.

Commission nationale de l'informatique et des libertés, *Digital rights of children*, https://www.cnil.fr/en/digital-rights-children.

Data Protection Commission, *Are there any limits on my child's data protection rights?*, https://www.dataprotection.ie/sites/default/files/uploads/2023-04/DPC_ChildrensData_Limits.pdf.

Data Protection Commission, *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*, https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf.

Data Protection Commission, *Children, Parents and Data Protection: Can I make a complaint on behalf of my child?*, https://www.dataprotection.ie/sites/default/files/uploads/2022-06/Guidance%20Children%20Parents%20and%20Data%20Protection-%20Can%20I%20make%20a%20complaint%20on%20behalf%20of%20my%20child.pdf.

Data Protection Commission, *Children's data and parental consent*, https://www.dataprotection.ie/sites/default/files/uploads/2023-04/DPC_ChildrensData_ParentalConsent.pdf.

Data Protection Commission, *My child's data protection rights – the basics,* https://www.dataprotection.ie/sites/default/files/uploads/2023-04/DPC_ChildrensRights_TheBasics.pdf.

Data Protection Commission, *Protecting my child's data*, https://www.dataprotection.ie/sites/default/files/uploads/2023-04/DPC_ChildrensData_ProtectingThem.pdf.

Datatilysnet, *Software development with Data Protection by Design and by Default*, https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true.

Information Commissioner's Office, *Age appropriate design: a code of practice for online service,* https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf.

Information Commissioner's Office, *What rights do children have?*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-rights-do-children-have/#a5.

Agencia Española de Protección de Datos, EIOD, *14 misunderstandings with regard to biometric identification and authentication*, https://edps.europa.eu/data-protection/our-work/publications/papers/14-misunderstandings-regard-biometric-identification_en.

14. Inne źródła

A. Cavoukian, *Privacy by Design. The 7 Foundational Principles*, https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

BBC News 21.05.2020, *Grandmother ordered to delete Facebook photos under GDPR*, https://www.bbc.com/news/technology-52758787.

BBC, *Shutter falls on life-logging camera start-up Narrative*, https://www.bbc.com/news/technology-37497900.
Berkman Klein Center, *Fairness and AI*, https://medium.com/berkman-klein-center/fairness-and-ai-c5596faddd20.

Biuro Rzecznika Praw Obywatelskich, *Inwigilacja i uprawnienia polskich służb specjalnych w ETPC. Rzecznik przedstawia swą opinię*, 30.07.2020, https://www.rpo.gov.pl/pl/content/etpc-zbada-uprawnienia-polskich-sluzb-specjalnych-opinia-rpo.

Cambridge Dictionary, https://dictionary.cambridge.org.

Centre for Information Policy Leadership, *White Paper on GDPR Implementation In Respect of Children's Data and Consent*, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf (dostęp: 07.02.2021).

CERT Polska – Naukowa i Akademicka Sieć Komputerowa, *Ważne zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych*, https://cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf.

Consumenten bond, wyniki testów bezpieczeństwa smartfonów wyposażonych w funkcję rozpoznawania twarzy,

https://www.consumentenbond.nl/veilig-internetten/gezichtsherkenning-te-hacken.

Encyklopedia PWN, https://encyklopedia.pwn.pl.

Europejski Urząd ds. Pracy, *Analysis of shortage and surplus occupations 2022*, https://www.ela.europa.eu/sites/default/files/2023-03/eures-labour-shortages-report-2022.pdf.

Fundacja Panoptykon, *Pogrzebana szansa na ochronę danych w służbach*, 10.05.2018, https://panoptykon.org/wiadomosc/pogrzebana-szansa-na-ochrone-danych-w-sluzbach.

Główny Urząd Statystyczny, *Wpływ epidemii COVID-19 na wybrane elementy rynku pracy w Polsce w II kwartale 2020 r.*, https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5820/4/2/1/wplyw_epidemii_covid-19_na_wybrane_elementy_rynku_pracy_w_polsce_w_drugim_kwartale_2020.pdf.

H. Brignull, M. Leiser, C. Santos, K. Doshi, *Deceptive Pattern*, https://www.deceptive.design.

Internet Matters, *Aplikacje poprawiające samopoczucie dla dzieci*, https://www.internetmatters.org/pl/resources/wellbeing-apps-guide-for-kids.

Internetowy słownik języka polskiego PWN, https://sjp.pwn.pl.

KE, *Czy dozwolone jest gromadzenie danych dotyczących dzieci?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_pl.

KE, *Report on the implementation of specific provisions of Regulation (EU) 2016/679. Final report (Authors: TIPIK Legal)*, https://ec.europa.eu/info/sites/info/files/study_implementation_gdpr.pdf.

Komunikat z dnia 5 maja 2015 r. Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów *Strategia jednolitego rynku cyfrowego dla Europy*, COM(2015) 192 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52015DC0192&from=EN.

L. Smith, *Woman faces £9,000 fine if she posts pictures of her son on Facebook*, „Independent" 12.01.2018, https://www.independent.co.uk/news/world/europe/facebook-fines-woman-son-photos-post-social-media-court-italy-rome-a8155361.html.

Ministerstwo Cyfryzacji, *Czym jest spoofing? Jak go rozpoznać i nie dać się nabrać?*, https://www.gov.pl/web/cyfryzacja/czym-jest-spoofing--jak-go-rozpoznac-i-nie-dac-sie-nabrac.

Ministerstwo Spraw Wewnętrznych i Administracji, *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013*, przyjęta w grudniu 2008 r., http://www.umwd.dolnyslask.pl/fileadmin/user_upload/spoleczenstwo_informacyjne/dokumenty/Strategia_Rozwoju_Spoleczenstwa_Informacyjnego_w_Polsce.pdf.

Puls Biznesu, *Lifelog, czyli zarejestruj całe swoje życie*, https://www.pb.pl/lifelog-czyli-zarejestruj-cale-swoje-zycie-715844.

Reuters, *Germany bans talking doll Cayla, citing security risk,* https://www.reuters.com/article/us-germany-cyber-dolls-idUSKBN15W20Q.

Strona internetowa rządu Wielkiej Brytanii, *Explanatory memorandum to the Age Appropriate Design Code 2020*, https://www.gov.uk/government/publications/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020#extent-and-territorial-application.

UN Convention on the Rights of the Child in Child Friendly Language, https://sites.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf.

Wielki Słownik Języka Polskiego, https://wsjp.pl.

SUMMARY

The subject of the dissertation is the analysis of the data protection legislation from the perspective of the issue of processing of children's personal data in a particular context - the provision of information society services. The need to extend special protection to children who are less aware of potential risks was accentuated during the legislative stage of the work on the EU reform of personal data protection, which resulted in the adoption of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46/EC (General Data Protection Regulation), hereinafter "Regulation 2016/679". The thesis of the dissertation is that the regulation of the processing of a child's personal data in Regulation 2016/679 is fragmentary, too general and raises numerous interpretative doubts and, as a result, the data protection reform does not fully realize one of its objectives, which is to strengthen the protection of the child's personal data in connection with the provision of information society services. The dissertation consists of an introduction, five substantive chapters and a conclusion. The first chapter is devoted to introductory issues. It presents the genesis of legal regulations to protect the rights of individuals in connection with the processing of personal data concerning them and analyzes key concepts. The second chapter concerns the guiding principles of personal data processing: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. Chapter three relates to the rights that a child has under Articles 15-22 of Regulation 2016/679 and how to exercise them. The fourth chapter is devoted to obligations related to the processing of the child's personal data. The fifth chapter focuseson the liability for violations related to the processing of the child's personal data in connection with the provision of information society services. As a result of the analysis carried out in the dissertation, the thesis of the dissertation has been proven. The result of the considerations is the formulation of *de lege ferenda* postulates regarding the processing of a child's personal data on the basis of consent, the exercise of the child's rights under Regulation 2016/679, the implementation of the controller's obligations relating to the design and conduct of projects involving the processing of personal data of a child user of information society services, data protection impact assessments, notification of personal data breach involving the personal data of a child user of information society services, the amount of administrative fines.