ACTA UNIVERSITATIS WRATISLAVIENSIS
No 3978
PRZEGLĄD PRAWA I ADMINISTRACJI CXX/1
WROCŁAW 2020
https://doi.org/10.19195/0137-1134.120.22

SYLWIA KOTECKA-KRAL
ORCID: 0000-0002-4425-805X
Uniwersytet Wrocławski
Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej

POSTULATY *DE LEGE FERENDA* DOTYCZĄCE OCHRONY PRYWATNOŚCI UŻYTKOWNIKÓW USŁUG *OVER-THE-TOP* W UNII EUROPEJSKIEJ

Abstrakt: Niniejsze opracowanie omawia problematykę nieistnienia wystarczającej regulacji prawnej ochrony prywatności w tak zwanych usługach *Over-the-Top*, czyli świadczonych ponad Internetem, na szczeblu Unii Europejskiej. Przedstawiono w nim propozycje *de lege ferenda* dla postulowanego aktu prawnego o randze rozporządzenia, które zastąpi nieprzystającą do realiów technologicznych dyrektywę 2002/58 oraz uzupełni postanowienia RODO w zakresie ochrony jednego z praw podstawowych, jakim jest prawo do prywatności.

Słowa kluczowe: prawo do prywatności, ochrona prywatności, dyrektywa 2002/58, RODO, dane osobowe, usługa łączności elektronicznej, usługa *Over-the-Top*, usługa łączności interpersonalnej

1. ZARYS PROBLEMATYKI I CEL OPRACOWANIA

Cyfryzacja gospodarki postępuje coraz szybciej. Technologie informacyjno-komunikacyjne nie stanowią już specyficznego sektora, lecz są podstawą wszystkich nowoczesnych, innowacyjnych systemów gospodarczych i społeczeństw. Dane elektroniczne przetwarzane w systemach informatycznych mogą przynieść ogromne korzyści, jeżeli podda się je analizie lub połączy z usługami i produktami. Jednocześnie szybki rozwój gospodarki opartej na danych oraz nowo powstające technologie, takie jak sztuczna inteligencja, produkty i usługi tak zwanego Internetu rzeczy, systemy autonomiczne, sieci 5G i *Big Data*, stwarzają nowe wyzwania prawne dotyczące kwestii dostępu do danych i ich ponownego wykorzystywania, odpowiedzialności, etyki oraz solidarności[1].

[1] Unijny ustawodawca dostrzegł zmiany technologiczne; zob. motyw 1 preambuły rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 roku w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz.Urz. UE seria L, Nr 303 z 28.11.2018 r., s. 59).

Władza rynkowa niektórych dostawców usług internetowych, które w wysoce nietransparentny sposób pozyskują ogromne ilości danych, także osobowych, rodzi wiele obaw, związanych między innymi z brakiem informacji co do sposobu wykorzystania tych danych i podmiotów, którym dane są dalej przekazywane[2]. Techniki śledzenia i profilowania użytkowników usług świadczonych za pomocą technologii informacyjno-komunikacyjnych, do których zaliczają się usługi *Over-the-Top*, stają się coraz bardziej powszechne i inwazyjne, nie oszczędzając żadnej sfery życia prywatnego. Treść, ale i metadane komunikacji elektronicznej mogą bowiem zawierać dane chronione, takie jak osobiste doświadczenia i uczucia osób zaangażowanych w wymianę informacji po ich stan zdrowia, orientację seksualną i poglądy polityczne, których ujawnienie mogłoby spowodować stratę ekonomiczną lub naruszenie dóbr osobistych. Do metadanych zalicza się między innymi wybierane numery telefonów, odwiedzane strony internetowe, lokalizację geograficzną, a także godzinę, datę i czas trwania połączenia; pozwalają one na wyciągnięcie konkretnych wniosków dotyczących prywatnego życia osób zaangażowanych w komunikację elektroniczną, takich jak ich relacje towarzyskie, zwyczaje, aktywności codziennego życia czy zainteresowania. Z metadanych — w połączeniu z informacjami o tym, w jaki sposób określona osoba korzystała na przykład z aplikacji mobilnej — powstaje dokładny profil użytkownika usług łączności elektronicznej, obejmujący również jego cechy osobowości. Takie dane mają niejednokrotnie wrażliwy charakter i głęboko ingerują w prywatność, co zostało potwierdzone wprost przez Trybunał Sprawiedliwości UE[3]. Kojarzeniem tego typu danych osobowych, lecz także nieosobowych[4], poza kontrolą podmiotów, których dane dotyczą, zainteresowani są nie tylko dostawcy usług łączności elektronicznej czy potencjalni pracodawcy, ale też partie polityczne. Większość wydawców mediów internetowych i podmiotów zajmujących się marketingiem nie zamierza zrezygnować z reklamy targetowanej[5], stawia więc użytkowników usług łączności elektronicznej przed nieuczciwym wyborem — albo wyrażą zgo-

[2] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów — Strategia jednolitego rynku cyfrowego dla Europy, COM(2015) final, s. 13 (dalej: Strategia).

[3] Zob. wyrok TSUE z dnia 8 kwietnia 2014 roku w sprawach połączonych C-293/12 i C-594/12 *Digital Rights Ireland* i *Seitlinger i inni*, pkt 39; wyrok TSUE z dnia 21 grudnia 2016 roku w sprawach połączonych C-203/15 oraz C-698/15 *Tele2 Sverige AB* i *Secretary of State for the Home Department.*

[4] Definicja legalna pojęcia „dane" znajduje się w art. 3 pkt 1 rozporządzenia 2018/1807. „Dane" oznaczają dane inne niż osobowe, zdefiniowane w art. 4 pkt 1 RODO.

[5] O pojęciach: reklamy behawioralnej, reklamy kontekstowej, reklamy segmentowej, reklamy targetowanej zob. S. Kotecka-Kral, *Zagrożenia związane z przetwarzaniem danych osobowych osób fizycznych w celu profilowania*, [w:] Ius est ars boni et aequi. *Księga pamiątkowa dedykowana Profesorowi Józefowi Frąckowiakowi*, red. A. Dańko-Roesler *et al.*, Wrocław 2018, s. 563–564. Zob. także opinia Grupy Roboczej Art. 29 nr 2/2010 (WP 171) w sprawie internetowej reklamy behawioralnej, przyjęta dnia 22 czerwca 2010 roku.

dę na śledzenie i profilowanie w celu otrzymywania takiej reklamy, albo nie będą mieć możliwości korzystania z usług elektronicznych świadczonych przez tych przedsiębiorców (podejście *take it or leave it*)[6].

Obecnie obowiązująca dyrektywa Parlamentu Europejskiego i Rady nr 2002/58/WE z dnia 12 lipca 2002 roku dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[7] miała na celu zapewnienie ochrony podstawowych praw i wolności, w szczególności poszanowania życia prywatnego, poufności komunikacji oraz ochrony danych osobowych w sektorze łączności elektronicznej. Od czasu ostatniego przeglądu tej dyrektywy, dokonanego w 2009 roku, doszło jednak do ważnych zmian technologicznych i gospodarczych. Konsumenci i przedsiębiorstwa w coraz większym stopniu zamiast na tradycyjnych usługach łączności polegają na nowych, opartych na Internecie usługach umożliwiających komunikację międzyludzką, takich jak usługi telefonii internetowej (*Voice over IP*, *VoIP*), komunikatory internetowe czy usługi poczty elektronicznej. Tymczasem przedmiotowym zakresem zastosowania dyrektywy 2002/58 nie są objęte kwestie ochrony prywatności w elektronicznych usługach łączności interpersonalnej, czyli tak zwanych usługach *Over-the-Top* (dalej: *OTT*).

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)[8], które stosuje się od 25 maja 2018 roku, zawiera także normy prawne ustanawiające obowiązki respektowania prywatności użytkowników usług *OTT* (a nie tylko tych, które polegają na przekazywaniu sygnałów w publicznych sieciach łączności), chociażby w postaci obowiązków administratorów związanych z zastosowaniem ochrony danych w fazie projektowania i domyślnej ochrony danych. RODO zapewnia ochronę danych osobowych żyjących osób fizycznych, z kolei dyrektywa 2002/58 — poufność komunikacji, która może zawierać również dane nieosobowe oraz dane dotyczące nie tylko osób fizycznych.

Europejski legislator dostrzegł konieczność uchwalenia aktu prawnego mającego uregulować praktyki branży internetowej coraz głębiej ingerujące w prywatność użytkowników, takie jak na przykład finansowanie usług łączności elektronicznej przez zyski z komercjalizacji danych osobowych czy wszechobecność inteligentnych sensorów oraz przedmiotów codziennego użytku komunikującego się z Internetem. W styczniu 2017 roku Komisja Europejska przyjęła wniosek o rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia

[6] Szerzej zob. K. Szymielewicz, K. Iwańska, *Śledzenie i profilowanie w sieci. Jak z klienta stajesz się towarem*, raport Fundacji Panoptykon (styczeń 2019), https://panoptykon.org/sites/default/files/publikacje/panoptykon_raport_o_sledzeniu_final.pdf (dostęp: 7.05.2020).

[7] Dz.Urz. UE seria L, Nr 201 z 31.07.2002 r., s. 37.

[8] Dz.Urz. UE seria L, Nr 119 z 4.05.2016 r., s. 1 (dalej: RODO).

prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej, tak zwane rozporządzenie *ePrivacy*)[9], określane „młodszą siostrą RODO". Przyjęcie wniosku było jednym z działań przewidzianych w „Strategii jednolitego rynku cyfrowego", mających na celu wzmocnienie zaufania i zwiększenie bezpieczeństwa na tym rynku. Projektowane rozporządzenie *ePrivacy* miało uszczegółowić RODO i uzupełnić je w kwestii danych pochodzących z łączności elektronicznej, które można zakwalifikować jako dane osobowe. Projekt rozporządzenia *ePrivacy* został jednak odrzucony 27 listopada 2019 roku.

W niniejszym opracowaniu pokrótce zostaną przedstawione powody, dla których europejski legislator powinien ponownie podjąć prace nad odrębnym aktem prawnym dotyczącym ochrony prywatności w dobie szybko zmieniającej się technologii umożliwiającej komunikację elektroniczną i wzrastającej ilości danych krążących w globalnej sieci. Obowiązujące regulacje związane z ochroną danych osobowych są bowiem niewystarczające. Opracowanie zawiera także postulaty *de lege ferenda* co do regulacji z zakresu ochrony prywatności w usługach łączności elektronicznej *Over-the-Top*.

2. UZASADNIENIE KONIECZNOŚCI UCHWALENIA ODRĘBNEJ LEGISLACJI W ZAKRESIE *ePRIVACY*

Obecnie obowiązująca dyrektywa 2002/58 zapewnia ochronę podstawowych praw i wolności, w szczególności poszanowania życia prywatnego, poufności komunikacji oraz ochrony danych osobowych. Gwarantuje również swobodny przepływ danych, sprzętu i usług związanych z łącznością elektroniczną w Unii. Stanowi wdrożenie do prawa wtórnego Unii prawa podstawowego, jakim jest poszanowanie życia prywatnego, w odniesieniu do komunikowania się, przewidzianego w art. 7 Karty Praw Podstawowych[10]. Pojęcie „komunikowanie się", użyte w treści art. 7 KPP, dotyczy wszelkich form technicznego przekazywania wiadomości, w szczególności obejmuje rozmowy telefoniczne, wymianę poczty elektronicznej i informacji „internetowych"[11]. Skuteczna ochrona poufności komunikacji jest kluczowa do korzystania z prawa wolności wypowiedzi i informacji oraz innych powiązanych praw, takich jak prawo do ochrony danych osobowych bądź wolność myśli, sumienia i religii.

[9] COM(2017) 10 final, 2017/0003 (COD) (dalej: projekt rozporządzenia *ePrivacy*).

[10] Dz.Urz. UE seria C, Nr 326 z 26.10.2012 r., s. 391 (dalej: KPP). Zob. także art. 8 Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności, sporządzonej w Rzymie dnia 4 listopada 1950 roku, zmienionej następnie protokołami nr 3, 5 i 8 oraz uzupełnionej protokołem nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284) i art. 17 Międzynarodowego paktu praw obywatelskich i politycznych, otwartego do podpisu w Nowym Jorku dnia 16 grudnia 1966 roku (Dz.U. z 1977 r. Nr 38, poz. 167).

[11] Szerzej zob. W. Sobczak, *Komentarz do art. 7*, [w:] *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, red. A. Wróbel, Warszawa 2013/Legalis, nb 23.

2.1. POJĘCIE USŁUGI *OVER-THE-TOP*

Konsumenci i przedsiębiorstwa w coraz większym stopniu zamiast na tradycyjnych usługach łączności polegają na nowych, opartych na Internecie usługach umożliwiających komunikację międzyludzką, takich jak usługi telefonii internetowej, komunikatory internetowe czy usługi poczty elektronicznej. Usługa *Over-the-Top* to usługa świadczona „ponad siecią"[12], polegająca na dostarczaniu zawartości (*content*), usług (*services*) lub aplikacji (*applications*) za pośrednictwem Internetu bez bezpośredniego zaangażowania dostawcy usługi dostępu do sieci. Według niektórych źródeł usługa *OTT* musi być rzeczywiście lub potencjalnie substytucyjna dla tradycyjnej usługi telekomunikacyjnej[13]. Odpłatność usługi nie wpływa przy tym na jej status jako usługi *OTT*.

Organ Europejskich Regulatorów Łączności Elektronicznej (BEREC) zaproponował podstawowy podział usług *OTT* na trzy kategorie: OTT-0, czyli usługa *OTT*, która jest jednocześnie usługą telekomunikacyjną, OTT-1 — usługa *OTT*, która ma lub potencjalnie może być substytucyjna dla usługi telekomunikacyjnej, a także OTT-2, oznaczająca usługę, która nie ma odpowiadającej jej usługi telekomunikacyjnej[14]. Do przykładowych usług *OTT* należy zaliczyć usługi audialne (na przykład Spotify, Deezer), audiowizualne (chociażby Hulu i Netflix) oraz usługi łączności (Facebook Messenger czy Skype).

Usługi łączności *OTT* zasadniczo nie są objęte unijnymi ramami dotyczącymi łączności elektronicznej, w tym dyrektywą 2002/58. Stosuje się ją bowiem do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności. Zgodnie z definicją zawartą w dyrektywie 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 roku w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa)[15], do której odsyła dyrektywa 2002/58 w zakresie definicyjnym, pojęcie „usługa łączności elektronicznej" oznacza usługę zazwyczaj świadczoną za wynagrodzeniem, polegającą całkowicie lub częściowo na przekazywaniu sygnałów w sieciach łączności elektronicznej, w tym usługi telekomunikacyjne i usługi transmisyjne świadczone poprzez sieci nadawcze; nie obejmuje jednak usług związanych z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci lub usług łączności elektronicznej. Spod zakresu tej definicji wyłączone są usługi społeczeństwa informacyjnego w rozumieniu art. 1 dyrektywy 98/34/WE, jeżeli nie polegają one całkowicie lub częściowo na przeka-

[12] Zob. *Regulating electronic communications — A level playing field for telecoms and OTTs?*, s. 2, http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/586641/EPRS_BRI%282016%29586641_EN.pdf (dostęp: 7.05.2020).

[13] Zob. *Economic Impact of OTTs, Technical Report 2017*, https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ECOPO-2017-PDF-E.pdf (dostęp: 7.05.2020).

[14] Zob. *Report on OTT services*, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services (dostęp: 7.05.2020).

[15] Dz.Urz. UE seria L, Nr 108 z 24.04.2002 r., s. 33.

zywaniu sygnałów w sieciach łączności elektronicznej. Z kolei „publiczna sieć łączności" to sieć łączności elektronicznej wykorzystywana całkowicie lub częściowo do świadczenia publicznie dostępnych usług łączności elektronicznej.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 roku ustanawiająca Europejski kodeks łączności elektronicznej[16] jednoznacznie kwalifikuje jako usługi telekomunikacyjne takie usługi *OTT*, które spełniają kryteria usługi łączności interpersonalnej, to znaczy usługi umożliwiające interpersonalną i interaktywną wymianę informacji, w tym połączenia głosowe między dwiema osobami, wszystkie rodzaje poczty elektronicznej, usługi przekazywania wiadomości lub czatów grupowych. Oznacza to, że usługi te będą traktowane tak samo jak tradycyjne usługi łączności elektronicznej, czyli usługi telekomunikacyjne[17]. Z punktu widzenia użytkownika końcowego nie ma jednak znaczenia, czy dostawca sam przekazuje sygnały lub czy łączność jest zapewniona za pośrednictwem usługi dostępu do Internetu.

Pojęcie usługi łączności elektronicznej zdefiniowano w art. 2 pkt 2 EKŁE jako usługę zazwyczaj świadczoną za wynagrodzeniem za pośrednictwem sieci łączności elektronicznej, która obejmuje, z wyjątkiem usług związanych z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci lub usług łączności elektronicznej, następujące rodzaje usług: po pierwsze, „usługę dostępu do Internetu", zdefiniowaną w art. 2 akapit drugi pkt 2 rozporządzenia (UE) 2015/2120[18]; po drugie, „usługę łączności interpersonalnej"; oraz po trzecie, usługi polegające całkowicie lub częściowo na przekazywaniu sygnałów, takie jak usługi transmisyjne stosowane na potrzeby świadczenia usług łączności maszyna–maszyna oraz na potrzeby nadawania. Z kolei usługa łączności interpersonalnej to usługa zazwyczaj świadczona za wynagrodzeniem, która umożliwia bezpośrednią interpersonalną i interaktywną wymianę informacji za pośrednictwem sieci łączności elektronicznej między skończoną liczbą osób, w ramach której osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy

[16] Dz.Urz. UE seria L, Nr 321 z 17.12.2018 r., s. 36 (dalej: EKŁE).

[17] Zgodnie z brzmieniem motywu 15 preambuły EKŁE, aby zapewnić skuteczną i równą ochronę użytkowników końcowych i ich praw w kontekście korzystania z funkcjonalnie równoważnych usług, definicji usług łączności elektronicznej nie należy opierać wyłącznie na parametrach technicznych, lecz na podejściu funkcjonalnym. Chociaż „przekazywanie sygnałów" pozostaje istotnym parametrem określania usług wchodzących w zakres dyrektywy 2018/1972, definicja usług łączności elektronicznej powinna obejmować również inne usługi umożliwiające komunikację.

[18] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 roku ustanawiające środki dotyczące dostępu do otwartego Internetu oraz zmieniające dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenie (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii (Dz.Urz. UE seria L, Nr 310 z 26.11.2015 r., s. 1). Zgodnie z jego brzmieniem „usługa dostępu do Internetu" oznacza publicznie dostępną usługę łączności elektronicznej, która zapewnia dostęp do Internetu, a tym samym łączność z praktycznie wszystkimi zakończeniami sieci Internetu, bez względu na stosowaną technologię sieci i urządzenia końcowe.

lub odbiorcach, natomiast nie obejmuje ona usług, które umożliwiają interpersonalną i interaktywną komunikację wyłącznie jako podrzędną funkcję dodatkową, która jest nieodłącznie związana z inną usługą.

2.2. DYREKTYWA 2002/58 A OCHRONA PRYWATNOŚCI W PRZEPISACH RODO

Przetwarzanie danych osobowych przez dostawców usług łączności elektronicznej, czy to w ramach wynagrodzenia, czy na innej zasadzie, powinno być zgodne z RODO. Dyrektywa 2002/58 zapewnia poufność komunikacji, która może zawierać również dane nieosobowe oraz dane dotyczące osób prawnych i innych jednostek organizacyjnych.

Przepisy RODO nałożyły na dostawców usług łączności elektronicznej obowiązek ujawnienia wszystkich podmiotów, którym przekazują dane użytkowników, i pozostawienie decyzji użytkownikom w kwestii zgody na śledzenie ich aktywności w Internecie w celach reklamowych. W praktyce sprowadza się to do stosowania plików *cookies*[19] (a także ich zapisywania w przeglądarce internetowej użytkownika) lub skryptów śledzących. Niektórych rodzajów plików *cookies* nie można jednak wyłączyć bez szkody dla korzystania z usługi łączności elektronicznej; w pewnych wypadkach niewyrażenie zgody na ich zainstalowanie oznacza niemożliwość skorzystania z usługi. W zależności od tego, czy istnieje możliwość uznania śledzenia zachowania użytkownika za zgodne z racjonalnymi oczekiwaniami i nieingerujące nadmiernie w prywatność użytkowników, przepisy RODO dopuszczają stosowanie zarówno modelu *opt out* (użytkownik może się sprzeciwić technikom śledzącym), jak i *opt in* (użytkownik musi wyrazić zgodę na śledzenie). Większość polskich dostawców usług łączności elektronicznej przyjęła model oparty na pozyskiwaniu zgody użytkowników, ale w praktyce tak zaprojektowany, aby trudno było — przez nieuwagę albo w wyniku narastającej frustracji użytkownika, spowodowanej wyskakującymi na ekranie urządzenia końcowego komunikatami — zgody nie udzielić. W wyniku zastosowania takiego technicznego rozwiązania każda czynność użytkownika, od zamknięcia okienka zawierającego informację o plikach *cookies* po przejście do serwisu, jest traktowana jako zaakceptowanie narzuconych reguł[20]. Takie postępowanie nie jest zgodne z obowiązującymi przepisami prawa[21].

---

[19] Zob. np. rodzaje plików *cookies* używanych przez Google w witrynach i usługach reklamowych: https://policies.google.com/technologies/types?hl=pl (dostęp: 7.05.2020).

[20] Szerzej zob. np. *Zgoda wyinterpretowana z niejednoznacznego działania (np. używania serwisu)*, https://panoptykon.org/wiadomosc/zgoda-wyinterpretowana-z-niejednoznacznego-dzialania-np-uzywania-serwisu (dostęp: 7.05.2020); *RODO na tacy. Sezon II: Subiektywny przegląd (złych i dobrych) praktyk*, https://panoptykon.org/rodo-na-tacy-sezon-ii (dostęp: 7.05.2020); *Zgoda domyślna*, https://panoptykon.org/wiadomosc/zgoda-domyslna (dostęp: 7.05.2020); *Zgoda wymuszona*, https://panoptykon.org/wiadomosc/zgoda-wymuszona (dostęp: 7.05.2020).

[21] Zob. art. 4 pkt 11, art. 7 i art. 8 RODO oraz wytyczne Grupy Roboczej Art. 29 dotyczące zgody na mocy rozporządzenia 2016/679, przyjęte 28 listopada 2017 roku (WP 259). Z tego powodu bardziej świadomi użytkownicy coraz częściej instalują oprogramowanie blokujące reklamy lub wy-

RODO zawiera także regulacje wzmacniające ochronę prywatności[22]. Aby móc wykazać przestrzeganie przepisów RODO, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania — zwaną też zasadą uwzględniania ochrony prywatności w fazie projektowania (ang. *privacy by design*) oraz z zasadą domyślnej ochrony danych — nazywaną również zasadą domyślnej ochrony prywatności (ang. *privacy by default*).

Podczas 32. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności, która odbywała się w dniach 27–29 października 2010 roku w Jerozolimie, przyjęto Rezolucję w sprawie prywatności w fazie projektowania[23]. Wymienia ona siedem podstawowych zasad, które zostały oderwane od pojęcia teleinformatyki; uznano bowiem, że dotyczą raczej zarządzania organizacją (prywatną lub publiczną) niż zarządzania systemem informatycznym lub projektem biznesowym. Zasady te są następujące:

1. podejście proaktywne, a nie reaktywne i podejście zaradcze, a nie naprawcze;
2. prywatność jako ustawienia domyślne;
3. prywatność włączona w projekt;
4. pełna funkcjonalność rozumiana jako osiąganie sumy dodatniej, a nie sumy zerowej;
5. ochrona prywatności od początku do końca cyklu życia informacji;
6. transparentność i przejrzystość;
7. poszanowanie dla prywatności użytkowników.

Aby wprowadzić je w życie, należy także przeprowadzić: ocenę skutków przedsięwzięć dla ochrony prywatności (ang. *privacy impact assesment — PIA*), prowadzić ciągłą analizę ryzyka, analizę luk, ocenę zagrożeń, zarządzanie ryzykiem, audyt, certyfikację i homologację oraz przygotować materiały szkoleniowe dla członków organizacji[24].

---

bierają wyszukiwarki i przeglądarki internetowe uniemożliwiające śledzenie. Tym samym aktywnie kontestują model finansowania treści internetowych oparty na komercjalizacji danych i profilowaniu, który w wielu wypadkach prowadzi do naruszenia prywatności, wykluczenia i dyskryminacji, krzywdzącego scoringu, manipulowania emocjami czy wpływania na wyniki wyborów; szerzej zob. S. Kotecka-Kral, *op. cit.*, s. 570–576.

[22] Zob. art. 25 i motyw 78 preambuły RODO.

[23] Tekst rezolucji: http://privacyconference2011.org/htmls/adoptedResolutions/2010_Jerusalem/2010_J5.pdf (dostęp: 7.05.2020).

[24] Szerzej zob. W. Wiewiórowski, Privacy by Design *jako paradygmat ochrony prywatności*, [w:] *Prawno-informatyczne problemy sieci, portali i e-usług*, red. G. Szpor, W. Wiewiórowski, Warszawa 2012, s. 13–29; M. Susałko, *Ochrona danych w fazie projektowania i domyślna ochrona danych*, [w:] *RODO w e-commerce*, red. D. Lubasz, Warszawa 2018, s. 162–178; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 25*, [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, P. Barta, M. Kawecki, Warszawa 2018, s. 453–461; D. Lubasz, K. Witkowska-Nowakowska, *Komentarz do art. 25*, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 599–612.

Pomocne dla ochrony prywatności mogą się również okazać przepisy art. 35 RODO, ustanawiające — w sytuacjach, w których dany rodzaj przetwarzania, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych — obowiązek przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (ang. *data protection impact assessment*). Ocena skutków ochrony danych jest wymagana zwłaszcza w wypadku systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną[25].

Przepisy RODO ustanawiające zasady dotyczące wysyłania niezamówionych informacji handlowych również okazują się istotne w dzisiejszym świecie. Mogą bowiem stanowić podstawę prawną do skierowania roszczenia odszkodowawczego wobec podmiotu rozsyłającego niezamówioną korespondencję handlową[26], jeżeli wiąże się to z naruszeniem danych osobowych adresata takiej korespondencji[27].

3. POSTULOWANE PODNIESIENIE POZIOMU OCHRONY PRYWATNOŚCI W USŁUGACH *OVER-THE-TOP*

Projektowane rozporządzenie *ePrivacy* miało być specjalną regulacją ustanawiającą nowe standardy ochrony prywatności w Internecie. W niniejszym opracowaniu postawiono tezę, że skuteczną ochronę prawa do prywatności powinien zapewniać oddzielny instrument prawny, który będzie podwyższać w stosunku do przepisów RODO poziom ochrony prywatności użytkowników usług łączności elektronicznej w odpowiedzi na coraz bardziej zaawansowane techniki śledzenia stosowane przez dostawców tych usług. Internetu i technologii cyfrowych granice nie dotyczą, wymiar problemu wykracza poza terytorium poszczególnych państw członkowskich UE. Przetwarzanie danych osobowych i nieosobowych pochodzących z łączności elektronicznej przez dostawców usług łączności elektronicznej

[25] Szerzej zob. wytyczne Grupy Roboczej Art. 29 przyjęte 4 kwietnia 2017 roku, ostatnio zmienione i przyjęte 4 października 2017 roku, dotyczące skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/676 (WP 248 rev.01).

[26] Zob. art. 82 RODO.

[27] W polskim systemie prawnym zagadnienie przesyłania niezamówionej informacji handlowej regulowane jest także w art. 172 ustawy z dnia 16 lipca 2004 roku — Prawo telekomunikacyjne (tekst jedn. Dz.U. z 2019 r. poz. 2460) i w art. 10 ustawy z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (tekst jedn. Dz.U. z 2019 r. poz. 123 ze zm.). Mnogość przepisów sprawia, że odpowiedzialność za wysyłanie spamu rozmywa się, co utrudnia walkę z tym zjawiskiem.

powinno być dozwolone jedynie zgodnie z postulowanym aktem prawa UE, zwanym dalej projektem nowego rozporządzenia *ePrivacy*. Poniżej przedstawione zostaną najważniejsze postulaty *de lege ferenda* dotyczące zakresu regulacji kwestii ochrony prawa do prywatności w usługach *Over-the-Top*. Zostały one oparte między innymi na analizie treści projektowanego rozporządzenia *ePrivacy*, zmieniającej się w czasie procesu legislacyjnego, który ostatecznie zakończył się odrzuceniem tego projektu pod koniec 2019 roku. Do zagadnień tych należą: zakres zastosowania nowego aktu prawnego, podstawy prawne przetwarzania danych pochodzących z łączności elektronicznej, regulacja plików *cookies*, *cookie-walls*, zgoda na śledzenie i centralizacja zgody w przeglądarce internetowej.

3.1. CEL I ZAKRES ZASTOSOWANIA PROJEKTU NOWEGO ROZPORZĄDZENIA *ePRIVACY*

Postulowany projekt nowego rozporządzenia *ePrivacy* powinien wprowadzać przejrzyste zasady ochrony danych i poufności komunikacji, sprzyjające rozwojowi modeli biznesowych opartych na zaufaniu i poszanowaniu autonomii informacyjnej użytkowników. Nowe rozporządzenie powinno uwzględniać perspektywę dalszego rozwoju narzędzi technologicznych umożliwiających głęboką ingerencję w prywatność, takich jak skrypty śledzące czy inteligentne sensory, i uwzględniać związane z tym ryzyka.

Przepisy nowego rozporządzenia *ePrivacy* powinny obejmować zarówno dane osobowe, jak i nieosobowe użytkowników usług łączności elektronicznej. Dane osobowe powinny być rozumiane tak jak w przepisach RODO, natomiast za dane nieosobowe powinny zostać uznane dane, których nie można zaliczyć do katerogii danych osobowych. Co ważne, ochroną powinna zostać objęta nie tylko sama treść komunikacji elektronicznej, lecz także jej metadane[28].

Nowe rozporządzenie *ePrivacy* powinno mieć zastosowanie do użytkowników końcowych będących zarówno osobami fizycznymi, jak i prawnymi. Pojęcie zgody użytkownika końcowego powinno być rozumiane tak jak w przepisach RODO[29]. Nowe rozporządzenie *ePrivacy* powinno również znaleźć zastosowanie

[28] Metadane są obecnie bardzo często wykorzystywane ponad miarę — zbierane są nie tylko te informacje, które są niezbędne do świadczenia usługi, lecz także takie, które służą przedsiębiorcom do budowania profili użytkowników i wykorzystywania ich w celach marketingowych, nierzadko wbrew woli i poza jakąkolwiek kontrolą użytkownika; zob. *Uwagi Fundacji Panoptykon z dnia 8.03.2018 r. w sprawie noty Prezydencji dotyczącej prac nad projektem rozporządzenia w sprawie prywatności i łączności elektronicznej*, s. 1, https://panoptykon.org/sites/default/files/stanowiska/panoptykon_mc_stanowisko_eprivacy_8.03.2018.pdf (dostęp: 7.05.2020).

[29] Zob. art. 4 pkt 11 RODO — zgoda osoby, której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych; zob. także wytyczne Grupy Roboczej Art. 29 dotyczące zgody na mocy rozporządzenia 2016/679, przyjęte 28 listopada 2017 roku (WP 259).

do osób fizycznych i prawnych, które korzystają z usług łączności elektronicznej, aby wysyłać materiały handlowe do celów marketingu bezpośredniego lub gromadzić informacje związane z urządzeniem końcowym użytkowników końcowych bądź przechowywane na takim urządzeniu. Organy nadzorcze powinny odpowiadać ponadto za monitorowanie stosowania nowego rozporządzenia *ePrivacy* w stosunku do osób fizycznych i prawnych, a osobom prawnym powinny przysługiwać takie same prawa w kwestii organów nadzorczych jak użytkownikom końcowym będącym osobami fizycznymi.

Aby zapewnić skuteczną i równą ochronę użytkowników końcowych podczas korzystania z usług równoważnych pod względem funkcjonalnym, projekt nowego rozporządzenia *ePrivacy* powinien odwołać się do definicji usług łączności elektronicznej zawartej EKŁE. Ochrona poufności komunikacji jest kluczowa również w odniesieniu do usług łączności interpersonalnej, które są usługami pomocniczymi względem innej usługi. Tego rodzaju usługi, które mają też funkcję komunikacyjną, powinny być zatem objęte projektem nowego rozporządzenia *ePrivacy*. Nowy akt prawny powinien mieć zastosowanie do dostawców usług łączności elektronicznej, dostawców publicznie dostępnych spisów numerów oraz dostawców oprogramowania umożliwiającego łączność elektroniczną, łącznie z odzyskiwaniem i przedstawianiem informacji w Internecie. Przedmiotowym zakresem zastosowania nowego rozporządzenia *ePrivacy* powinno zostać objęte przetwarzanie danych pochodzących z łączności elektronicznej prowadzonej w związku ze świadczeniem usług łączności elektronicznej i korzystaniem z tych usług oraz informacji związanych z urządzeniem końcowym użytkowników końcowych.

Rozporządzenie winno mieć zastosowanie do danych pochodzących z łączności elektronicznej przetwarzanych w związku z zapewnieniem i zastosowaniem usług łączności elektronicznej w Unii, niezależnie od tego, czy przetwarzanie odbywa się na jej terytorium. Ponadto, aby uniknąć pozbawienia użytkowników końcowych w Unii skutecznej ochrony, rozporządzenie powinno mieć zastosowanie również do danych pochodzących z łączności elektronicznej przetwarzanych w związku ze świadczeniem użytkownikom końcowym w Unii usług łączności elektronicznej pochodzących spoza Wspólnoty.

3.2. PODSTAWY PRAWNE PRZETWARZANIA DANYCH POCHODZĄCYCH Z ŁĄCZNOŚCI ELEKTRONICZNEJ

3.2.1. UZASADNIONY INTERES ADMINISTRATORA

Należy zgłosić postulat *de lege ferenda* rezygnacji w projekcie nowego rozporządzenia *ePrivacy* z podstawy prawnej przetwarzania danych pochodzących z łączności elektronicznej, opartej na uzasadnionym interesie administratora[30].

[30] Taka podstawa prawna przetwarzania danych osobowych znajduje się w art. 6 ust. 1 lit. f) RODO.

Zamiast tego trzeba bezpośrednio odwołać się do zasad proporcjonalności i minimalizacji danych ujętych w RODO. Oparcie przetwarzania danych pochodzących z łączności elektronicznej na uzasadnionym interesie administratora ma sens w bezpośredniej relacji między podmiotem a administratorem danych, szczególnie kiedy te podmioty łączy stała relacja umowna, umożliwiająca dwustronną komunikację, w tym bezproblemowe wyrażenie sprzeciwu przez podmiot danych. Projekt nowego rozporządzenia *ePrivacy* powinien jednak dotyczyć sytuacji, w których — ze względu na złożoność ekosystemu łączności elektronicznej — często mamy do czynienia z tak zwanymi podmiotami trzecimi, „zaufanymi partnerami" i rozbudowanym łańcuchem pośredników w przekazywaniu danych. Podstawa prawna oparta na uzasadnionym interesie administratora otworzyłaby zatem bardzo szeroko możliwość przetwarzania danych poza kontrolą osób, których te dane dotyczą. Podstawy prawne przetwarzania zarówno metadanych, jak i treści komunikacji powinny być do siebie jak najbardziej zbliżone z uwagi na pojawiające się często wątpliwości, jak zakwalifikować daną informację — czy jako treść komunikacji, czy jako jej metadaną[31].

Wydaje się, że istnieje też potrzeba doprecyzowania lub poszerzenia przesłanek przetwarzania danych w takich celach, jak możliwość świadczenia dodatkowych usług, monitorowanie ruchu na stronie internetowej czy rozliczenie realizowanych usług, także w relacji z podmiotami trzecimi, na przykład w kontekście remarketingu, o ile nie ingeruje to w prywatność użytkowników[32].

Negatywnie należy ocenić także propozycję, pojawiającą się w toku prac legislacyjnych nad projektem rozporządzeniem *ePrivacy*, wprowadzenia możliwości dalszego przetwarzania danych bez zgody użytkownika do celów innych niż te, do których dane zostały pierwotnie zebrane. Rozwiązanie to jest niezgodne z zasadą ograniczenia celu przetwarzania, na której oparte jest RODO. Efektem tej propozycji byłoby wprowadzenie niebezpiecznego wyjątku, który może posłużyć do przetwarzania danych do celów komercyjnych bez zgody użytkownika, zwłaszcza biorąc pod uwagę obecne realia biznesowe i stosowane natarczywe oraz nieprzejrzyste metody śledzenia zachowań użytkowników w sieci. Wprowadzenie możliwości dalszego przetwarzania spowoduje znaczące osłabienie pozycji użytkownika, który — udostępniając przedsiębiorcy dane potrzebne do wykonania usługi — nie będzie w stanie przewidzieć, do jakich celów dane te będą następnie wykorzystywane[33].

---

[31] Zob. *Uwagi Fundacji Panoptykon z dnia 21.11.2017 r. w sprawie propozycji Prezydencji dotyczących projektu rozporządzenia w sprawie prywatności i łączności elektronicznej*, s. 2–3, https://panoptykon.org/sites/default/files/stanowiska/panoptykon_mc_stanowisko_eprivacy_21.11.2017_0.pdf (dostęp: 7.05.2020).

[32] Zob. *ibidem*.

[33] Zob. *Uwagi Fundacji Panoptykon z dnia 15.01.2018 r. w sprawie noty Prezydencji dotyczącej prac nad projektem rozporządzenia w sprawie prywatności i łączności elektronicznej*, s. 1, https://

W jednej z wersji projektu rozporządzenia *ePrivacy* zaproponowano wprowadzenie możliwości dalszego przetwarzania metadanych do innych celów niż te, do których metadane zostały pierwotnie zebrane, ale pod warunkiem spełnienia „testu kompatybilności". Jako przykład podano wykorzystywanie danych o lokalizacji na potrzeby *smart city*, między innymi do zarządzania ruchem. W opisywanej propozycji to jednak sam administrator miałby przeprowadzać test kompatybilności i określać, czy nowy cel przetwarzania danych jest podobny do pierwotnego. Takie ukształtowanie testu kompatybilności *de facto* wprowadza nową podstawę prawną przetwarzania danych w postaci uzasadnionego interesu administratora[34].

3.2.2. OFEROWANIE KORZYSTNIEJSZYCH CEN, PRODUKTÓW I USŁUG

Za stanowczo niewskazane należy uznać wprowadzenie przesłanki umożliwiającej zbieranie metadanych na potrzeby oferowania użytkownikom korzystniejszych cen, produktów i usług, albowiem tak sformułowana podstawa prawna przetwarzania danych rodzi ryzyko nadużyć. Oferowanie użytkownikom korzystniejszych cenowo usług i produktów powinno być możliwe jedynie pod warunkiem uzyskania od nich zgody na przetwarzanie danych osobowych w tym celu[35].

3.3. *COOKIES*, *COOKIE-WALLS*, ZGODA NA ŚLEDZENIE I JEJ CENTRALIZACJA

Istnieją różne typy plików *cookies* — niektóre z nich są niezbędne do technicznego działania usługi łączności elektronicznej, inne są instalowane przez podmioty trzecie na różnych stronach internetowych w celu śledzenia internetowej aktywności użytkownika i tworzenia jego profilu behawioralnego. W projekcie nowego rozporządzenia *ePrivacy* powinien znaleźć się zakaz zapisywania plików śledzących na urządzeniu końcowym użytkownika bez jego zgody. Nie należy przyjmować założenia, zgodnie z którym śledzenie aktywności użytkowników w Internecie w celach reklamowych jest nieodłącznym elementem usług, których źródłem finansowania są dochody z reklam[36]. Oparcie się na twierdzeniu, że re-

panoptykon.org/sites/default/files/stanowiska/panoptykon_mc_stanowisko_eprivacy_15.01.2018.pdf (dostęp: 7.05.2020).

[34] Zob. *Uwagi Fundacji Panoptykon z dnia 13.07.2018 r. w sprawie noty Prezydencji dotyczącej prac nad projektem rozporządzenia w sprawie prywatności i łączności elektronicznej*, s. 1–2, https://panoptykon.org/sites/default/files/stanowiska/panoptykon_mc_stanowisko_eprivacy_13.07.2018.pdf (dostęp: 7.05.2020).

[35] Zob. *Uwagi Fundacji Panoptykon z dnia 8.03.2018*…, s. 2.

[36] Wysoki stopień ingerencji w prywatność technik stosowanych przy dopasowywaniu reklamy behawioralnej wielokrotnie podkreślała Grupa Robocza Art. 29, między innymi w opinii 2/2010 w sprawie internetowej reklamy behawioralnej (WP 171). W tej opinii Grupa stanowczo opowiedziała się za wyraźną zgodą jako podstawą prawną takiego przetwarzania danych. Z kolei w wytycznych w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania (WP 251) Grupa wskazała, że w kontekście reklamy targetowanej może również dochodzić do podejmowania zautomatyzowanych decyzji, o których mowa w art. 22 RODO.

klama targetowana jest integralnym elementem świadczonej usługi, ponieważ pozwala na jej finansowanie, odbiera użytkownikom możliwość sprzeciwu wobec profilowania w celach marketingowych — jedynym wyjściem będzie wówczas rezygnacja z usługi (podejście *take it or leave it*)[37]. Takie rozwiązanie powinno zostać uznane za niedopuszczalne zarówno z punktu widzenia nadmiernej ingerencji w prawo do prywatności, jak i z przewidzianym w RODO wymogiem pozyskiwania świadomej i w pełni dobrowolnej zgody na przetwarzanie danych osobowych[38]. Ustawodawca powinien mieć również na uwadze to, że ekosystem reklamy targetowanej jest wyjątkowo skomplikowany technicznie i nietransparentny[39]. Nawet profilując użytkowników na podstawie zgody, dostawcy usług łączności elektronicznej nie przekazują użytkownikom wystarczających informacji na temat funkcjonowania tych mechanizmów[40].

W projekcie nowego rozporządzenia *ePrivacy* powinien znaleźć się więc wyraźny zakaz ograniczania użytkownikom dostępu do usług łączności elektronicznej w razie niewyrażenia zgody na śledzenie w celach marketingowych, w tym instalację plików *cookies* (tak zwane *cookie-walls*)[41]. Chodzi o sytuację, w której bez wyrażenia przez użytkownika zgody na instalację plików *cookies* niemożliwe jest korzystanie z danej usługi łączności elektronicznej. Ze względu na powszechność stosowania *cookie-walls* i dalekosiężne konsekwencje wymuszania zgody na przetwarzanie danych ten wątek rozważań ma duże znaczenie dla ochrony autonomii informacyjnej użytkowników[42].

Kolejnym zagadnieniem mającym praktyczne znaczenie jest techniczny aspekt wyrażania zgody na istalację plików śledzących dostawcy świadczące-

[37] Zob. K. Szymielewicz, K. Iwańska, *ePrywatność czy eŚledzenie — czy branża reklamowa postawi na swoim?*, https://panoptykon.org/eprivacy-czy-esledzenie (dostęp: 7.05.2020).

[38] W szczególności motyw 42 preambuły RODO stanowi, że „wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji".

[39] O mechanizmie *real-time bidding* zob. K. Szymielewicz, K. Iwańska, *Śledzenie i profilowanie*…, s. 16–24.

[40] Szerzej zob. *Uwagi Fundacji Panoptykon z dnia 24.10.2018 r. w sprawie noty Prezydencji dotyczącej prac nad projektem rozporządzenia w sprawie prywatności i łączności elektronicznej*, s. 1–2, https://panoptykon.org/sites/default/files/stanowiska/panoptykon_mc_stanowisko_eprivacy_24.10.2018.pdf (dostęp: 7.05.2020).

[41] Tymczasem w trakcie prac nad projektem rozporządzenia *ePrivacy* pojawiały się propozycje, których celem była próba wymuszenia na użytkownikach usług łączności elektronicznej wyrażenia zgody na instalację plików *cookies* w dodatkowych celach, przez które należy rozumieć śledzenie i profilowanie użytkowników w celach reklamowych, a nie związanych bezpośrednio ze świadczeniem usługi. Projektowano, że uzależnianie dostępu do usługi łączności elektronicznej od wyrażenia zgody na tego typu pliki *cookies* nie będzie co do zasady uznane za nieproporcjonalne; zob. *Uwagi Fundacji Panoptykon z dnia 13.07.2018*…, s. 1.

[42] Szerzej zob. *Uwagi Fundacji Panoptykon z dnia 21.11.2017*…, s. 3–4; oraz *Uwagi Fundacji Panoptykon z dnia 10.05.2018 r. w sprawie noty Prezydencji dotyczącej prac nad projektem rozporządzenia w sprawie prywatności i łączności elektronicznej*, s. 1, https://panoptykon.org/sites/default/files/stanowiska/panoptykon_mc_stanowisko_eprivacy_10.05.2018.pdf (dostęp: 7.05.2020).

go usługę łączności elektronicznej lub osób trzecich, często nazywanych przez dostawcę zaufanymi partnerami. Jednym z możliwych rozwiązań jest tak zwana centralizacja wyrażania zgody na pliki *cookies* bądź braku akceptacji dla plików *cookies* w oprogramowaniu używanym przez użytkownika, jakim jest przeglądarka internetowa. Scentralizowana zgoda nie powinna pozbawiać dostawców usług łączności elektronicznej możliwości uzyskania zgody w drodze indywidualnych próśb skierowanych do użytkowników końcowych, dzięki czemu utrzymaliby oni swój obecny model biznesowy[43]. Prawodawca unijny powinien przy tym zachęcić przedsiębiorców do stosowania technologii sprzyjających prywatności (tak zwanych *PET*, z ang. *privacy enhancing technologies*), które pozwalałyby użytkownikom kontrolować wyrażone zgody na poziomie przeglądarki[44].

Natomiast negatywnie należy ocenić jedną z przedstawionych w toku prac legislacyjnych nad projektem rozporządzenia *ePrivacy* opcji, zgodnie z którą wymóg uzyskania zgody (*opt in*) na instalację plików *cookies* lub stosowanie innych technik śledzących w sytuacji, gdy ich funkcją jest dostarczanie reklamy targetowanej, należy zastąpić możliwością wyrażenia sprzeciwu przez użytkowników (*opt out*)[45].

Nie należy także dopuszczać do zamieszczania postanowień dotyczących stosowania ciasteczek i podobnych technologii w celach śledzenia i profilowania użytkowników w regulaminach usług łączności elektronicznej, których treści użytkownicy nie mają możliwości negocjować z dostawcami usług. Takie postanowienia regulaminów portali — jako niezgodne z RODO, ponieważ w praktyce wymuszające zgodę na profilowanie — zostały zakwestionowane przed organami nadzorczymi w innych państwach[46].

4. WNIOSKI

Niewątpliwie należy ponownie podjąć prace nad nowym rozporządzeniem *ePrivacy*. RODO nie jest bowiem w stanie wypełnić luki spowodowanej brakiem regulacji chroniącej prywatność użytkowników korzystających z usług *OTT*, a obecnie obowiązująca dyrektywa 2002/58 nie obejmuje swym zakresem zastosowania usług świadczonych ponad siecią. Głównymi korzyściami związanymi z przyjęciem nowego, odrębnego instrumentu prawnego dotyczącego ochrony

[43] Szerzej zob. *Uwagi Fundacji Panoptykon z dnia 25.09.2018 r. w sprawie noty Prezydencji dotyczącej prac nad projektem rozporządzenia w sprawie prywatności i* łączności *elektronicznej*, s. 1, https://panoptykon.org/sites/default/files/stanowiska/panoptykon_mc_stanowisko_eprivacy_25.09.2018.pdf (dostęp: 7.05.2020).

[44] Zob. *ibidem*.

[45] Zob. *Uwagi Fundacji Panoptykon z dnia 15.01.2018*…, s. 1.

[46] Francuski organ nadzorczy CNIL 21 stycznia 2019 roku nałożył na Google karę 50 milionów euro za wymuszanie zgody użytkowników na śledzenie i profilowanie w celach reklamowych podczas korzystania z jego usług; szerzej zob. *Uwagi Fundacji Panoptykon z dnia 24.10.2018*…, s. 2.

prywatności w usługach łączności elektronicznej są między innymi: lepsza ochrona poufności komunikacji elektronicznej przez rozszerzenie zakresu stosowania przedmiotowego instrumentu prawnego w celu uwzględnienia nowych, funkcjonalnie równoważnych usług łączności elektronicznej, wzmocnienie ochrony przed niezamówionymi komunikatami, a także uproszczenie i doprecyzowanie otoczenia regulacyjnego poprzez ograniczenie pola manewru państw członkowskich.

LEGISLATIVE POSTULATES CONCERNING PRIVACY PROTECTION IN OVER-THE-TOP SERVICES IN THE EUROPEAN UNION

Summary

The study discusses the issue of insufficient legal regulation of privacy protection in so-called Over-the-Top services, i.e. provided over the Internet at European Union level. It presents proposals for a postulated legal act with the rank of a regulation, which will replace Directive 2002/58 incompatible with technological realities and supplement the provisions of the GDPR in the protection of one of the fundamental rights, which is the right to privacy.

Keywords: right to privacy, privacy protection, Directive 2002/58, GDPR, personal data, electronic communications service, Over-the-Top service, interpersonal communications service

BIBLIOGRAFIA

Kotecka-Kral S., *Zagrożenia związane z przetwarzaniem danych osobowych osób fizycznych w celu profilowania*, [w:] Ius est ars boni et aequi. *Księga pamiątkowa dedykowana Profesorowi Józefowi Frąckowiakowi*, red. A. Dańko-Roesler, M. Leśniak, M. Skory, B. Sołtys, Wrocław 2018.

Litwiński P., Barta P., Kawecki M., *Komentarz do art. 25*, [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, P. Barta, M. Kawecki, Warszawa 2018.

Lubasz D., Witkowska-Nowakowska K., *Komentarz do art. 25*, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Sobczak W., *Komentarz do art. 7*, [w:] *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, red. A. Wróbel, Warszawa 2013/Legalis.

Susałko M., *Ochrona danych w fazie projektowania i domyślna ochrona danych*, [w:] *RODO w e-commerce*, red. D. Lubasz, Warszawa 2018.

Szymielewicz K., Iwańska K., *ePrywatność czy eŚledzenie — czy branża reklamowa postawi na swoim?*, https://panoptykon.org/eprivacy-czy-esledzenie.

Szymielewicz K., Iwańska K., *Śledzenie i profilowanie w sieci. Jak z klienta stajesz się towarem, raport Fundacji Panoptykon* (styczeń 2019), https://panoptykon.org/sites/default/files/publikacje/panoptykon_raport_o_sledzeniu_final.pdf.

Wiewiórowski W., Privacy by Design *jako paradygmat ochrony prywatności*, [w:] *Prawno-informatyczne problemy sieci, portali i e-usług*, red. G. Szpor, W. Wiewiórowski, Warszawa 2012.