E-USŁUGI A RODO

Małgorzata Ciechomska

Wolters Kluwer

E-USŁUGI A RODO

Małgorzata Ciechomska

Wolters Kluwer

WARSZAWA 2021

Stan prawny na 20 maja 2021 r.

Recenzent
Prof. dr hab. Dagmara Kornobis-Romanowska

Wydawca
Dagna Kordyasz

Redaktor prowadzący
Tomasz Pietrzak

Opracowanie redakcyjne
Katarzyna Rybczyńska

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski

ISBN 978-83-8246-137-4 *ISBN PDF-a: 978-83-8246-445-0*

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

Niniejszą publikację dedykuję
wszystkim cudownym kobietom, które spotkałam na swojej drodze:
mojej kochanej Mamie i Siostrze za nieustającą wiarę we mnie i moje możliwości,
Przyjaciółkom za cierpliwość i wsparcie
„and last but not least", Szanownej Pani Profesor ALK Agnieszce Grzelak,
za mądrość, metodologię i spokój, które są dla mnie źródłem inspiracji.

SPIS TREŚCI

Część III
OCHRONA DANYCH OSOBOWYCH USŁUGOBIORCÓW USŁUG SPOŁECZEŃSTWA INFORMACYJNEGO NA PODSTAWIE RODO

WYKAZ SKRÓTÓW

Źródła prawa

dyrektywa 95/46/WE	–	dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. WE L 281 z 23.11.1995 r., s. 31) – (uchylona)
dyrektywa 97/66/WE	–	dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z 15.12.1997 r. w sprawie przetwarzania danych osobowych i ochrony danych w sektorze telekomunikacyjnym (Dz.Urz. WE L 24 z 30.01.1998 r., s. 1) – (uchylona)
dyrektywa 2000/31/WE	–	dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 8.06.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (Dz.Urz. WE L 178 z 17.07.2000 r., s. 1)
dyrektywa 2002/58/WE	–	dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), (Dz.Urz. WE L 201 z 31.07.2002 r., s. 37 ze zm.)
dyrektywa ramowa	–	dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z 7.07.2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (Dz. Urz. WE L 108 z 24.04.2002 r., s. 33).

EKŁE	–	Europejski Kodeks łączności elektronicznej, wprowadzony dyrektywą Parlamentu Europejskiego i Rady (UE) 2018/1972 z 11.12.2018 r. ustanawiającą Europejski Kodeks łączności elektronicznej (Dz.Urz. UE L 321 z 17.12.2018 r., s. 36)
EKPCz	–	Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie 4.11.1950 r. (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.)
konwencja nr 108	–	Konwencja nr 108 Rady Europy, sporządzona w Strasburgu 28.01.1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. z 2003 r. Nr 3, poz. 25)
KPP	–	Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE C 326 z 26.10.2012 r., s. 391)
RODO	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 4.05.2016 r., s. 1)
rozporządzenie Rzym I	–	rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 593/2008 z 17.06.2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I), (Dz.Urz. UE L 177 z 4.07.2008 r., s. 6)
rozporządzenie w sprawie danych nieosobowych	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z 14.11.2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz.Urz. UE L 303 z 28.11.2018 r., s. 59)
TFUE	–	Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana: Dz.Urz. UE C z 2016 r. C 202, s. 47)
TUE	–	Traktat o Unii Europejskiej (Dz.U. z 2004 r. Nr 90, poz. 864/30 ze zm.)
u.o.d.o.	–	ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)
u.o.d.o. z 1997 r.	–	ustawa z dnia 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.)
u.ś.u.d.e.	–	ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344)

Publikatory i czasopisma

CLSR	–	Computer Law & Security Review
Dz.U.	–	Dziennik Ustaw
Dz.Urz. UE	–	Dziennik Urzędowy Unii Europejskiej
Dz.Urz. WE	–	Dziennik Urzędowy Wspólnot Europejskich
EDPL	–	European Data Protection Law Review
EPS	–	Europejski Przegląd Sądowy
Harv. L. Rev.	–	Harvard Law Review
IAP	–	Informacja w Administracji Publicznej
IDPL	–	International Data Privacy Law
IKAR®	–	Internetowy Kwartalnik Antymonopolowy i Regulacyjny
JILT	–	Journal of Information Law & Technology
Mon. Praw.	–	Monitor Prawniczy
MPB	–	Monitor Prawa Bankowego
PiP	–	Państwo i Prawo
PME	–	Kwartalnik Naukowy Prawo Mediów Elektronicznych

Inne

CNIL	–	Commission Nationale de l'Informatique et des Libertés
DPC	–	Data Protection Commission (irlandzka Komisja ds. Ochrony Danych Osobowych)
EROD	–	Europejska Rada Ochrony Danych
Grupa Robocza art. 29	–	nieistniejąca już Grupa robocza ds. ochrony danych powołana na mocy art. 29 dyrektywy 95/46, niezależny organ doradczy w zakresie ochrony danych i prywatności; została rozwiązana 25.05.2018 r., a w jej miejsce została powołana Europejska Rada Ochrony Danych
ICO	–	Information Commissioner's Office
ICT	–	Information and Communication Technologies (technologie informacyjno-komunikacyjne)
IT	–	Information Technology (technologia informacyjna, która umożliwia cyfrowe przetwarzanie informacji)
KE	–	Komisja Europejska
LIBE	–	Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego

NIST	–	National Institute of Standards and Technology (Narodowy Instytut Standaryzacji i Technologii)
OECD	–	Organisation for Economic Co-operation and Development (Organizacja Współpracy Gospodarczej i Rozwoju)
OTT	–	Over-the-Top communication services (usługi świadczone ponad siecią)
SIN	–	Społeczna Inicjatywa Narkopolityki
SNS	–	social networking service („sieciowy serwis społecznościowy")
TSUE	–	Trybunał Sprawiedliwości Unii Europejskiej
URL	–	unique resource locators (ujednolicony format określania lokalizacji danych stosowany w internecie)

WSTĘP

1. Kształtowanie się społeczeństwa informacyjnego

XXI wiek to początek nowej cywilizacji nazywanej erą informacyjną czy cyfrową, a świat, który nas otacza, określany jest mianem cyfrowej wioski[1]. Jak słusznie zauważa Y. Masuda „cywilizacja, którą zbudujemy, zbliżając się do końca XX wieku, nie będzie faktycznie cywilizacją materialną, (...), ale będzie faktycznie cywilizacją niewidoczną". Precyzyjnie powinno się ją nazwać cywilizacją informacyjną.

Obecna rewolucja technologiczna wywiera zasadniczy wpływ na funkcjonowanie rynku usług i sposobów ich świadczenia. Całkowicie zmienił się dotychczasowy model rynkowy. Zarówno usługodawcy, jak i usługobiorcy usług społeczeństwa informacyjnego[2], muszą zmierzyć się z nowymi wyzwaniami, wymuszonymi przez rozwój technologii informacyjno-komunikacyjnych. Rozwój tego typu usług jest traktowany jako element procesu kreowania społeczeństwa informacyjnego. Na przedmiotowy proces istotny wpływ ma również wzrastająca liczba osób posiadających urządzenia (tj. komputer, telefon czy tablet) z dostępem do internetu[3], a to z kolei wpływa na dynamikę wzrostu świadczenia usług *online*.

---

[1] Zob. D. Lombard, *Globalna wioska cyfrowa. Drugie życie sieci*, Warszawa 2009.

[2] Zgodnie z art. 1 ust. 1 lit. b dyrektywy 2015/1535 usługa społeczeństwa informacyjnego to: „każda usługa świadczona normalnie za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie usługobiorcy" (np. usługi wideo na żądanie, niezamówione informacje handlowe, aplikacje mobilne, portale społecznościowe czy chmury obliczeniowe), zwana również „e-usługą".

[3] Według raportu *Digital in 2018* serwisu We Are Social 4,021 mld użytkowników posiada dostęp do internetu, stanowi to 46% globalnej penetracji, więcej zob. https://

Początek rewolucji internetowej sięga roku 1964, kiedy to ukazała się seria raportów P. Barana[4]. To wówczas po raz pierwszy zostały zaprezentowane założenia rozproszonej, zdecentralizowanej sieci komputerowej, zdolnej do funkcjonowania nawet w przypadku awarii wielu węzłów sieci. Następnie w 1969 r. powiązana z wojskiem agencja ARPA[5] na zlecenie Departamentu Obrony USA zainstalowała pierwsze węzły sieci ARPA-NET na Uniwersytecie Kalifornijskim w Los Angeles i tym samym powstała pierwsza cywilna sieć komputerowa. Kolejnym krokiem milowym w rozwoju sieci Internet było stworzenie dokumentów hipertekstowych World Wide Web, a następnie podstaw języka HTML, w której została napisana pierwsza strona internetowa przez Tima Berners-Lee. To właśnie wynalezienie sieci Internet oraz upowszechnienie koncepcji stron internetowych stworzyło dogodne warunki dla globalnej rewolucji komunikacyjnej. W latach 1994–1995 powstały pierwsze sklepy internetowe, m.in. amazon.com, e-Bay.com, wyszukiwarki internetowe Google, Yahoo – to ten moment powszechnie uznawany jest za początek ery nowoczesnego handlu elektronicznego[6]. Natomiast największy portal społecznościowy Facebook powstał w 2004 r. Z całą pewnością bez rewolucji technologicznej, tj. bez wynalezienia sieci Internet, stron WWW i pakietowej transmisji danych, nie byłoby możliwe powstanie społeczeństwa informacyjnego.

Społeczeństwo informacyjne po raz pierwszy zostało zdefiniowane w 1963 r. w artykule T. Umesao, poświęconym teorii ewolucji społeczeństwa opartego na „przemysłach informacyjnych"[7]. Autor w ten sposób określił japońską gospodarkę, tworzoną w oparciu o informacje i technologie. W Polsce 35 lat później T. Goban-Klas i P. Sienkiewicz

wearesocial.com/blog/2018/01/global-digital-report-2018 (dostęp: 5.05.2021 r.).

[4] Zob. P. Baran, *On Distributed Communications Networks*, więcej zob. https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf (dostęp: 5.05.2021 r.).

[5] Advanced Research Project Agency (ARPA) była główną agencją Departamentu Obrony w Stanach Zjednoczonych Ameryki.

[6] P. Polański, *Europejskie prawo handlu elektronicznego. Mechanizmy regulacji usług społeczeństwa informacyjnego*, Warszawa 2014, s. 3.

[7] T. Umesao, *Joho sangyo ron (On information industries)*, Kyoto 1963, za: T. Kamińska, J. Fryca, B. Majecka, *Efektywność gospodarki opartej na wiedzy. Teoria i praktyka*, Gdańsk 2007, s. 76.

zdefiniowali społeczeństwo informacyjne jako: „społeczeństwo, które nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz środki te są podstawą tworzenia dochodu narodowego i dostarczają źródła utrzymania większości społeczeństwa"[8]. Według M. Castellsa[9] dynamiczny rozwój technik informacyjnych prowadzi w konsekwencji do transformacji nie tylko w sferze ekonomicznej czy politycznej, ale – co równie istotne – w sferze społecznej, powodując wyłonienie się nowej struktury społecznej opartej na informacji i globalizacji. Z kolei organizacje, które najlepiej przystosują się do przetwarzania ogromnych ilości danych (ang. *big data*) i skomercjalizują je w skali globalnej dzięki sieci Internet, staną się filarami owego nowego porządku społecznego. M. Castells twierdzi, że efektem zmian technologicznych będzie powstanie „społeczeństwa sieciowego" (ang. *network society*)[10]. Już teraz najmłodsze pokolenie usługobiorców usług społeczeństwa informacyjnego, które dorastało w otoczeniu cyfrowym, definiowane jest jako *digital natives*[11].

Społeczeństwo informacyjne jest z jednej strony bardziej zaangażowane w rozwój nowych technologii poprzez chociażby korzystanie z e-usług, ale z drugiej strony w znacznie większym stopniu narażone jest na zagrożenia z tym związane, tj. utratę prywatności czy nieuprawnione przetwarzanie danych osobowych.

[8] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999.

[9] Zob. M. Castells, *Społeczeństwo sieci*, Warszawa 2010.

[10] Zob. M. Castells, *The Information Age: Economy, Society and Culture*, t. 1, *The rise of the Network Society* (1996), t. 2, *The Power of Identity* (1997), t. 3, *End of Millennium* (1998).

[11] Zob. J. Palfrey, U. Gasser, *Born digital. Understanding the First Generation of Digital Natives*, Philadelphia 2010.

2. Rozwój internetu i technologii informacyjno-komunikacyjnych i związane z tym zagrożenia dla ochrony danych osobowych – zarys problemu

Społeczeństwo informacyjne znajduje się w stanie ciągłego strumienia zmian technologicznych. Sieć Internet, jako kanał informacji (strony internetowe) i komunikacji (e-mail, chat, IM, VoIP), staje się miejscem przechowywania i przetwarzania olbrzymiej ilości danych. Dynamiczny rozwój internetu i technologii informacyjno-komunikacyjnych (ang. ICT), a co za tym idzie – radykalna zmiana naszego stylu życia, nawyków czy zachowań, powoduje, że technologie te są wszechobecne. Co więcej, są one w stanie funkcjonować jako autonomiczne systemy, które nie tylko zbierają nasze dane, ale również przetwarzają je na niespotykaną dotąd skalę. Zjawisko to związane jest z ewolucją technologii przetwarzania danych, tj. konwergencją mediów oraz rozwiązań technologicznych, powszechnością dostępu do internetu, dostępnością urządzeń podłączonych do internetu, w tym rozwojem tzw. internetu rzeczy[12], wydajnością sprzętu i oprogramowania służącego do przetwarzania danych, popularnością portali społecznościowych, zakupów *online*, usług w chmurze obliczeniowej[13] czy usług e-administracji.

W dobie postępującej informatyzacji życia społecznego, kiedy miliony usługobiorców korzysta za pośrednictwem internetu z usług społeczeństwa informacyjnego, dochodzi coraz częściej do naruszenia prawa do ochrony danych osobowych. Usługa społeczeństwa informacyjnego to każda usługa świadczona normalnie za wynagrodzeniem, na odleg-

[12] Internet rzeczy (również internet przedmiotów, ang. *Internet of Things* – IoT) – koncepcja, zgodnie z którą jednoznacznie identyfikowalne przedmioty mogą pośrednio albo bezpośrednio gromadzić, przetwarzać lub wymieniać dane za pośrednictwem sieci komputerowej. Zob. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20100312STO70527+0+DOC+XML+V0//PL (dostęp: 5.05.2021 r.) oraz opinię Grupy Roboczej art. 29 w sprawie ostatnich postępów w dziedzinie internetu przedmiotów, 8/2014 (WP 223) z 16.09.2014 r.

[13] Chmura obliczeniowa (ang. *cloud computing*) obejmuje zestaw technologii i modeli usług, które koncentrują się na wykorzystywaniu i dostarczaniu poprzez internet aplikacji informatycznych, możliwości przetwarzania, zasobów pamięci (ang. *storage and memory space*). Zob. opinię Grupy Roboczej art. 29 w sprawie przetwarzania danych w chmurze obliczeniowej, 5/2012 (WP 196) z 1.07.2012 r.

łość, drogą elektroniczną i na indywidualne żądanie usługobiorcy[14]. To właśnie szybkie tempo zmian technologicznych oraz postępująca globalizacja radykalnie zmieniły sposób zbierania stale rosnącej ilości danych, dostępu do nich, ich dalszego przetwarzania, w tym chociażby wykorzystywania i przekazywania, a te wszystkie „działania" na danych stały się stałym elementem życia dużej części z 4,021 mld[15] użytkowników internetu. Jedynie w ciągu ostatnich kilku lat przyrost danych w postaci cyfrowej osiągnął 90% wszystkich zgromadzonych dotychczas danych. Według raportów pochodzących od firmy IBM, codziennie generowane jest 2,5 tryliona bajtów danych[16]. Ten gwałtowny wzrost ilości cyfrowych danych spowodował, że dotychczasowe tradycyjne techniki ich przetwarzania i przechowywania stały się nieadekwatne do obecnych potrzeb. Powyższe zjawisko należy wiązać z pojawieniem się nowego terminu: *big data*[17], który w powszechnym znaczeniu dotyczy technologii gromadzenia i analizy danych o dużej wielkości i złożoności. Źródłem tych danych mogą być zarówno tradycyjne bazy danych, jak i analiza różnego rodzaju e-dokumentów, e-maili, danych pochodzących z mediów społecznościowych, różnego typu czujników elektronicznych, w tym wykorzystywanych w inteligentnych sieciach *smart grid*[18], czy w końcu urządzeń lokalizacyjne typu GPS[19]. Obserwowany intensywny przyrost danych, w tym danych nowej generacji (np. dane o lokalizacji), był również możliwy ze względu na pojawienie się urządzeń do przekazu i przesyłu danych, takich jak telefony komórkowe, smartfony czy tablety. W tych dużych zbiorach dane przetwarzane są niemalże w sposób

[14] Zob. art. 1 ust. 1 lit. b dyrektywy 2015/1535.

[15] Zob. raport Agencji We are social, http://wearesocial.com/blog/2018/01/global-digital-report-2018 (dostęp: 17.05.2021 r.).

[16] Zob. http://www-01.ibm.com/software/data/bigdata/ (dostęp: 5.05.2021 r.).

[17] Zob. A. Cavoukian, J. Jonas, *Privacy by Design in the Age of Big Data*, https://www.datatilsynet.no/globalassets/global/seminar_foredrag/innebygdpersonvern/privacy-by-design-and-big-data_ibmvedlegg1.pdf (dostęp: 5.05.2021 r.).

[18] Inteligentna sieć (*smart grid*) – inteligentne sieci elektroenergetyczne, gdzie istnieje komunikacja między wszystkimi uczestnikami rynku energii mająca na celu dostarczanie usług energetycznych, zapewniając obniżenie kosztów i zwiększenie efektywności oraz zintegrowanie rozproszonych źródeł energii, w tym także energii odnawialnej. Zob. W.R. Wiewiórowski, *Prawo do prywatności w systemie inteligentnych sieci*, Mon. Praw. – dodatek 2013/8, s. 22.

[19] GPS (*Global Positioning System*) – system nawigacji satelitarnej.

ciągły do analizy rozmaitych korelacji i przy pomocy coraz bardziej skomplikowanych i wysublimowanych algorytmów.

W dzisiejszych cyfrowym świecie „jednostka jest beneficjentem, ale zarazem ofiarą nowoczesnych technik zbierania informacji"[20]. Z jednej strony profilowanie danych w zbiorach *big data* może stanowić zagrożenie zarówno dla ochrony prywatności, w tym ochrony danych osobowych usługobiorców usług społeczeństwa informacyjnego, jak i prowadzić do ich dyskryminacji czy naruszenia zasad równego traktowania poprzez przypisanie ich do określonych grup (tzw. targetowanie ofert). Natomiast z drugiej strony analiza zbiorów *big data* ma także swoje pozytywne strony, może okazać się przydatna dla społeczeństwa w celu wykrywania epidemii chorób, skutków ubocznych lekarstw czy zwalczania zanieczyszczenia środowiska[21].

W tym miejscu warto zwrócić uwagę na model biznesowy świadczenia usług społeczeństwa informacyjnego. Usługobiorcy coraz częściej biorą za standard korzystanie z pozornie bezpłatnych e-usług. Ukrytą opłatę stanowią ich dane pozyskane wraz ze świadczoną e-usługą. Dzięki powyższym działaniom możliwe jest monitorowanie i profilowanie zachowań *online* usługobiorców, co w oczywisty sposób może wpływać na ograniczenie ich autonomii informacyjnej. Dotyczy to również wykorzystywania do analiz danych osobowych uprzednio zanonimizowanych. Natomiast duża liczba danych na temat konkretnej osoby (często pochodzących z różnych źródeł), przetworzona przez nowoczesne narzędzia analityczne, może doprowadzić do jej reidentyfikacji, tj. wskazania jej, bez konieczności podania takich danych, jak jej imię czy nazwisko. Innymi słowy, dzięki rozwojowi nowoczesnych systemów teleinformatycznych oraz nowych rodzajów danych (np. dane o lokalizacji typu GPS, pozwalające na lokalizowanie adresów zamieszkania bądź przebywania usługobiorców, śledzenia cyberaktywności za pomocą plików *cookies*,

[20] M. Safjan, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informacyjnym*, PiP 2002/6, s. 7.

[21] Zob. Opis analizy zachorowań na wirus H1N1 przeprowadzoną przez systemy firmy Google, V. Mayer-Schonberger, K. Cukier, *Big Data. Rewolucja, która zmieni nasze myślenie, pracę i życie*, Warszawa 2014, s. 15.

adresów IP, e-maila czy tzw. *social loginów*) możliwe jest stworzenie zbioru danych pozwalających na reidentyfikację konkretnego usługobiorcy. Zagrożeniem dla ochrony danych osobowych usługobiorców e-usług wydaje się również fakt, iż połączone dane pochodzące z różnych źródeł i są wykorzystywane do celów innych niż te, do których zostały pierwotnie zebrane. Powyższe informacje mają określoną wartość ekonomiczną, a połączone z danymi o charakterze osobowym stanowią o przewadze konkurencyjnej między przedsiębiorcami, co jest szczególnie istotne w dzisiejszym otoczeniu biznesowym, tj. ciągłej walce o klienta, jego utrzymaniu czy zachowaniu dotychczasowej pozycji rynkowej[22]. Według danych przedstawionych przez GIODO w „Raporcie o ochronie danych osobowych"[23] wartość danych obywateli UE w 2011 r. wynosiła 315 mld euro, natomiast do końca roku 2021 r. może wzrosnąć do blisko 1 bln euro rocznie.

Nie ulega wątpliwości, że coraz większy wachlarz usług społeczeństwa informacyjnego stanowi ogromne wyzwanie dla skuteczności regulacji dotyczących prawa do ochrony danych osobowych. Dzięki wykorzystaniu nowoczesnych narzędzi przetwarzania danych oraz internetu obserwujemy znaczący wzrost zagrożenia dla prywatności usługobiorców usług społeczeństwa informacyjnego, których dane poddawane są automatycznemu przetwarzaniu, ich autonomii informacyjnej czy bezprawnego przetwarzania ich danych osobowych. Obecnie prawo do ochrony danych osobowych, w tym zagrożenia dla prywatności jednostki związane z gromadzeniem i automatycznym przetwarzaniem danych osobowych, nabiera nowego znaczenia. Nie mówimy już o wykorzystywaniu „zwykłych" systemów teleinformatycznych do przetwarzania danych osobowych, ale o skali tego przetwarzania w dobie ery *big data*, jego nieprzewidywalności z punktu widzenia podmiotów danych, jak również pojawienia się nowych zjawisk, takich jak wspominane profilowanie, przetwarzanie danych w chmurze obliczeniowej, portalach społecznościowych, wykorzystanie danych o lokalizacji, plików *cookies*.

[22] Zob. D. Fleszer, *Zakres przetwarzania danych osobowych w działalności gospodarczej*, Warszawa 2008, s. 112.

[23] *Raport o ochronie danych osobowych*, http://www.giodo.gov.pl/487/id_art/9146/j/pl (dostęp: 5.05.2021 r.).

Już wstępna analiza przedstawionego w publikacji problemu wskazuje, że zagrożenia dla ochrony danych osobowych usługobiorców usług społeczeństwa informacyjnego wynikają m.in. z zastosowania technik profilowania opartych na danych bardzo dobrej jakości oraz ilości danych udostępnianych w trakcie świadczenia z e-usług, korzystania z powyższych usług za pomocą wielu urządzeń podłączonych do internetu, „nałożenia" otrzymanych danych na dane ogólnodostępne w ramach analiz dużych zbiorów danych. W usługach społeczeństwa informacyjnego potencjalnie wszystkie sfery działalności zarówno prywatnej, jak i zawodowej, generują dane osobowe. Te pozornie bezsensowne dane „wytwarzane" podczas korzystania z e-usług mogą być łączone i analizowane przy pomocą zbiorów *big data*, tworząc profil użytkownika. W konsekwencji profile skonstruowane na podstawie danych generowanych przez usługi społeczeństwa informacyjnego są znacznie bardziej szczegółowe, przez co reidentyfikacja profilowanych użytkowników staje się bardzo prawdopodobna. Dodatkowo e-usługi zmieniają w szczególności jakość danych, w tym sensie, że zwiększają zakres obszarów, z których możliwe jest objęcie i wychwycenie danych, co znacząco wpływa na dalsze możliwości łączenia tych danych, jak i wytwarzaniu w oparciu o nie nowych danych. Zjawisko to nazywane jest danetyzacją. Poza wskazanymi powyżej zagrożeniami dla ochrony danych e-usługobiorców, kolejna trudność wiąże się z faktycznym sprawowaniem przez nich kontroli nad swoimi danymi. Usługobiorcy często nie mają świadomości, że ich dane czy zachowania są cały czas zbierane i monitorowane w ramach świadczonej usługi. Rzeczony pogląd zdaje się potwierdzać M. Maras[24], który dostrzega zagrożenia w ograniczonych możliwościach kontroli e-usługobiorców nad swoimi danymi, zwłaszcza w sytuacji, kiedy są one wykorzystywane bez wiedzy lub wbrew woli osoby, której dotyczą. Na wiele zagrożeń dla ochrony danych osobowych – takich jak m.in. utrata kontroli nad swoimi danymi, wykorzystywanie danych w innych celach niż te, do których je zebrano czy profilowanie usługobiorców na podstawie pozornie anonimowych danych – wskazuje

[24] Zob. M. Maras, *Internet of Things: security and privacy implications*, IDPL 2015/2, s. 102.

również W.R. Wiewiórowski[25]. Z kolei, jak zauważa G. Szpor, istotą nowych zagrożeń w dobie rozwoju społeczeństwa informacyjnego jest ograniczenie autonomii informacyjnej, która jest powiązana z utratą kontroli nad przechowywanymi przez nią danymi, obserwowaniem jej działań i próbami sterowania tymi działaniami[26].

Odpowiedzią na powyższe zagrożenia powinny być regulacje prawne, w których zawarte są mechanizmy pozwalające na skuteczną ochronę danych osobowych usługobiorców usług społeczeństwa informacyjnego. W związku z powyższym należy zweryfikować skuteczność regulacji unijnych z zakresu ochrony danych osobowych usługobiorców e-usług. Warto podkreślić, że impulsem do zmiany przepisów i przyjęcia RODO był zarówno rozwój technologii informacyjno-komunikacyjnych, jak i zjawisko globalizacji w wymiarze wymiany i przepływu informacji poprzez internet. W tym nowym otoczeniu cyfrowym usługobiorcy usług społeczeństwa informacyjnego mają prawo do skutecznej kontroli swoich danych osobowych. Dodatkowo zapewnienie wysokiego poziomu ochrony danych osobowych w świecie *online* ma również zasadnicze znaczenie dla zwiększenia zaufania do usług internetowych i wykorzystania potencjału gospodarki cyfrowej, co ma się bezpośrednio przełożyć na pobudzenie wzrostu gospodarczego i zwiększenia konkurencyjności Unii Europejskiej[27]. Zgodnie z wynikami badań Eurobarometru[28] opublikowanymi w 2016 r., zaufanie obywateli do internetu, w tym usług cyfrowych, pozostaje na bardzo niskim poziomie, aż 67% respondentów odpowiedziało, że martwi się faktem, że nie mają kontroli nad informacjami, które podają w internecie. Tylko 15% uznało, że mają pełną kontrolę nad swoimi danymi przetwarzanymi *online*. Ponadto respondenci zgłosili poważne obawy co do konsekwencji gromadzenia,

[25] Więcej W.R. Wiewiórowski, *Ochrona danych osobowych w świecie Internetu przedmiotów* [w:] *Aktualne problemy prawnej ochrony danych osobowych*, red. G. Sibiga, Mon. Praw. – dodatek 2014, s. 9.

[26] G. Szpor, *Internet: Ochrona wolności, własności i bezpieczeństwa*, Warszawa 2011, s. 1.

[27] Zob. specjalna ankieta Eurobarometru nr 359, 06.2011, s. 23.

[28] Zob. Raport Eurobarometru, http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/STANDARD/surveyKy/2098 (dostęp: 5.05.2021 r.).

przetwarzania i wykorzystania ich danych, w szczególności co do ich wykorzystania w celach innych niż ten, dla którego je pierwotnie zebrano.

Pomimo przyjętej w ostatnim czasie reformy ochrony danych osobowych, tj. wejścia w życie RODO, rozwój technologii informacyjno-komunikacyjnych w dalszym ciągu stawia przed nami pytanie odnośnie do aktualności i elastyczności obowiązujących pojęć związanych z ochroną danych osobowych. Powyższe pytanie dotyczy również podmiotów uczestniczących w procesie zarówno przetwarzania danych, świadczenia e-usług, jak i określenia ich wzajemnych relacji. Dotychczasowy podział ról, w związku z przetwarzaniem danych osobowych, na administratora danych i podmiot, którego dane są przetwarzane, może okazać się nieaktualny. Konieczne jest uwzględnienie coraz większej liczby czynników, jak i uczestników biorących udział w przetwarzaniu danych osobowych. Konsekwencje zastosowań rozwiązań technologicznych ze względu na bezprecedensową dotychczas skalę przechowywania, przetwarzania czy transmisji danych, mocy i miniaturyzacji urządzeń, konwergencji mediów czy w końcu dostępu do internetu stanowią wyzwanie dla ochrony danych osobowych w dobie społeczeństwa informacyjnego. Wiąże się to z utrzymaniem swoistej równowagi pomiędzy efektywnością narzędzi technologicznych z jednej strony, a ochroną praw i interesów osób fizycznych, których dane dotyczą, z drugiej strony. Przetwarzanie danych w zbiorach *big data*, jak i zjawisko danetyzacji stanowią najważniejsze z wyzwań współczesnego świata cyfrowego. W obecnych czasach ten ciągły napływ olbrzymiej ilości informacji pochodzących z różnych źródeł wymusza wręcz wprowadzanie i udoskonalanie nowych technik analizy danych przez przedsiębiorców, przy jednoczesnym zapewnieniu optymalnego poziomu ochrony danych osobowych w ramach świadczonych e-usług. Dane osobowe w dobie rewolucji cyfrowej stanowią jedno z najbardziej pożądanych dóbr, które powinny być chronione zarówno przez systemowe gwarancję prawne, jak i odpowiednie zabezpieczenia techniczne. W praktyce może to oznaczać odejście od dotychczasowego „klasycznego" schematu przechowywania i przetwarzania danych osobowych.

3. Problemy badawcze

Przedmiotem niniejszej publikacji jest dokonanie oceny obowiązującego (tj. zgodnego z RODO) modelu ochrony danych osobowych w Unii Europejskiej w kontekście świadczenia usług społeczeństwa informacyjnego.

W związku z powyższym problemem głównym należy również podjąć próbę odpowiedzi na poniższe pytania badawcze:

- *Czy obecny system ochrony prawnej danych osobowych usługobiorców usług społeczeństwa informacyjnego jest wystarczający, biorąc pod uwagę rozwój i wykorzystanie technik informacyjno-komunikacyjnych i czy w związku z tym mamy do czynienia z następczym brakiem odpowiednich środków ochrony prawnej w przedmiotowym zakresie, które nie nadążają za dynamicznie zmieniającym się otoczeniem cyfrowym?*
- *Czy dotychczasowy fundament europejskich standardów ochrony danych osobowych, oparty na koncepcji autonomii informacyjnej jednostki, ulegnie wzmocnieniu poprzez wdrożenie podejścia opartego na ocenie ryzyka (ang. risk based approach)?*
- *Czy w dobie ery big data model ochrony danych osobowych usługobiorców usług społeczeństwa informacyjnego powinien zostać zaktualizowany o nową koncepcję wykorzystania danych osobowych uwzględniającą „tworzenie" nowych danych – tzw. danetyzacja (ang. datafication)?*
- *Czy ryzyko nieuprawnionego przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego związane jest zarówno ze wzrostem ilości przetwarzania danych (w ramach zbiorów big data), jak i ich dalszego łączenia z danymi wysokiej jakości pochodzącymi bezpośrednio od usługobiorców lub wytworzonymi w procesie danetyzacji, które następnie za pomocą zastosowania chociażby technik profilowania mogą prowadzić do reidentyfikacji użytkowników?*

Ponadto, w celu zachowania jasności prezentowanych wywodów, na wstępie każdego z rozdziałów będą definiowane cząstkowe pytania badawcze, które pozwolą na precyzyjne odniesienie się do powyższych pytań.

4. Struktura publikacji

Publikacja podzielona została na 8 rozdziałów zgrupowanych w III częściach. Część I odnosi się do podstawowej siatki definicyjnej pojęć i zagadnień związanych z ochroną danych osobowych usługobiorców e-usług, jak i zdefiniowaniem podmiotów uczestniczących w świadczeniu przedmiotowych usług, ich zakresów odpowiedzialności i współdziałania. Rozdział 1 rozpoczynają rozważania na temat prawa do prywatności, jak i historycznego rozwoju prawa do ochrony danych osobowych w Unii Europejskiej. Rozdział 2 poświęcony jest przedstawieniu specyfiki pojęcia danych osobowych w kontekście świadczenia usług społeczeństwa informacyjnego. Omówiona zostanie kwestia aktualności przesłanki identyfikowalności, która stanowi główny determinant definicji danych osobowych. Następnie zaprezentowane zostaną wybrane nowe kategorie danych, w tym identyfikatory internetowe, takie jak: pliki *cookies*, adres IP, *social login*, które zostaną przeanalizowane pod kątem spełnienia kryterium danych osobowych. W dalszej kolejności podejmowane będzie zagadnienie skuteczności technik anonimizacji i pseudonimizacji, w kontekście świadczenia e-usług. W rozdziale 3 szczegółowej analizie poddana zostanie sama definicja usługi społeczeństwa informacyjnego, która następnie zostanie zestawiona z zakresem pojęcia usługi łączności elektronicznej. Rozdział 3 traktuje również o modelu współpracy pomiędzy stronami w ramach świadczenia usług społeczeństwa informacyjnego. Wyjaśnione zostaną zakresy definicyjne podmiotów, zarówno świadczących usługi społeczeństwa informacyjnego, jak i podmiotów przetwarzających dane osobowe w związku z realizacją e-usług.

W części II zidentyfikowane zostaną konkretne zagrożenia dla ochrony danych osobowych usługobiorców na podstawie wybranych usług społeczeństwa informacyjnego. W rozdziale 4 zostanie przedstawiona charakterystyka wybranych usług społeczeństwa informacyjnego,

tj. portali społecznościowych i chmury obliczeniowej. Na tej podstawie została przeprowadzona analiza zagrożeń dla ochrony danych osobowych usługobiorców i wskazanie konkretnych ryzyk. W rozdziale 5 w ramach odrębnego podrozdziału, ze względu na istotę i zakres tematyczny, omówiono technikę profilowania i podejmowania automatyzowanych decyzji w kontekście wykazania zagrożeń dla ochrony danych osobowych użytkowników.

W części III publikacji dokonana zostanie ocena, w jaki sposób przepisy o ochronie danych osobowych wprowadzone RODO odpowiadają na zagrożenia dla ochrony danych osobowych usługobiorców, które zostały zdefiniowane w części II i czy ta odpowiedź prawodawcy europejskiego jest odpowiednia do skali wskazanych ryzyk. Ponadto intencją autorki jest zobrazowanie niedoskonałości rozwiązań ochronnych wprowadzonych przedmiotową regulacją przy jednoczesnym sformułowaniu wniosków *de lege ferenda* odnośnie do minimum, jakie powinno zostać uwzględnione w przyszłych działaniach legislacyjnych, tak aby prawo w odpowiedni sposób reagowało na zidentyfikowane zagrożenia dla ochrony danych osobowych użytkowników i tym samym zapewniło skuteczną ochronę w tym zakresie. W rozdziale 6 zostanie przeprowadzone badanie instytucji kontroli i bezpieczeństwa danych osobowych usługobiorców w oparciu o analizę podstawowych zasad przetwarzania danych osobowych, podejścia opartego na zasadzie ryzyka, które konkretyzuje się poprzez nałożenie na administratora wielu obowiązków i jest związane z zasadą ochrony danych w fazie projektowania, domyślną ochroną danych czy oceną skutków przetwarzania. W dalszej części autorka odniesie się do zakresu terytorialnego zastosowania RODO, co ma szczególne znaczenie zważywszy na fakt, że znakomita większość dostawców e-usług ma swoje siedziby poza Unią Europejską. W rozdziale 7 zostaną przenalizowane możliwości i zasady zastosowania przepisów, które stanowią o legalności przetwarzania danych osobowych w kontekście świadczenia usług społeczeństwa informacyjnego. Ponadto badaniu zostaną poddane instrumenty prawne dotyczące obowiązków informacyjnych usługodawców, jak również uprawnienia przysługujące usługobiorcom. Szczególna uwaga zostanie poświęcona kwestii wyrażenia zgody przez usługobiorcę na przetwarzanie jego danych osobowych, a także zagadnieniu dotyczącemu wyrażenia zgody przez

dziecko w przypadku usług społeczeństwa informacyjnego. Natomiast w rozdziale 8 zbadana zostanie skuteczność środków ochrony prawnej, odpowiedzialności i sankcji wprowadzonych RODO z perspektywy zagrożeń dla ochrony danych osobowych usługobiorców. Publikacja zostanie podsumowana wnioskami końcowymi.

5. Zakres przedmiotowy

Ze względu na mnogość usług społeczeństwa informacyjnego analiza zagrożeń ochrony danych osobowych usługobiorców musi zostać ograniczona w ocenie autorki do najbardziej reprezentatywnych e-usług, tj. chmury obliczeniowej oraz portali społecznościowych[29]. Powyższy wybór zdają się potwierdzać badania Eurostatu, z których wynika, że tylko w 2017 r.[30] 35% wszystkich użytkowników internetu w Europie korzystało z usług chmury obliczeniowej, co stanowi wzrost o 8% w świadczeniu tej usługi w porównaniu w rokiem 2014. Z kolei w 2019 r.[31] użytkowników internetu, którzy korzystali z serwisów społecznościowych, było ponad 54%. Wybrane usługi społeczeństwa informacyjnego stanowią na tyle reprezentatywny zbiór, że wyjaśnienie i wskazanie zagrożeń dla ochrony danych osobowych na ich przykładzie będzie można odnieść również do innych e-usług. Dodatkowo, aby niejako usprawiedliwić dokonane zawężenie przedmiotowe, należy wskazać, że szczegółowa analiza zagrożeń dla ochrony danych w odniesieniu do wszystkich usług społeczeństwa informacyjnego, ze względu na ich ilość, jak i różnorodność, wydaje się nie tylko niemożliwa, ale również niecelowa. Wynika to z faktu, że ciągle pojawiają się nowe rodzaje e-usług, jak również nowe sposoby i technologie korzystania

[29] Autorka oczywiście ma świadomość, że portale społecznościowe stanowią szczególną postać chmur obliczeniowych i stanowią względem siebie usługi substytucyjne. Natomiast założeniem przy wyborze powyższych usług poza wskaźnikami jakościowymi było wskazanie na unikalne funkcjonalności każdej z powyższych usług i na tej podstawie analizowanie zagrożeń dla ochrony danych osobowych usługobiorców.

[30] Zob. badanie Eurostatu *Statistics in focus 16/2014*, H. Seybert, P. Reinecke, https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=401602 (dostęp: 5.05.2021 r.).

[31] Więcej https://ec.europa.eu/eurostat/databrowser/view/tin00127/default/table?lang=en (dostęp: 5.05.2021 r.).

z nich za pośrednictwem internetu. Z drugiej strony „abstrakcyjna" analiza zagrożeń dla ochrony danych osobowych, tj. bez zaprezentowania charakterystyki chociażby wybranych usług, czyli portali społecznościowych i chmury obliczeniowej, byłaby w ocenie autorki niepełna.

Kolejne zawężenie zakresu przedmiotowego w ramach niniejszej publikacji dotyczy analizy wybranych usług społeczeństwa informacyjnego w oparciu o cyfrowy przekaz treści, które nie podlegają całkowicie lub częściowo na przesyłaniu sygnałów w internecie. Tym samym jedynie uzupełniająco autorka odniesie się do prawa telekomunikacyjnego[32], które nie obejmuje zagadnień związanych z kontrolną treścią usług świadczonych drogą elektroniczną, tj. usług społeczeństwa informacyjnego. Wyjątek stanowić będą technologie *cookies*. Powyższe rozróżnienie wynika z braku jednolitych unormowań prawnych przyjętych na poziomie prawodawstwa europejskiego, tzn. nie został stworzony jeden spójny system, który regulowałby zarówno sposób przesyłania sygnałów w sieci, jak i kwestie dotyczące treści[33]. Został on rozbity na dwie części: pierwsza z nich, będąca przedmiotem niniejszych badań, dotyczy regulacji treści usług społeczeństwa informacyjnego i została unormowana w dyrektywie 2000/31/WE, z kolei druga dotyczy regulacji sposobów przekazywania informacji, nie jest objęta zakresem tematycznym niniejszej publikacji, została uregulowana m.in. w dyrektywie 2002/58/WE, która obecnie jest w trakcie rewizji. Tym samym analizą w ramach niniejszej publikacji nie zostanie objęte badanie skuteczności in-

[32] Zob.: dyrektywa 2002/21/WE z 7.03.2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (Dz.Urz. WE L 108 z 24.04.2002 r., s. 33); dyrektywa 2002/20/WE z 7.03.2002 r. w sprawie zezwoleń na udostępnienie sieci i usługi łączności elektronicznej (Dz.Urz. WE L 108 z 24.04.2002 r., s. 21); dyrektywa 2002/19/WE z 7.03.2002 r. w sprawie dostępu do sieci łączności elektronicznej i urządzeń towarzyszących oraz ich łączenia (Dz.Urz. WE L 108 z 24.04.2002 r., s. 7); dyrektywa 2002/22/WE z 7.03.2002 r. w sprawie usługi powszechnej i praw użytkowników odnoszących się do sieci i usług łączności elektronicznej (Dz.Urz. WE L 108 z 24.04.2002 r., s. 51); dyrektywa 2002/58/WE z 12.07.2002 r. w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz.Urz. WE L 201 z 31.07.2002 r., s. 37); obecnie trwają prace nad projektem rozporządzenia e-privacy.

[33] Więcej P. Polański, *Europejskie prawo handlu elektronicznego...*, s. 104.

strumentów prawnych dotyczących ochrony danych osobowych i ochrony prywatności w sektorze łączności elektronicznej wynikające zarówno z dyrektywy 2002/58/WE, jak i projektu rozporządzenia e-privacy[34].

6. Metodologia

Przyjęta w publikacji metodyka badań opiera się na wykorzystaniu kilku metod badawczych. Zastosowana została głównie metoda dogmatyczna i empiryczna, a także pomocniczo metoda historyczna. Metoda dogmatyczna[35] zostanie wykorzystana do analizy wybranych instrumentów prawnych harmonizujących prawo ochrony danych osobowych. Zakres badań przeprowadzonych tą metodą obejmuje przede wszystkim analizę aktów normatywnych, tj. źródeł prawa Unii Europejskiej, dokumentów urzędowych (m.in. komunikatów Komisji Europejskiej, opinii wyrażanych przez Grupę Roboczą art. 29 – obecnie EROD), poglądy wyrażane w publikacjach naukowych czy regulacje globalnych korporacji. Jako przykład należy wskazać chociażby regulaminy korzystania z e-usług firm takich jak Google czy Facebook. W ten sposób międzynarodowe firmy poprzez wprowadzanie we wszystkich państwach zunifikowanych standardów świadczenia usług kształtują „oryginalne pisane normy pozaprawne o zasięgu globalnym"[36].

W celu dokonania wykładni prawa Unii Europejskiej należy uwzględnić cały dorobek prawny, tj. zarówno teksty źródłowe prawa pierwotnego UE (TUE, TFUE oraz KPP), jak i pochodnego (m.in. obowiązującego rozporządzenia, dyrektyw, decyzji ramowych oraz decyzji), lecz także orzeczeń TSUE (co pozwoli na ustalenie znaczenia przypisywanego poszczególnym przepisom w praktyce). Dodatkowo analizie zostanie poddany dorobek prawny Rady Europy, tj. Europejska Konwencja Praw

[34] Szczegółowa analiza usług łączności elektronicznej na tle usługi społeczeństwa informacyjnego znajduje się w rozdziale 3.

[35] J. Wróblewski, *Metody logiczno-językowe w prawoznawstwie* [w:] *Metody badania prawa*, red. A. Łopatka, Wrocław 1973, s. 47.

[36] J. Jabłońska-Bonca, *Prywatna ochrona bezpieczeństwa. Koncepcje, podmioty, zadania, normy, konteksty*, Warszawa 2017, s. 79.

Człowieka, konwencja nr 108 wraz z protokołami modernizacyjnymi oraz orzecznictwo ETPCz. W ograniczonym zakresie zostanie wykorzystana metoda historyczna do analizy ewolucji pojęcia prawa do prywatności i rozwoju prawa do ochrony danych osobowych.

Część I

OCHRONA DANYCH OSOBOWYCH USŁUGOBIORCÓW USŁUG SPOŁECZEŃSTWA INFORMACYJNEGO – PODSTAWOWE POJĘCIA I ZAGADNIENIA