

osobowych w Unii nie jest ograniczany ani zakazany z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

Art. 2. [Materialny zakres stosowania]

1. Niniejsze rozporządzenie 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.

2. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:

- a) w ramach działalności nieobjętej zakresem prawa Unii;
- b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;
- c) przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;
- d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

3. Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do zasad i przepisów niniejszego rozporządzenia zgodnie z art. 98.

4. Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy 2000/31/WE, w szczególności dla zasad odpowiedzialności usługodawców będących pośrednikami, o których to zasadach mowa w art. 12–15 tej dyrektywy.

Spis treści

	Nb
1. Znaczenie i charakter normy ustanawiającej stosowanie RODO . . .	1
2. Zakres podmiotowy	2
3. Zakres przedmiotowy	3
4. Przetwarzanie w sposób zautomatyzowany przy braku utrwalenia danych	4
5. Ograniczenie stosowania z uwagi na przedmiot działań administratora	5
6. Cele osobiste i domowe a przetwarzanie danych bez związku z działalnością zawodową lub handlową	6
7. Stosowanie RODO przez instytucje, organy i jednostki organizacyjne UE	7
8. RODO a stosowanie dyrektywy 2000/31/WE (o handlu elektronicznym)	8

1. **Znaczenie i charakter normy ustanawiającej stosowanie RODO.** Mając 1 na uwadze podstawowe założenia RODO, jego neutralność technologiczną, organizacyjną, długą perspektywę czasową stosowania, a także założoną swobodę działania administratora oraz szerokie ujęcie właściwości terytorialnej, określenie materialnego zakresu stosowania tego aktu ma kluczowe znaczenie dla ostatecznego wskazania zakresu ochrony praw jednostki będącej obywatelem UE lub znajdującej się pod władztwem któregoś z krajów członkowskich lub należącego do Europejskiego Obszaru Gospodarczego.

Wskazanie przedmiotowego zakresu stosowania RODO, określonego od strony pozytywnej, nie daje jednak pełnego obrazu działania tej regulacji. Zawiera ono wprawdzie niezwykle ważne, z polskiej perspektywy nowe, rozwiązania wymagające odmiennego podejścia do przetwarzania danych, jednak ujęcie przedmiotowego zakresu stosowania RODO niesie za sobą pewne ograniczenia wpisane immanentnie w przyjętą formułę. Należy również podkreślić, że komentowany przepis posłużył do ustanowienia ograniczeń materialnych stanowiących istotną część wyłączeń obejmujących stosowanie RODO, które będą dotyczyć obywateli UE (zarówno tych występujących w roli administratorów, jak i osób, których dane dotyczą).

Należy podkreślić, że na poziomie rozważań o materialnym obowiązywaniu RODO nie ma znaczenia rodzaj przetwarzanych danych osobowych. Zarówno dane zwykłe, jak i szczególnych kategorii, w kontekście przedmiotowego zasięgu regulacji, podlegają ochronie na tych samych warunkach.

Chcąc właściwie odczytywać zakres przedmiotowy RODO, należy jednak, poza tekstem ujętym w art. 2, mieć na uwadze odnoszące się doń motywy 15–21 oraz kwestie dopuszczalności odrębnych rozwiązań krajowych ustanowionych na podstawie art. 85–91 i wynikające z art. 94–96 relacje z obowiązującymi wcześniej regulacjami (zwłaszcza brak dodatkowych obowiązków w związku ze świadczeniem ogólnodostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii w sprawach, w których podmioty te podlegają szczegółowym obowiązkom mającym ten sam cel określony w dyrektywie 2002/58/WE).

Wejście w życie OchrDanychU 25.5.2018 r. dookreśla stosowanie RODO i samej ustawy (art. 6 OchrDanychU). Przepis ten zakłada brak możliwości stosowania tych aktów w dwóch odrębnych sytuacjach. Pierwsza z nich dotyczy przetwarzania danych osobowych przez część jednostek sektora finansów publicznych (organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały, agencje wykonawcze, instytucje gospodarki budżetowej, inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego) w zakresie, w jakim przetwarzanie to jest konieczne do realizacji zadań mających na celu zapewnienie bezpieczeństwa narodowego, jeżeli przepisy szczególne przewidują niezbędne środki ochrony praw i wolności osoby, której dane dotyczą – co wydaje się mieścić w zakresie art. 2 ust. 2 lit. a RODO, o czym świadczy zwłaszcza treść motywu 16 wprost powołującego się na działalność dotyczącą bezpieczeństwa narodowego.

Druga obejmuje działalność służb specjalnych w rozumieniu art. 11 ustawy z 24.5.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz.U. z 20017 r. poz. 1920 ze zm.), czyli ABW, AW, oraz Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego. Wyłączenie to ma podmiotowy charakter obejmujący całą działalność wskazanych podmiotów, co może rodzić wątpliwości w zakresie właściwego użycia techniki legislacyjnej. O ile ich obecne działania zdają się mieścić w zakresie art. 2 ust. 2 lit. a i d RODO, to w przypadku zmiany obszarów ich zainteresowania należało będzie dokonać ewentualnych korekt przepisu zawartego w OchrDanychU. Sama nazwa służby czy agencji nie przesądza bowiem o jej rzeczowej właściwości, zwłaszcza że zazwyczaj mogą one podejmować działania określone w odrębnych ustawach i umowach międzynarodowych (zob. np. art. 5 ust. 1 pkt 5 ABWU).

Wskazane wyżej rozwiązanie zdaje się potwierdzać uprawnienie krajów członkowskich do rozszerzania stosowania przepisów RODO (lub ich części) na sfery nieobjęte jego działaniem. Ustawodawcy krajowi nie są bowiem objęci ograniczeniami wiążącymi prawodawcę unijnego – w przypadku OchrDanychU widać to choćby w art. 34 ust. 2, który częściowo rozszerza nadzór Prezesa Urzędu Ochrony

Danych Osobowych na podmioty objęte tzw. dyrektywą „policyjną” – dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.4.2016 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 uchyłająca decyzję ramową Rady 2008/977/WSiSW, Dz.Urz. UE L Nr 119, s. 89 (zob. komentarz do art. 55).

2. Zakres podmiotowy. Należy wskazać, że zasady wyrażone w art. 2 wyznaczają krąg podmiotów zobligowanych do przestrzegania RODO. Określenie materialnego zakresu stosowania jego norm prowadzi bowiem do wyznaczenia kategorii podmiotów, które mogą działać poza jego regulacjami. Należy jednak pamiętać o uprawnieniu ustawodawcy krajowego do samodzielnego regulowania stosunków społecznych. Nie można zatem wykluczyć wtórnego obejmowania regulacjami wynikającymi z RODO podmiotów i sfer działania teoretycznie z niego wyłączonych.

Co do zasady RODO skierowane jest do administratorów danych, podmiotów przetwarzających, inspektorów ochrony danych, krajowych organów nadzorczych i innych instytucji biorących udział w procesach nadzoru (w tym instytucji europejskich i EROD) oraz osób, których dane dotyczą.

3. Zakres przedmiotowy. Przyjęta metoda określenia materialnego zakresu stosowania RODO wymaga odrębnego omówienia przesłanek mieszczących się w ust. 1–3 komentowanego artykułu. Należy bowiem wskazać, że ustanowione wyłączenia nie odnoszą się do przesłanek określonych w ust. 1, ale mają charakter podmiotowy (ust. 3) lub związany z celem aktywności, która w sposób obiektywny może być uznana za przetwarzanie danych (ust. 2).

W przypadku działań nieobjętych przesłankami przetwarzania danych wskazanych w ust. 1 zarówno RODO, jak i ustawodawstwo krajowe dotyczące ochrony danych osobowych nie znajdzie zastosowania. Zatem również ten przepis powinien być traktowany jako definiujący ograniczenia stosowania RODO. Nie wyklucza to oczywiście objęcia takich „pominiętych” aktywności innymi rygorami prawnymi gwarantującymi jednostkom ochronę ich wolności i praw – nie będą to jednak normy należące do sfery ochrony danych osobowych.

Przechodząc do analizy zakresu przedmiotowego stosowania reguł ochrony danych osobowych, wynikającego z ust. 1 komentowanego artykułu, należy podkreślić, że na gruncie prawa polskiego prezentowane w nim podejście stanowić będzie pewne *novum*. Jest to jednak wynik wcześniejszej, niespójnej z art. 3 ust. 1 dyrektywy 95/46/WE, implementacji rozwiązań europejskich, przeprowadzonej w ramach art. 2 OchrDanychU16, a w szczególności w jego pierwotnej wersji – sprzed zmian wprowadzonych art. 1 pkt 1 ustawy z 22.1.2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz.U. Nr 33, poz. 285). Pomimo wprowadzonej kilkanaście lat temu nowelizacji w praktyce często dochodziło do błędnej interpretacji obowiązujących przepisów. Wprawdzie wypowiedzi doktryny, GIODO i sądów, pojawiające się po korekcie, nie pozostawiały wątpliwości, że podleganie OchrDanychU16 nie wymaga budowy zbiorów danych w sytuacji, gdy przetwarzanie ma miejsce w systemie informatycznym, ale znaczna część administratorów ograniczała się do analizy art. 2 ust. 1 OchrDanychU16, pomijając jego dalszą część. Należy oczekiwać, że likwidacja rozbieżności przesłanek stosowania reguł ochrony danych i nowa formuła językowa powinny wpłynąć na zmianę świadomości podmiotów zobligowanych do ich stosowania.

Porównanie wskazanego przepisu dyrektywy 95/46/WE i komentowanego artykułu ujawnia jednak, że rozwiązanie przyjęte w RODO bezpośrednio nawiązuje do przyjętych wcześniej regulacji (zestawiając teksty w języku angielskim, można

nawet uznać je za identyczne znaczeniowo), co *de facto* oznacza, że zmiana obserwowana w krajowym systemie prawa nie jest fundamentalna (przynajmniej normatywnie).

Pewne praktyczne znaczenie mieć będzie również zmiana używanego w polskim ustawodawstwie desygnatu przetwarzania danych odbywającego się w systemie informatycznym (który, zgodnie z art. 7 pkt 2a OchrDanychU16, stanowił zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych) na przetwarzanie danych osobowych w sposób całkowicie lub częściowo zautomatyzowany. Pojęcie występujące w RODO jest szersze i można oczekiwać objęcia zasadami ochrony danych również tych sytuacji, w których brać będą udział pojedyncze urządzenia „inteligentne” (np. liczniki, zamki, klucze) i inne urządzenia mechaniczne.

Problem inteligencji urządzeń służących do przetwarzania danych osobowych zyska jednak nowy wymiar, gdy będziemy się starać uznać za przetwarzanie zautomatyzowane operacje podejmowane w niedalekiej przyszłości przez działającą sztuczną inteligencję (SI). Już obecnie istniejące sieci neuronowe wydają się utrudniać kwalifikowanie ich jako automatów – nie jesteśmy bowiem w stanie w pełni kontrolować przebiegających w nich procesów, niemniej do czasu uzyskania przez SI prawnego statusu osoby będzie można traktować procesy przetwarzania danych dokonywane przy ich udziale jako całkowicie lub częściowo zautomatyzowane. Zagadnienie to stanowi poważny problem w sytuacji błyskawicznie rozwijających się technologii tworzenia autonomicznych urządzeń (np. samochodów, dronów, automatów bojowych itd.), które nie tylko przetwarzają dane, ale również wpływają bezpośrednio na wolności i prawa osób fizycznych mających z nimi kontakt.

Podsumowując tematykę zautomatyzowanego lub częściowo zautomatyzowanego przetwarzania, nie sposób pominąć wyrażonej w motywie 15 preambuły woli, by wprowadzana ochrona osób fizycznych, wynikająca z RODO, była neutralna pod względem technicznym i nie zależała od stosowanych technik przetwarzania. Zaistnienie jakiegokolwiek przetwarzania danych osobowych odbywającego się w sposób całkowicie lub częściowo zautomatyzowany potencjalnie wymusza stosowanie RODO, o ile nie zaistnieje wyłączenie takiego obowiązku z uwagi na cel przetwarzania. Bez względu na sekwencję występujących po sobie operacji mieszczących się w pojęciu przetwarzania (zob. komentarz do art. 4 pkt 2 RODO), jeśli choć jedna z nich odbywa się w sposób zautomatyzowany, to całość procesu należy uznać za częściowo zautomatyzowany i jako taki podlegający zasadom RODO.

W przypadku przetwarzania odbywającego się w sposób inny niż zautomatyzowany będzie ono objęte regulami RODO, jeśli dotyczyć będzie danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Stosowanie reguł ochrony danych do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych, sugeruje konieczność występowania elementu wolicjonalnego (decydujący ma być zamiar umieszczenia danych w zbiorze, choćby nawet ostatecznie do tego nie dochodziło) po stronie potencjalnego administratora. Takie ujęcie zgodne jest z poglądami doktryny rozwiniętymi w czasie obowiązywania OchrDanychU16 i przesądza o podleganiu zasadom RODO również wtedy, gdy administrator jeszcze nie pozyskał danych mających trafić do zbioru. Jest to oczywiście również dlatego, że tylko wtedy, gdy administrator ma zamiar tworzyć zbiór, może spełnić wymogi art. 25 RODO nakazującego uwzględnić ochronę danych również przy określaniu sposobów przetwarzania, co bezsprzecznie obejmuje fazę projektowania i budowy struktury zbioru.

Należy jednak podkreślić, że świadome pominięcie realizacji obowiązków z art. 25 w celu ukrycia zamiaru tworzenia zbiorów lub tworzenia, znanych na gruncie OchrDanychU16, zbiorów doraźnych stanowić może okoliczność braną pod uwagę przy ewentualnym ustaleniu wymiaru administracyjnej kary pieniężnej,

zwiększając jej wysokość. Tworzenie nawet chwilowo istniejącego zbioru doraźnego jest przesłanką wymuszającą działanie zgodne z RODO. Szczególnie ostrożnie należy podchodzić do procesów przetwarzania danych osobowych, realizowanych w sposób inny niż zautomatyzowany, które nie mają prowadzić do tworzenia zbiorów. Największym problemem może się w ich wypadku okazać niekonsekwentne trzymanie się technik manualnych i użycie w trakcie realizowania celów, dla których je pozyskano, narzędzi służących do zautomatyzowanego przetwarzania danych (np. digitalizacja zasobów papierowych).

Należy jednak podkreślić, że RODO w sposób jednoznaczny nakazuje brać pod uwagę istnienie zbioru lub zamiaru jego tworzenie jedynie w kontekście przetwarzania danych osobowych w sposób inny niż zautomatyzowany. Tym samym zbiór przestaje być centralnym elementem procesów przetwarzania wykorzystujących, choćby częściowo, metody zautomatyzowane. Nie musi to jednak prowadzić do sytuacji nadmiernej formalizacji procesów przetwarzania danych z uwagi na dużą swobodę, jaką posiada administrator w zakresie doboru odpowiednich środków technicznych i organizacyjnych, wynikającą z art. 24 i 25 (zob. komentarz do art. 24 i 25 RODO). Racjonalizacji stosowania zasad ochrony danych osobowych służy też katalog ograniczeń, który odwołuje się do przesłanek opartych na kryterium celu – z najważniejszym, z punktu widzenia osoby fizycznej przetwarzającej dane, wyłączeniem z zakresu RODO przetwarzania danych przez taką osobę w ramach czynności o czysto osobistym lub domowym charakterze (zob. niżej pkt 5).

4. Przetwarzanie w sposób zautomatyzowany przy braku utrwalenia danych. 4

Rezygnacja z konieczności budowy zbioru może powodować daleko idące konsekwencje przekładające się również na brak wymogu utrwalenia przetwarzanych danych. Podejście takie wpisuje się w zasadę minimalizacji przetwarzania, a rezygnacja ze zbędnych elementów procesu przetwarzania, jeśli nie przyczyniają się one do osiągnięcia jego celu, wydaje się oczywista.

Przykładem takiego przetwarzania może być monitoring dokonywany w czasie rzeczywistym bez nagrywania obrazu, gdzie cel (np. zapewnienie bezpieczeństwa osobom lub ochrona mienia) osiągnięty zostaje dzięki bezpośredniej obserwacji nadzorującego monitora strażnika. Działania administratora również w takiej sytuacji mają jednak wpływ na prawa osób, których dane dotyczą – w tym wypadku dochodzić może choćby do naruszenia prywatności. W przypadku przesyłania danych (obrazu) pomiędzy urządzeniami, co jest istotą monitoringu, dochodzić może również do przechwycenia transmisji, co dodatkowo może wpływać na ryzyko naruszenia wolności i praw osób obserwowanych. Należy zatem przyjąć i wdrożyć odpowiednie zabezpieczenia dla takiego procesu przetwarzania – będzie on jednak prowadzony w warunkach ograniczenia (w sposób immanentnie wynikający z jego natury) realizacji praw jednostki wynikających z RODO. W praktyce administratorowi pozostanie stworzenie warunków umożliwiających dopełnienie obowiązku informacyjnego z art. 13 RODO.

5. Ograniczenie stosowania z uwagi na przedmiot działań administratora. 5

Chcąc prawidłowo ocenić zakres stosowania RODO, należy zwracać uwagę na znajdujące się w nim wyjątki i ograniczenia. Zawarte w ust. 2 komentowanego przepisu cztery punkty zdają się w znacznym zakresie ograniczać stosowanie rozporządzenia ogólnego. Dwa pierwsze zdają się wynikać z samego faktu wyboru formy regulacji, w dwóch kolejnych decydującym elementem jest wola prawodawcy zmierzająca do ich ustanowienia, co oczywiście nie wyklucza ich obiektywnych uwarunkowań. Jak się wydaje, wyłączenia ujęte w lit. a, b i d mają rzeczywiste znaczenie dla prawodawców krajowych i bez ich interwencji nie mają praktycznego wymiaru. Podmioty mogące z nich potencjalnie korzystać (w wyniku materialnego spełnienia kryteriów wskazanych w ograniczeniach stosowania RODO) nie mogą samodzielnie

uznać się za objęte tymi wyłączeniami. Ich zakres w każdym kraju członkowskim zależy bowiem formalnie od nadanego przez ustawodawcę znaczenia poszczególnym pojęciom, które, pomimo posiadania pewnego uniwersalnego wymiaru, nie zostały definicyjnie dookreślone w RODO. Ich rzeczywiste znaczenie odnajdywane jest bowiem na gruncie analizy krajowego porządku prawnego, poczynając od konstytucji i zestawiania osiągniętego rezultatu z prawem pierwotnym i pochodnym UE. Zauważana jest więc pewna swoboda kraju członkowskiego w rozszerzaniu lub zawężaniu granic przesłanek, w ich podmiotowym i przedmiotowym ujęciu, wynikających z art. 2 ust. 2 lit. a i b oraz szczególnie d.

Można oczekiwać, że nazbyt swobodne podejście prowadzące do zbyt szerokiego ujęcia wyłączeń przetwarzania:

- 1) w ramach działalności nieobjętej zakresem prawa Unii (czego przykładem może być wprost wskazane w motywie 16 preambuły bezpieczeństwo narodowe czy też kwestie integralności państwa, obronności, a nawet zagadnienia stanu cywilnego),
- 2) jak też działania objętego wyłączeniem podejmowanego przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE (wspólna polityka zagraniczna i bezpieczeństwo Unii),
- 3) oraz realizowanego przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom (w tym zakresie wydano dyrektywę „policijną”),
– zaowocuje sporem z Komisją, a następnie oddaniem sprawy przed TSUE.

Odmienny charakter ma wyłączenie ujęte w lit. c omawianego przepisu, czyli przetwarzanie danych osobowych realizowane przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze. Zostało ono objęte wskazaniem ujawnionym w motywie 18 preambuły. Zakłada się w nim, że wyłączone spod reżimu RODO powinno zostać przetwarzanie danych osobowych przez osobę fizyczną w ramach działalności czysto osobistej lub domowej, takiej, która pozostaje bez związku z działalnością zawodową lub handlową. Polegać ona może między innymi na korespondencji i przechowywaniu adresów, podtrzymywaniu więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej działalności. Z uwagi na brak definicji legalnej pojęcia czynności o czysto osobistym lub domowym charakterze „komentarz” prawodawcy unijnego staje się istotnym elementem pomagającym zrekonstruować jego znaczenie. Widać w nim chęć przeciwstawienia sobie aktywności osobistej lub domowej, której podejmowanie ma związek z działalnością zawodową lub handlową.

Posiłkując się dotychczasową interpretacją budowaną na analogicznym rozwiązaniu funkcjonującym na gruncie OchrDanychU16 i dyrektywy 95/46/WE, można wskazać, że nie budziło większych wątpliwości stanowisko pozwalające na wyłączenie przetwarzania danych spod rygorów prawa unijnego „(...) jedynie w wypadku, gdy jest ono wykonywane w ramach sfery o czysto osobistym lub domowym charakterze, należącej do osoby, która dokonuje tego przetwarzania”. Z drugiej strony przetwarzanie (w kontekście wyroku, z którego zaczerpnięto wzorzec – chodziło o stały nadzór kamer wideo), które rozciąga się choćby częściowo na przestrzeń publiczną i tym samym jest skierowane poza sferę prywatną osoby dokonującej w ten sposób przetwarzania danych, nie powinno być rozumiane jako czynność o czysto „osobistym lub domowym charakterze” (por. pkt 31 i 33 wyr. z 11.12.2014 r., C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*).

W tej samej sprawie można było również zapoznać się z opinią rzecznika generalnego, w której stwierdzano, że czynności o charakterze domowym „(...) są związane z życiem rodzinnym i normalnie mają miejsce w ramach gospodarstwa

domowego lub w innych miejscach dzielonych z członkami rodziny, takich jak drugie miejsce zamieszkania, hotel pokojowy lub samochód prywatny. Wszystkie one mają związek z ochroną życia prywatnego, o której mowa w art. 7 karty” (por. pkt 51 opinii rzecznika generalnego *N. Jääskinen*, przedstawionej 10.7.2014 r. w sprawie *C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů*).

Jak słusznie wskazuje *D. Lubasz*, na gruncie polskich regulacji „cel osobisty i domowy stawiano w opozycji do działalności statutowej, jako nierealizowanej co do zasady przez osoby fizyczne, oraz zarobkowej i zawodowej, które przesądzały pozytywnie o zastosowaniu ustawy. W przypadku tych dwóch ostatnich, tj. czynności zarobkowych, które wykładano w oparciu o przesłankę zysku, oraz zawodowych, wyróżnianych w oparciu o kryterium profesjonalizmu wykonywania, powstawały jednak wątpliwości interpretacyjno-zakresowe w związku z zasięgiem pojęć czynności osobistych i domowych” (zob. *Bielak-Jomaa, Lubasz, RODO*, s. 136–137). Utrzymanie przedstawionej wyżej sposobu interpretacji wydaje się jednak być nieracjonalne, a w dłuższej perspektywie niemożliwe. Prezes Urzędu Ochrony Danych Osobowych nie ma i nie będzie miał wystarczających możliwości technicznych i organizacyjnych, by sprostać zadaniom, które realizowane miałyby być również w odniesieniu do osób fizycznych działających na granicy cienia semantycznego pojęć mieszczących się w formule „przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze”. Wprowadzenie nowej regulacji daje jednak szansę na zmianę podejścia do niektórych „zastanych” pojęć, zwłaszcza że zmieniająca się rzeczywistość oraz nowe zasady normatywne mogą prowadzić do efektów przeciwnych do oczekiwań prawodawcy. Zalew skarg na działania osób fizycznych, będące wstępem do pozywania ich w ramach procedur opartych na art. 82 RODO, może skutecznie uniemożliwić realizację innych zadań Prezesa Urzędu Ochrony Danych Osobowych. Warto zatem wypracować nowy model rozumienia pojęcia czynności o czysto osobistym lub domowym charakterze.

Należy zauważyć, że pojęcie prywatności podlega ciągłej redefinicji, a jego stały rozwój nie wyklucza objęcia nim w przyszłości różnorodnej aktywności realizowanej publicznie. Zmianie ulega również charakter więzi społecznych wyrażających się choćby w przeniesieniu części aktywności występujących w tej sferze w przestrzeń wirtualną czy choćby posługiwanie się narzędziami opierającymi się na działaniu sieci. Utrzymanie sztywnego podziału na czynności realizowane prywatnie i publicznie, zwłaszcza w przypadku tych dokonywanych przy użyciu narzędzi i technik informatycznych, stanie się praktycznie bezużyteczne. Jako przykład nierozwiązywalny na gruncie dotychczasowego rozumienia wyłączeń z uwagi na ich osobisty lub domowy charakter czy cel, niech posłuży utrzymywanie „domowego archiwum” w chmurze, które ktoś w pewnym momencie postanowi upublicznić poprzez zamieszczenie linku pozwalającego na pobranie zawartych w nim treści na ogólnie dostępnych stronach. Czy i jak odpowiadać będzie taka osoba za łamanie zasad RODO – przecież od początku przetwarzała dane w sposób zautomatyzowany.

Rozwinięcie znaczenia pojęcia przetwarzania w ramach czynności o czysto osobistym lub domowym charakterze na nowe pola aktywności osób fizycznych można rozpocząć od przyjęcia założenia wykluczenia równoczesnego stosowania rygorów RODO w ramach czynności o czysto osobistym lub domowym charakterze (nieobjętych RODO) i działania usługodawcy (objętego jego rygorami), z czego wynika dopuszczalność szeroko ujętej aktywności osób fizycznych podejmowanej w ramach społeczeństwa informacyjnego związanej z upublicznianiem informacji. Następnie dokonać można wyraźnego przeciwstawienia działalności czysto osobistej lub domowej – czyli bez związku z działalnością zawodową lub handlową – tej, która niesie ze sobą takie konotacje. Cel czysto osobisty, a więc niehandlowy, nie musi wykluczać okazjonalnej sprzedaży w ramach aukcji internetowych czy umieszczania ogłoszeń na portalach (nawet z opcją uzyskiwania zysku). Nie wydaje się bowiem

racjonalne dążenie do objęcia czynności będących odpowiednikiem wyprzedazy garażowej wymogami wynikającymi z RODO. Podobne zdanie prezentowali, na gruncie OchrDanychU16, P. Litwiński i P. Barta (zob. P. Barta, P. Litwiński, Ustawa o ochronie danych osobowych, 2016, art. 3a, Nb 2, s. 49). Przykłady przetwarzania danych osobowych przez osobę fizyczną w ramach działalności czysto osobistej lub domowej, wskazane w motywie 18 preambuły, mają charakter otwarty, a mogąc przybierać postać podtrzymywania więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej działalności, nie zamykają drogi do szerokiego korzystania z tych kanałów wymiany informacji. Nie wydaje się racjonalne, by traktować dotychczasowy dorobek orzecznicy TSUE dotyczący interpretacji analogicznego wyłączenia z art. 3 ust. 2 tiret drugie dyrektywy 95/46/WE, w szczególności w sprawie C-101/01, *Lindqvist*, ECLI:EU:C:2003:596, oraz C-73/07, *Satamedia*, ECLI:EU:C:2008:727, za niewzruszalny i mający szansę na zachowanie aktualności w długiej perspektywie czasowej.

Na zakończenie należy podkreślić, że wyłączenie spod rygorów RODO działań osób fizycznych nie prowadzonych w celach zawodowych lub handlowych, a mieszczących się w szeroko ujętych czynnościach realizowanych w ramach działalności czysto osobistej lub domowej, nie wyklucza stosowania innych reżimów ochrony wolności i praw w stosunku do czynności, które zostały nimi objęte, np. prawa autorskiego (obejmującego ochronę wizerunku) czy przepisów prawa karnego i cywilnego w zakresie czynów zabronionych lub powodujących szkodę.

6. **6. Cele osobiste i domowe a przetwarzanie danych bez związku z działalnością zawodową lub handlową.** Bez względu na potencjalną głębokość pojęcia działalności czysto osobistej czy przetwarzania w ramach czynności o czysto osobistym lub domowym charakterze można uznać, że ich stałym elementem może być brak formalizacji relacji w ramach podejmowanych działań. Oznaczałoby to, że przetwarzanie danych podejmowane przez osobę fizyczną, niemające charakteru zawodowego lub handlowego, a związane choćby z realizacją wszelkich hobby, filantropią czy działalnością społeczną i artystyczną, będzie mogło być potencjalnie objęte zwolnieniem z rygorów wynikających z RODO, jeśli nie przybierze postaci sformalizowanej w ramach zewnętrznych struktur, np. stowarzyszeń czy fundacji. Podmioty te nie mogą być bowiem traktowane jak osoby fizyczne czy nawet szeroko pojęta rodzina czy wspólnota domowników. Podmioty, pod szyldem których odbywa się przetwarzanie, będą zatem miały status administratora, a charakter ich relacji z osobą fizyczną przetwarzającą dane i działającą w ich imieniu lub na ich rzecz nie ma istotnego znaczenia (nie jest istotne, czy osoba ta będzie wolontariuszem, czy członkiem stowarzyszenia).

Oceniając zakres działań nieobjętych regulacjami RODO w ramach czynności o czysto osobistym charakterze, należy baczyc na immanentne ograniczenia prawodawstwa pochodnego UE i wyartykułowane w motywie 4 preambuły dążenie do tego, by przetwarzanie danych osobowych zorganizować w taki sposób, aby służyło ludzkości. Przy czym samego prawa do ochrony danych osobowych nie należy traktować jako bezwzględnie, gdyż należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności. Szerokie ujęcie działalności osobistej wynikać powinno też z faktu zadeklarowanego nienaruszania przez RODO „praw podstawowych, wolności i zasad uznanych w Karcie praw podstawowych – zapisanych w Traktatach – w szczególności prawa do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania się, ochrony danych osobowych, wolności myśli, sumienia i religii, wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu oraz różnorodności kulturowej, religijnej i językowej”. Większość z deklarowanych *expressis verbis*, w przytoczonej części motywu 4 preambuły, wolności i praw może

być realizowana przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze, więc nazbyt wąskie postrzeganie zakresu analizowanego pojęcia prowadzić będzie *de facto* do ich ograniczenia. Stosowanie RODO do zwykłej aktywności osób fizycznych, użytkowników czatów czy komunikatorów, blogerów, czy nawet członków wspólnot graczy – klanów, realizowanej w ramach mediów społecznościowych (wszystkie te aktywności związane są z automatycznym przetwarzaniem danych), powodowałby efekt mrozący w zakresie podejmowania swobodnej aktywności (choćby z uwagi na potencjalne kary).

Wyłączenie stosowania RODO w obszarze działalności osób fizycznych związanej z czynnościami o czysto osobistym charakterze nie powinno też prowadzić do nadmiernego ograniczenia praw osób, których dane dotyczą. Wniosek taki wynika z wyartykułowanej w motywie 18 preambuły wskazówki, że RODO ma jednak zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby działalności osobistej lub domowej, czyli wszelkich operatorów sieci, administratorów portali internetowych itp. Oznacza to, że działalność podejmowana osobiście przez osobę fizyczną i tak będzie podlegała pewnej kontroli wynikającej z poddania podmiotów udostępniających środki rygorom RODO, co prowadzi do wniosku, że prawa osób, których dane będą podlegały przetwarzaniu, znajdują ochronę na gruncie tej regulacji. W ekstremalnych przypadkach będzie to prowadziło do budowania i stosowania przez podmioty komercyjne mechanizmów cenzury, zarówno prewencyjnej, jak i następczej, mającej zabezpieczyć je przed skutkami nadużycia praw przez jednostki korzystające z ich usług (tendencje te są już obecne i odczuwalne choćby w ramach kontroli działań podejmowanych przez użytkowników wiodących portali społecznościowych).

7. Stosowanie RODO przez instytucje, organy i jednostki organizacyjne UE. Trzeci ustęp komentowanego artykułu stanowi regułę podmiotowo wyłączającą stosowanie RODO w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne UE. Wskazany w nim akt, rozporządzenie Parlamentu Europejskiego i Rady (WE) Nr 45/2001 z 18.12.2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.Urz. UE L Nr 8, s. 1), oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania będą podlegać dostosowaniu do zasad RODO. 23.5.2018 r. ogłoszono porozumienie polityczne w sprawie przyjęcia równoważnych do RODO zasad, którymi objęte zostaną instytucje i organy UE (zob. informacje na stronie Europejskiego Inspektora Danych Osobowych https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2018-05-revised_reg_45_en.pdf, dostęp: 25.6.2018 r.). To autonomiczne podejście do działania instytucji i organów UE wynika z konieczności ich jednolitego traktowania (oraz równego poziomu realizacji praw jednostki przez te podmioty), co mogłoby być utrudnione, gdyby działające w różnych krajach członkowskich podmioty podlegały krajowym przepisom szczególnym (modyfikującym stosowanie RODO) oraz nadzorowi realizowanemu przez krajowe organy, które w początkowym okresie mogą przyjmować różniącą się wykładnię przepisów RODO.

8. RODO a stosowanie dyrektywy 2000/31/WE (o handlu elektronicznym). Zgodnie z ostatnim ustępem komentowanego artykułu stosowanie RODO w niczym nie narusza ustanowionych zasad wynikających z dyrektywy Parlamentu Europejskiego i Rady 2000/31/WE z 8.6.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.Urz. UE L Nr 178, s. 1). Ma to swój wyraz m.in. w tym, że RODO nie powinno stanowić istotnej przesłanki ograniczenia stosowania dyrektywy, a raczej traktowane być winno jako komplementarny system ochrony praw konsumentów.

Owo uzupełnianie może się wyrażać choćby tym, że np. posiadanie zgody na świadczenie usług drogą elektroniczną może być traktowane jako przesłanka legalizująca proces przetwarzania danych, stanowiąc podstawę wskazania prawnie uzasadnionego interesu administratora – pojawia się on właśnie jako konsekwencja wyrażenia tej zgody. Konkluzja taka wynika wprost z regulacji implementującej dyrektywę 2000/31/WE, czyli ustawy z 18.7.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2017 r. poz. 1219 ze zm.), której art. 10 ust. 1 zakazuje przesyłania niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. Jednakże ust. 2 tego artykułu otwiera taką możliwość, uznając dopuszczalność wysyłki informacji handlowych, jeżeli oznaczony odbiorca wyraził zgodę na ich otrzymywanie, w szczególności, gdy udostępnił w tym celu identyfikujący go adres elektroniczny. Bez wątpienia nie jest to jednak zgoda na przetwarzanie danych osobowych, zatem możliwości ich przetwarzania należy szukać w zawartej pomiędzy podmiotami umowie lub – w przypadku wątpliwości co do jej treści i zakresu – właśnie w prawnie uzasadnionym interesie realizowanym przez administratora lub przez stronę trzecią. Na marginesie należy dodać, że zgoda na otrzymywanie informacji handlowej, nie stanowiąc zgody na przetwarzanie danych, nie jest też objęta regulacjami wynikającymi z art. 12 RODO.

Art. 3. [Terytorialny zakres stosowania]

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.

2. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:

- a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
- b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.

3. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

Spis treści

	Nb
1. Skutek ekstraterytorialny RODO	1
2. Łączniki warunkujące zastosowanie RODO	2
3. Pojęcie monitorowania	3
4. Brak wpływu ogólnych wyłączeń zastosowania prawa UE	4
5. Administrator niemający jednostki organizacyjnej w UE	5

- 1 1. **Skutek ekstraterytorialny RODO.** Ustęp 1 omawianego przepisu wskazuje na ekstraterytorialny skutek RODO. Zgodnie bowiem z tym przepisem RODO ma zastosowanie do przetwarzania danych osobowych niezależnie od tego, czy ma ono miejsce „w Unii” (a więc na terytorium objętym zakresem terytorialnym zastosowania prawa UE, zgodnie z art. 52 TUE i art. 355 TFUE), czy też poza Unią Europejską. Rozwiązanie to jest odmienne od wynikającego z dyrektywy 95/46/WE,