ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4072
PRZEGLĄD PRAWA I ADMINISTRACJI CXXVII
WROCŁAW 2021

https://doi.org/10.19195/0137-1134.127.15

BOGUSŁAW SOŁTYS
ORCID: 0000-0002-8359-7732
Uniwersytet Wrocławski

KONIECZNOŚĆ PRZYJĘCIA EUROPEJSKIEJ REGULACJI W SPRAWIE WARUNKÓW PRZETWARZANIA DANYCH CYFROWYCH OSÓB ZMARŁYCH

Abstrakt: Artykuł wskazuje na konieczność przyjęcia unijnej regulacji wykorzystywania danych cyfrowych osób zmarłych. Europejska strategia w zakresie danych nie poświęca temu zagadnieniu adekwatnej uwagi, podczas gdy rośnie jego znaczenie dla prawidłowego funkcjonowania i rozwoju europejskiej przestrzeni danych.

RODO nie reguluje problematyki przetwarzania danych osobowych po śmierci osób fizycznych, natomiast państwa członkowskie Unii Europejskiej mogą przyjmować przepisy w tym zakresie. Takie rozwiązanie prowadzi jednak do istotnego zróżnicowania warunków przetwarzania na wspólnym rynku danych cyfrowych osób zmarłych. Należy je uznać za nieuzasadnioną barierę wpływającą hamująco na jego rozwój.

Problematyki przetwarzania danych cyfrowych osób zmarłych w sposób odrębny nie traktuje również rozporządzenie w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej. Poddanie wszystkich danych cyfrowych osób zmarłych jednolitej regulacji tego rozporządzenia nie zasługuje na aprobatę. Nie tylko nie uwzględnia specyfiki tego rodzaju danych, ale może również prowadzić do kolizji z przepisami państw członkowskich, w szczególności motywowanych ich nadrzędnym interesem publicznym.

Liczba danych cyfrowych osób zmarłych będzie stale przyrastać, co zaowocuje powstawaniem różnych i nieraz złożonych problemów związanych z przetwarzaniem ich w europejskiej przestrzeni danych. Biorąc pod uwagę niejednorodny charakter oraz specyfikę tych danych, wydaje się, że warunki ich przechowywania oraz przetwarzania na wspólnym rynku należy unormować w sposób szczególny.

Słowa kluczowe: europejski rynek danych cyfrowych, dane osobowe, dane bezosobowe, dane cyfrowe osób fizycznych po ich śmierci, ponowne wykorzystanie danych cyfrowych, unijna swoboda przepływu danych cyfrowych

WPROWADZENIE

Celem artykułu jest zwrócenie uwagi na niedostatki unijnej regulacji przetwarzania danych cyfrowych (elektronicznych) osób zmarłych oraz obiektywną

potrzebę odrębnego unormowania tej kategorii danych cyfrowych. Dotyczy to zarówno danych osobowych, jak i danych bezosobowych, które są wykorzystywane po śmierci osób fizycznych. Aktualnie obowiązujące regulacje, raporty z ich stosowania oraz założenia nowych przepisów nie poświęcają temu zagadnieniu właściwego zainteresowania[1], mimo że dane cyfrowe osób zmarłych mają swoją specyfikę i stanowią coraz większy zbiór z wyraźnie rysującą się tendencją do znacznego i stałego powiększania się[2]. W europejskiej przestrzeni danych nie ma wykształconych odpowiednich mechanizmów identyfikowania statusu osób jako żyjących lub zmarłych. W praktyce obrotu cyfrowego można natomiast zaobserwować coraz więcej różnego rodzaju usług cyfrowych świadczonych nadal mimo śmierci, a także usług adresowanych do osób fizycznych po ich śmierci. Z uwagi na brak dostępu elektronicznego do danych cyfrowych osób zmarłych nierzadko dzieje się tak bez wiedzy i woli osób bliskich zmarłemu czy jej spadkobierców. W wielu przypadkach świadczenie usług cyfrowych skierowanych do osób zmarłych lub ich świadome utrzymywanie może nie tylko wprowadzać w błąd i wywoływać szereg innych niepożądanych konsekwencji, ale również negatywnie oddziaływać na bezpieczeństwo publiczne, zwłaszcza w związku z ryzykiem przejmowania cyfrowej tożsamości osób zmarłych. Z drugiej strony należy mieć na względzie, że niektóre pośmiertne usługi cyfrowe mogą być również świadczone na podstawie woli osoby fizycznej wyrażonej jeszcze za jej życia. W ostatnim czasie na popularności zyskują zwłaszcza usługi polegające na utrzymywaniu wirtualnego grobu oraz podtrzymywaniu, a nawet kreowaniu dobrego wizerunku osoby zmarłej. Generalnie wydaje się, że poza ściśle określonymi przypadkami uzasadnionymi czy to interesem publicznym, czy prawami spadkobierców dane cyfrowe dotyczące osób zmarłych powinny służyć wszystkim żyjącym oraz całym społeczeństwom.

1. STATUS PRAWNY DANYCH CYFROWYCH OSÓB ZMARŁYCH

Dane cyfrowe osób fizycznych po ich śmierci nie przestają automatycznie istnieć, a ich dalszy los zależy od różnych złożonych czynników natury faktycznej i prawnej. Generalnie można stwierdzić, że na skutek śmierci wygasają prawa osób fizycznych do dotyczących ich danych osobowych. Nie implikuje to jednak powszechnego zakazu posługiwania się tymi danymi, zarówno przez usługodaw-

[1] Zob. komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Europejska strategia w zakresie danych*, COM/2020/66 final oraz komunikat Komisji do Parlamentu Europejskiego i Rady, *Ochrona danych jako filar wzmocnienia pozycji obywateli i podejście UE do transformacji cyfrowej — dwa lata obowiązywania ogólnego rozporządzenia o ochronie danych*, COM/2020/264 final.

[2] Por. W. Dubis, M. Daćków, *Prawo do bycia zapomnianym w Internecie — za życia i po śmierci?*, [w:] Non omnis moriar*: osobiste i majątkowe aspekty prawne śmierci człowieka: zagadnienia wybrane*, red. J. Gołaczyński *et al.*, Wrocław 2015, s. 174 n.

ców świadczących uprzednio usługi cyfrowe na rzecz tych osób, jak i przez organy wykonujące zadania publiczne na podstawie przepisów prawa. W każdym razie przetwarzanie danych osobowych, jeśli jest oparte wyłącznie na zgodzie osoby, której dane dotyczą, w razie jej śmierci nie powinno być kontynuowane. Jednak w praktyce obrotu cyfrowego nie zawsze tak się dzieje. Osobowe dane cyfrowe, choć w następstwie śmierci osoby fizycznej obiektywnie przestają mieć status danych osobowych, często nadal są w ten sposób traktowane. Nie ma bowiem odpowiednio skutecznych mechanizmów prawnych i technicznych, które zapewniałyby lub przynajmniej stwarzały możliwość aktualizacji danych bez udziału osoby, której dane dotyczą.

Zgodnie z przepisami po śmierci osób fizycznych ich dane osobowe stają się danymi bezosobowymi. Wniosek taki wynika z rozporządzenia (UE) 2016/679[3] oraz rozporządzenia (UE) 2018/1807[4]. W świetle RODO danymi osobowymi są jedynie dane pozwalające zidentyfikować określoną osobę fizyczną, co po jej śmierci obiektywnie przestaje być możliwe[5]. Motyw 27 uzasadnienia RODO wprost stanowi, że regulacja ta nie ma zastosowania do danych osobowych osób zmarłych. Zgodnie natomiast z intencją RODO państwa członkowskie władne są przyjąć przepisy o przetwarzaniu danych osobowych osób zmarłych. Z kolei według rozporządzenia FFD jego przepisy stosuje się do danych bezosobowych, którymi są wszelkie dane niebędące danymi osobowymi w rozumieniu RODO[6]. Nie chodzi tu więc tylko o dane, które z różnych przyczyn przestały być danymi osobowymi, ale również o wszelkie inne dane niepozwalające na identyfikację osób fizycznych, w tym dotyczące osób prawnych oraz wskazujące na działalność innych jednostek organizacyjnych.

Wydaje się, że możliwość wydawania przez państwa członkowskie UE przepisów regulujących przetwarzanie danych osobowych osób zmarłych może prowadzić do istotnego zróżnicowania warunków korzystania z danych cyfrowych na wspólnym rynku. Pomijając dyskusyjną kwestię dopuszczalności uznawania w krajowych porządkach prawnych danych cyfrowych identyfikujących osoby zmarłe za dane osobowe, należy zauważyć, że na gruncie rozporządzenia FFD mają one charakter danych bezosobowych, chyba że umożliwiają również identyfikację określonych osób żyjących. Nie można więc wykluczyć powstawania ewentualnych kolizji między prawem unijnym, a porządkami prawnymi niektó-

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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 osobowych), Dz.U. L 119 z 4 maja 2016 roku, s. 1–88, dalej: RODO.

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 roku w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej, Dz.U. L 303 z 28 listopada 2018 roku, s. 59–68, dalej: rozporządzenie FFD.

[5] Zob. art. 4 pkt 1 RODO.

[6] Zob. art. 2 ust. 1 w zw. z art. 3 pkt 1 FFD.

rych państw członkowskich, które z różnych względów mogą być zainteresowane utrzymywaniem partykularnych reguł przetwarzania danych cyfrowych osób zmarłych. Takie rozwiązanie nie sprzyja jednak budowaniu ujednoliconej europejskiej przestrzeni danych i należy postrzegać je jako barierę rozwoju wspólnego rynku danych cyfrowych.

Analizując status prawny danych cyfrowych osób zmarłych, nie można zapominać także o tym, że niektóre dane cyfrowe mają charakter majątkowy i wskutek śmierci osób fizycznych podlegają dziedziczeniu. Z reguły ich dalsze przetwarzanie może być więc kontynuowane, ale wiąże się z koniecznością uzyskania zgody spadkobierców, ewentualnie również dochowania innych wymogów formalnych. Mimo że ten rodzaj danych zalicza się także do kategorii danych bezosobowych, to jednak nie należy zrównywać go z niemajątkowymi danymi cyfrowymi, które za życia osoby fizycznej były danymi osobowymi. Wyróżnienie zbioru danych bezosobowych, do których ma zastosowanie rozporządzenie FFD, niewątpliwie łączy wspólna cecha. Jest ona związana z brakiem technicznych możliwości bezpośredniego lub pośredniego powiązania tych danych z określoną osobą fizyczną w sposób pozwalający na jej zidentyfikowanie. Dane bezosobowe tworzą więc bardzo szeroki katalog różnych danych cyfrowych, które obejmują dane dotyczące zarówno osób żyjących, jak i zmarłych oraz dane o charakterze majątkowym lub niemajątkowym[7].

2. SWOBODA PRZEPŁYWU DANYCH CYFROWYCH OSÓB ZMARŁYCH

Dane cyfrowe osób zmarłych wskutek zakwalifikowania ich do kategorii danych bezosobowych podlegają regulacji rozporządzenia FFD. Jego przepisy gwarantują swobodę przepływu danych bezosobowych na terytorium Unii Europejskiej. Co do zasady zabraniają państwom członkowskim wprowadzania zakazów lub ograniczeń dotyczących możliwości przetwarzania tego rodzaju danych w innym państwie członkowskim, w tym obejmującego ich przechowywanie. Wyjątki w powyższym zakresie mogą być przyjmowane w ustawodawstwach państw członkowskich tylko w przypadkach uzasadnionych względami bezpieczeństwa publicznego[8]. W celu zagwarantowania swobody przepływu danych bezosobowych na rynku unijnym państwa członkowskie zobowiązane są do uchylenia swoich przepisów krajowych, które przewidują wymóg lokalizacji danych do terytorium określonego państwa członkowskiego. Ponadto mają obowiązek powiadomienia Komisji Europejskiej o każdym przypadku utrzymania takich

[7] Zob. M. Finck, F. Pallas, *They Who Must Not Be Identified — Distinguishing Personal from Non-personal Data under the GDPR*, „International Data Privacy Law" 2020, nr 1, s. 11–35.

[8] Zob. art. 4 ust. 1 FFD.

wymogów oraz ich uzasadnieniu, a także o każdym projekcie nowych przepisów przewidujących unormowanie lokalizacji danych[9].

Swobodzie przepływu danych bezosobowych na rynku unijnym służą również dwa inne istotne instrumenty kształtowania wspólnej polityki w zakresie europejskiej przestrzeni danych. Pierwszy wyraża się w formalnym zapewnieniu istnienia prawa właściwych organów państw członkowskich do żądania i uzyskiwania dostępu do danych bez względu na ich lokalizację w celu wykonywania obowiązków urzędowych zgodnie z prawem Unii Europejskiej lub z prawem krajowym[10]. Bez takiej gwarancji likwidacja dyskryminacyjnych wymogów prawnych dotyczących lokalizacji danych bezosobowych nie byłaby możliwa. Natomiast czy i w jakim czasie znikną różnego rodzaju bariery faktyczne, zależeć będzie raczej od sprawności działania systemu egzekwowania dostępu do danych, budowania zaufania oraz dalszego rozwoju integracji politycznej i gospodarczej państw członkowskich. Z kolei drugi instrument ma charakter samoregulacyjny i należy do sfery tak zwanego „prawa miękkiego"[11]. Od strony merytorycznej umożliwia on przyjęcie odpowiednich warunków technicznych i organizacyjnych, które sprzyjają optymalnemu korzystaniu z unijnej swobody przepływu danych bezosobowych. W celu zwiększenia mobilności danych oraz podniesienia konkurencyjności usług ich przechowywania i przetwarzania w inny sposób rozporządzenie FFD zapewnia podjęcie różnych działań mających zachęcać usługodawców i użytkowników do opracowania oraz wdrażania szczegółowych i transparentnych kodeksów postępowania zawierających ogólnodostępne informacje na temat warunków przenoszenia danych bezosobowych[12].

Mimo że rozporządzenie FFD najwyraźniej manifestuje swobodę przepływu danych cyfrowych, to jednak również RODO nie zakazuje ani nie ogranicza ich lokalizacji na wspólnym rynku z powodu ochrony danych osobowych[13]. Zapewniając jednolity i wysoki poziom ochrony danych osobowych i nieosobowych, oba rozporządzenia tworzą fundamenty europejskiej przestrzeni danych cyfrowych. Dane osobowe i nieosobowe w praktyce obrotu często ze sobą współistnieją w ramach jednego zbioru danych cyfrowych. Nie istnieje bowiem obowiązek ich odrębnego przechowywania i przetwarzania, a niektóre dane wskutek różnych zabiegów organizacyjnych i technicznych (na przykład anonimizacji) mogą ulegać przekształceniom, a nawet ostatecznie zmieniać swój status. Dane osobowe mogą zatem stawać się danymi nieosobowymi i odwrotnie. Nie dotyczy to jednak danych cyfrowych osób zmarłych, które w następstwie śmierci ich dysponentów, jeśli jednocześnie nie identyfikują innych osób żyjących, przekształcają się w sposób nie-

[9] Zob. art. 4 ust. 2 i 3 FFD.

[10] Zob. art. 5 FFD.

[11] Zob. na przykład Kodeks postępowania UE dotyczący gwarancji przetwarzania danych w usługach chmury, https://eucoc.cloud/en/home.html (dostęp: 13.11.2021).

[12] Zob. art. 6 FFD.

[13] Zob. art. 1 ust. 3 RODO.

odwracalny w dane nieosobowe. W przypadku mieszanego zbioru danych przepisy RODO mają zastosowanie tylko do danych osobowych, natomiast rozporządzenie FFD stosuje się do danych nieosobowych. Jeśli zaś w danym zbiorze dane osobowe i nieosobowe są ze sobą nierozerwalnie związane, prawa i obowiązki wynikające z RODO obowiązują w całym zbiorze danych mieszanych także wtedy, gdy dane osobowe stanowią jego niewielką część[14].

3. NADRZĘDNY INTERES PAŃSTW CZŁONKOWSKICH

Zgodnie z teorią wymogów imperatywnych państwa członkowskie UE władne są w swoich ustawodawstwach wyjątkowo ograniczać unijne swobody z uwagi na swój nadrzędny interes publiczny. Uznanie nadrzędności określonego interesu publicznego kraju członkowskiego możliwe jest jednak tylko w razie spełnienia pewnych warunków mających na celu wykluczenie pozorności, arbitralnej dyskryminacji oraz ukrytych restrykcji, które nie byłyby do pogodzenia z prawem unijnym. Regulacja krajowa przewidująca ograniczenie swobód wspólnego rynku powinna być więc konieczna dla zagwarantowania ochrony konkretnie określonego interesu publicznego oraz proporcjonalna, co wiąże się z odpowiednim wyważeniem wartości chronionych i ograniczanych. Wymaga ono zwłaszcza stwierdzenia niemożliwości zaspokojenia krajowego interesu publicznego za pomocą mniej ingerencyjnych środków, niewykraczania poza to, co jest niezbędne dla osiągnięcia zakładanych efektów regulacyjnych oraz zapewnienia skuteczności ich wdrożenia[15]. Spełnienie wymienionych wymogów, które można również uznać za pewne wzorce kontroli, pozwala nie tylko na uznanie nadrzędności krajowego interesu publicznego nad swobodami wspólnego rynku, ale także na stwierdzenie legalności krajowych regulacji ograniczających te swobody z punktu widzenia prawa unijnego.

Porównując regulację dopuszczalności wprowadzania odstępstw od unijnej swobody przepływu danych osobowych i nieosobowych, należy stwierdzić, że została ona ujęta znacznie bardziej precyzyjnie w stosunku do danych nieosobowych. Zgodnie z rozporządzeniem FFD przechowywanie lub inny rodzaj przetwarzania danych nieosobowych w państwie członkowskim, szczególnie w zakresie wymogów dotyczących ich lokalizacji, dostępności dla właściwych organów i przenoszenia przez użytkowników profesjonalnych może podlegać zakazom lub ograniczeniom tylko w przypadkach uzasadnionych względami bezpieczeństwa

[14] Zob. Komunikat Komisji Parlamentu Europejskiego i Rady, *Wytyczne dotyczące rozporządzenia w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej*, Bruksela 2019, COM/2019/ 250 final.

[15] Zob. C. Barnard, *The Substantive Law of the UE: the Four Freedoms*, Oxford 2007, s. 380; oraz N. Emiliou, *The Principle of Proportionality in European Law: a Comparative Study*, London 1996, s. 134–139, 267–269.

publicznego[16]. O ile są one podyktowane koniecznością zaspokojenia określonego interesu publicznego, mogą natomiast dotyczyć zarówno sfery bezpieczeństwa wewnętrznego, jak i zewnętrznego danego państwa członkowskiego[17].

Ingerowanie w unijną swobodę przepływu danych nieosobowych z innych powodów niż konieczność zapewnienia bezpieczeństwa publicznego państwa członkowskiego jest możliwe jedynie poza zakresem stosowania rozporządzenia FFD albo w ogóle poza zakresem stosowania prawa unijnego. W pierwszym przypadku chodzi o usługi, które są świadczone na rzecz użytkowników mieszkających lub mających siedzibę poza UE niezależnie od *domicilium* dostawcy usług albo świadczone na potrzeby własne dostawcy, który ma miejsce zamieszkania lub siedzibę poza UE. Natomiast w drugim przypadku państwa członkowskie w ogóle nie są zobowiązane do respektowania wspólnotowej swobody przepływu danych nieosobowych[18].

Swoboda przepływu danych osobowych w ramach wspólnego rynku została zagwarantowana dzięki ujednoliceniu poziomu ich ochrony oraz zapewnieniu mechanizmów współpracy krajowych organów nadzorczych. Wysoki poziom unijnej ochrony danych osobowych stwarza jednak dla innych obszarów gospodarczych barierę, która porównywana jest do protekcjonistycznych wymogów dotyczących lokalizacji danych[19]. Zgodnie z RODO państwa członkowskie UE wyjątkowo mogą ograniczyć swobodę przepływu danych osobowych pod warunkiem, że takie ograniczenie nie narusza istoty podstawowych praw i wolności, jest środkiem niezbędnym i proporcjonalnym oraz służącym realizacji określonej kategorii interesu publicznego społeczeństwa demokratycznego[20]. W przeciwieństwie do danych bezosobowych swoboda przepływu danych osobowych może być więc ograniczona w ustawodawstwach krajowych państw członkowskich nie tylko ze względu na konieczność ochrony bezpieczeństwa publicznego czy zabezpieczenia różnych interesów z nim związanych, ale również z uwagi na ochronę osoby, której dane dotyczą lub praw i wolności innych osób, zapewnienie egzekucji roszczeń cywilnoprawnych albo ze względu na inny ważny cel leżący w ogólnym interesie publicznym UE lub państwa członkowskiego, w szczególności dotyczący interesów gospodarczych, finansowych, zdrowia publicznego czy zabezpieczenia społecznego. W każdym razie krajowe wymogi ograniczające unijną swobodę przepływu danych osobowych powinny zawierać przynajmniej określenie celu

[16] Zob. art. 4 ust. 1 w zw. z art. 1 FFD.

[17] Zob. na przykład wyrok TSUE z 23 listopada 2010 roku, *Land Baden-Württemberg v Panagiotis Tsakouridis*, C-145/09, ECLl: EU:C:2010:708, pt 43 oraz wyrok TSUE z 4 kwietnia 2017 roku, *Sahar Fahimian v Bundesrepublik Deutschland*, C-544/15, ECLI: EU: C: 2017: 225, pkt 39.

[18] Zob. art. 2 FFD.

[19] Zob. S. Yakovleva, K. Irion, *Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade*, „International Data Privacy Law" 2020, nr 3, s. 201–221.

[20] Zob. art. 23 ust. 1 RODO.

lub kategorii przetwarzania i rodzaju danych osobowych, zakresu wprowadzanych ograniczeń, zabezpieczeń zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi do danych, okresu przechowywania danych, ryzyka naruszenia praw lub wolności osób, których dane dotyczą, oznaczenie administratora danych oraz prawa do informacji o ograniczeniach dotyczących osób uprawnionych, o ile nie narusza to dopuszczalnego celu ograniczenia[21].

4. PONOWNE WYKORZYSTANIE DANYCH CYFROWYCH

Możliwość ponownego wykorzystania danych cyfrowych ma istotne znaczenie nie tylko dla optymalizacji procesów gospodarczych, ale również dla rozwoju innowacyjnych i zupełnie nowych usług opartych na zastosowaniu nowoczesnych technologii, takich jak na przykład przetwarzanie danych w chmurze, *big data*, sztuczna inteligencja (AI) czy tak zwany internet rzeczy (IoT, *internet of things*). Wymienione zagadnienia stanowią przedmiot regulacji dyrektywy (UE) 2019/1024[22] oraz uzupełniającego ją rozporządzenia (UE) 2020/0340[23].

Dyrektywa w sprawie otwartych danych ustanawia wspólne ramy prawne dotyczące ponownego wykorzystania danych sektora publicznego finansowanych ze środków publicznych zarówno w celach komercyjnych, jak i niekomercyjnych. ODA zakłada wolny dostęp do tej kategorii danych w najszerszym możliwym zakresie, pozwalając jednocześnie wyjątkowo na zamknięcie lub ograniczenie dostępu do danych tylko wtedy, gdy jest to konieczne na przykład z uwagi na kwestie związane z bezpieczeństwem narodowym, uzasadnionymi interesami handlowymi, ochroną tajemnicy przedsiębiorstwa, poufnością, prywatnością oraz ochroną danych osobowych. Dyrektywy ODA nie stosuje się jednak do danych będących przedmiotem praw własności przemysłowej lub intelektualnej osób trzecich. Natomiast ponowne wykorzystanie danych osobowych jest dopuszczalne tylko po dokonaniu ich anonimizacji, która wykluczy możliwość identyfikacji osoby fizycznej, a w stosunku do niektórych danych potrzebne jest także podjęcie innych środków ograniczających ryzyko. Zgodnie z dyrektywą ODA ponowne wykorzystanie danych co do zasady powinno być nieodpłatne, co nie wyklucza jednak możliwości pobierania opłat stanowiących pokrycie uzasadnionych kosztów reprodukcji, anonimizacji i rozpowszechniania dostępu do danych. Nieodpłatność nie dotyczy organów sektora publicznego, które muszą uzyskiwać dochody w celu pokrycia

[21] Zob. art. 23 ust. 2 RODO.

[22] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 roku w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego, Dz.U. L 172. s. 56–83, dalej: dyrektywa w sprawie otwartych danych lub ODA.

[23] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2020/0340 w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi), 25 listopada 2020 roku, COM (2020) 767 final, dalej: DGA.

znacznej części kosztów związanych z wykonywaniem swoich zadań publicznych, bibliotek, muzeów, archiwów oraz przedsiębiorstw publicznych[24].

Z kolei głównym celem rozporządzenia w sprawie zarządzania danymi jest zwiększenie dostępności i ponownego wykorzystywania danych cyfrowych poprzez wzmocnienie mechanizmów ich podaży oraz zaufania do różnych pośredników wspomagających posiadaczy danych, zarówno osobowych, jak i nieosobowych. Rozporządzenie DGA reguluje możliwość ponownego wykorzystywania danych sektora publicznego w zakresie, w jakim są one objęte prawami innych osób[25], komercyjne udostępnianie danych między przedsiębiorstwami, udostępnianie danych osobowych oferowanych bezpośrednio przez ich posiadaczy lub przez pośredników oraz korzystanie z danych przekazanych z pobudek altruistycznych. Ustanawia również specjalne ramy prawne dotyczące warunków świadczenia usług udostępniania danych, zgłaszania dostawców tych usług i nadzoru nad ich działalnością[26], a także rejestracji podmiotów gromadzących i przetwarzających dane przekazane z pobudek altruistycznych w celu ich udostępnienia w interesie ogólnym na potrzeby badań naukowych lub poprawę jakości usług publicznych[27]. W stosunku do organizacji o altruistycznym podejściu do danych, oprócz ich rejestracji we właściwym organie każdego z państw członkowskich UE, rozporządzenie DGA wymaga, aby były one tworzone w celu realizacji interesu ogólnego, prowadziły działalność o charakterze niekomercyjnym i w sposób niezależny od jakiegokolwiek podmiotu nastawionego na zysk oraz wykonywały swoje zadania związane z przetwarzaniem danych z pobudek altruistycznych z zachowaniem transparentności, w odrębnej strukturze danych. Na potrzeby zapewnienia prawidłowej realizacji zadań o altruistycznym podejściu do danych rozporządzenie DGA wprowadza ujednolicony europejski formularz zgody na gromadzenie i przetwarzanie danych oraz ustanawia szczególne wymogi dotyczące ochrony praw i interesów osób fizycznych, a także innych podmiotów uprawnionych do poszczególnych danych osobowych lub nieosobowych[28].

5. POTRZEBA ODRĘBNEJ REGULACJI WARUNKÓW PRZETWARZANIA DANYCH CYFROWYCH OSÓB ZMARŁYCH

Wydaje się, że wskazane regulacje RODO, FFD oraz ODA i DGA składające się na fundamenty europejskiej przestrzeni danych są niewystarczające dla zapewnienia prawidłowego rozwoju gospodarki opartej na ponownym wykorzystaniu danych cyfrowych. Nie uwzględniają one specyfiki złożonej sytuacji prawnej

[24] Zob. art. 6 ODA.
[25] Zob. art. 3–8 DGA.
[26] Zob. art. 15–22 DGA.
[27] Zob. *ibidem*. Por. art. 5 ust. 1 „e" i art. 89 RODO.
[28] Zob. art. 19 i 22 DGA.

danych cyfrowych osób zmarłych. Prawo do dysponowania danymi cyfrowymi osób zmarłych, bez względu na ich jednostkowy, osobowy czy nieosobowy charakter, powinno zostać unormowane na poziomie prawa unijnego. Jest to niezbędne nie tylko dla zachowania jednolitości i transparentności europejskiego rynku cyfrowego, ale również zwiększenia bezpieczeństwa obrotu. Posiadacze danych cyfrowych przed ich udostępnieniem różnym użytkownikom powinni mieć bowiem zapewnioną możliwość nabycia prawa do udzielania dostępu do danych, a taki efekt ze względu na specyfikę obrotu cyfrowego wymaga odpowiedniego skoordynowania ustawodawstw państw członkowskich. Natomiast obecnie nie ma nawet systemu weryfikacji statusu danych cyfrowych w zakresie identyfikowania ich jako danych osób żyjących lub zmarłych, w konsekwencji czego stosunkowo łatwo może dochodzić do różnych nadużyć. Po śmierci osób fizycznych brak jest również ustandaryzowanych reguł ustalania prawa do ich danych cyfrowych, co negatywnie wpływa na możliwość ponownego ich wykorzystania. Wydaje się, że osoby fizyczne powinny mieć zapewnioną możliwość decydowania na wypadek śmierci o przeznaczeniu swoich danych cyfrowych i to przynajmniej w określonym zakresie w sposób niezależny od zasad prawa spadkowego. Usługodawcy powinni zaś otrzymać gwarancję możliwości świadczenia usług cyfrowych do czasu sprzeciwu ze strony spadkobierców.

WNIOSKI

Obowiązujące regulacje prawa unijnego — ze szkodą dla prawidłowego funkcjonowania europejskiej przestrzeni danych cyfrowych — nie zawierają odrębnego unormowania dotyczącego losu danych osób fizycznych po ich śmierci. Liczba danych cyfrowych osób zmarłych ciągle wzrasta i brak odpowiedniej regulacji ich statusu prawnego hamująco wpływa na wspólny rynek usług cyfrowych. Biorąc pod uwagę niejednorodny charakter tych danych oraz specyfikę, wydaje się, że warunki ich przechowywania oraz przetwarzania należy unormować w sposób szczególny — niezależny od istniejących regulacji dotyczących danych osobowych i nieosobowych.

THE NECESSITY OF IMPLEMENTING THE EUROPEAN REGULATION ON THE CONDITIONS OF PROCESSING THE DIGITAL DATA OF DECEASED PERSONS

Summary

The article indicates the necessity of implementing the EU regulation on using the digital data of deceased persons. The European strategy on data does not pay enough attention to this issue, while its significance for the proper functioning and development of European data space increases.

GDPR does not regulate the problematics of processing personal data after the death of physical persons, but members of the EU can implement their own regulations. This solution leads to a significant diversification of the conditions of processing in the common market the digital data of deceased persons. This solution should be considered an unfounded barrier restraining its development.

The problematics of processing the personal data of deceased persons is not addressed in the regulation on the framework for the free flow of non-personal data in the EU either. Applying the provisions of this regulation to processing the data of the deceased does not deserve approval. Not only does it not include the specifics of this kind of data but it might also lead to collisions between the regulations of respective Member States, especially motivated by their overriding public interest.

The amount of data of the deceased will constantly rise, which will result in different kinds of complicated problems related to processing this data in the European data space. Taking into consideration the heterogenous character of this data and its specifics it seems that the conditions of their possessing and processing in the common market require special regulation.

Keywords: digital data European market, personal data, non-personal data, personal data of physical persons after their death, re-using digital data, free-flow of personal data in the EU

BIBLIOGRAFIA

Barnard C., *The Substantive Law of the UE: the Four Freedoms*, Oxford 2007.

Dubis W., Daćków M., *Prawo do bycia zapomnianym w Internecie — za życia i po śmierci?*, [w:] Non omnis moriar*: osobiste i majątkowe aspekty prawne śmierci człowieka: zagadnienia wybrane*, red. J. Gołaczyński, J. Mazurkiewicz, J. Turłukowski, D. Karkut, Wrocław 2015.

Emiliou N., *The Principle of Proportionality in European Law: a Comparative Study*, London 1996.

Finck M., Pallas F., *They Who Must Not Be Identified — Distinguishing Personal from Non-personal Data under the GDPR*, „International Data Privacy Law" 2020, nr 1.

Yakovleva S., Irion K., *Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade*, „International Data Privacy Law" 2020, nr 3.