# POJĘCIE I ZAKRES TAJEMNICY KOMUNIKACJI ELEKTRONICZNEJ

MACIEJ ROGALSKI*

PRZEMYSŁAW SZUSTAKIEWICZ**

DOI: 10.26399/iusnovum.v16.1.2022.4/m.rogalski/p.szustakiewicz

## WPROWADZENIE

Przygotowany został projekt Ustawy z dnia 2 grudnia 2021 r. Prawo komunikacji elektronicznej[1], którego celem jest m.in. wdrożenie postanowień dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r., ustanawiającej Europejski kodeks łączności elektronicznej[2], oraz dyrektywy Parlamentu Europejskiego i Rady 2002/58/WE z dnia 12 lipca 2002 r., dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej[3]. Dyrektywa o prywatności jest dyrektywą sektorową, która poszerza w obszarze łączności elektronicznej ogólne wymagania w zakresie ochrony danych osobowych zawarte w dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych[4]. W odróżnieniu od pozostałych dyrektyw w sprawach łączności elektronicznej, dyrektywa o prywatności posiada głównie charakter ochronny[5]. Głównym jej celem ochrona podstawowych praw i wolności człowieka, a w szczególności prawa do prywatności w związku z przetwarzaniem danych.

* prof. dr hab., Wydział Prawa i Administracji Uczelni Łazarskiego, e-mail: maciej@rogalski.waw.pl, ORCID: 0000-0003-4366-642X

** dr hab., prof. UŁa Wydział Prawa i Administracji Uczelni Łazarskiego, e-mail: przemyslaw.szustakiewicz@lazarski.edu.pl, ORCID: 0000-0001-9102-9308

1 https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-prawo-komunikacji-elektronicznej.html (dostęp: 20.12.2021), dalej jako: PKE.

2 Dz. Urz. WE L 321/36, dalej jako: EKŁE.

3 Dz. Urz. WE L 201, dalej jako: dyrektywa o prywatności.

4 Dz. Urz. UE L Nr 281, dalej jako: dyrektywa 95/46/WE.

5 A. Mednis, *Ochrona danych osobowych w świetle dyrektywy UE z 12 lipca 2002 roku o prywatności w komunikacji elektronicznej*, „Prawo i Ekonomia w Telekomunikacji" 2002, nr 4, s. 61 i n.

W zakresie ochrony danych osobowych istotne zmiany nastąpiły po uchyleniu dyrektywy 95/46/WE i rozpoczęciu stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[6]. RODO odnosi się w motywie 173 oraz w art. 21 ust. 5 i art. 95 do dyrektywy o prywatności. Stosunek RODO do dyrektywy o prywatności wyjaśnia motyw 173 RODO. Zgodnie z tym motywem RODO powinno mieć zastosowanie do wszystkich tych kwestii dotyczących ochrony podstawowych praw i wolności w związku z przetwarzaniem danych osobowych, które nie podlegają szczególnym obowiązkom mającym ten sam cel określony w dyrektywie o prywatności, w tym obowiązkom nałożonym na administratora oraz prawom osób fizycznych.

Przedmiotem artykułu będzie zbadanie, jakie są zakresy – podmiotowy i przedmiotowy – tajemnicy komunikacji elektronicznej sformułowane w projekcie nowego prawa komunikacji elektronicznej oraz w jakim stopniu nowe rozwiązania stanowią realizację konstytucyjnej zasady ochrony tajemnicy komunikowania się. Zbadane zostanie również, czy w sposób prawidłowy zostały określone w zakresie ochrony danych osobowych relacje pomiędzy projektowanymi postanowieniami PKE a RODO. Przeanalizowane zostaną także relacje projektowanych przepisów do przepisów o dostępie do informacji publicznej. W analizie zostanie wykorzystany dotychczasowy dorobek orzeczniczy w zakresie wskazanych relacji pod rządami Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[7] oraz Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[8].

## TAJEMNICA KOMUNIKOWANIA SIĘ W KONSTYTUCJI RP

Tajemnica komunikacji elektronicznej powinna spełniać w odniesieniu do telekomunikacji wymogi związane z określoną w art. 49 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.[9] – tajemnicą komunikowania się. Przepis art. 49 Konstytucji RP zapewnia wolność i ochronę tajemnicy komunikowania się, a zatem ma bardzo szeroki zakres[10]. Ograniczenie tych gwarancji może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony. „Dla prawidłowego określenia znaczenia gwarancji określonych w art. 49 Konstytucji RP wskazać należy, że w istocie posiada on charakter ochronny, ponieważ jest on jedną z gwarancji określonej w art. 39 ust. 1 Konstytucji RP wolności człowieka. Wolność człowieka chroniona jest w konstytucji poprzez nie tylko ogóle jej przywołanie, ale przede wszystkim przez system szeregu rodzaju prawnych zabezpieczeń, które chronią różnorodnego rodzaju elementy umożliwiające jedno-

[6] Dz. Urz. UE L Nr 119, dalej jako: RODO.
[7] Dz.U. z 1997 r., nr 171, poz. 1800 ze zm., dalej jako: p.t.
[8] Dz.U. z 2002 r., nr 101, poz. 926 ze zm., dalej jako: u.o.d.o.
[9] Dz.U. z 1997 r., nr 78, poz. 483, dalej jako: konstytucja.
[10] Por. M. Safjan, L. Bosek (red.), *Konstytucja RP, t. I, Komentarz do art. 1–86*, Legalis 2016, kom. do art. 49 cz. III, pkt 2.

stce ludzkiej suwerenne i autonomiczne podejmowanie decyzji o sobie. Ingerencje władzy publicznej w tę swobodę następować mogą tylko w sytuacjach i w formach przewidzianych konstytucyjnie. Innymi słowy, zasada wolności formułuje domniemanie swobody decyzji i działań, natomiast dla poddawania ich ograniczeniom konieczna jest zawsze interwencja prawodawcy"[11].

Tajemnica komunikowania się chroni wolność porozumiewania się ludzi, rozumianą jako wolność nieskrępowanego wyboru podmiotu, z którym można pozostać w więzi, treść przekazanych temu podmiotowi informacji i danych od niego otrzymanych, a także środka komunikacji. Tajemnica komunikowania się wraz z prawem do prywatności (art. 47 Konstytucji RP) i prawem do ochrony danych osobowych (art. 51 ust. 1 Konstytucji RP) stanowią rozbudowany katalog uprawnień gwarantujący, że ingerencja państwa w prywatność osoby fizycznej będzie ograniczona do niezbędnego minimum. Trybunał Konstytucyjny („TK") wskazuje, że „immanentnym elementem wszystkich konstytucyjnych wolności człowieka jest spoczywający na państwie obowiązek ich prawnego poszanowania i ochrony, a także powstrzymywania się od ingerowania w wolności zarówno przez państwo, jak i podmioty prywatne"[12]. Chronione powinny być informacje wchodzące w zakres sfery prywatnej człowieka, których ujawnienie mogłyby posłużyć do manipulowania nim, co mogłoby utrudniać podejmowanie przez niego racjonalnych decyzji[13].

Podmiotami zobowiązanymi na gruncie art. 49 Konstytucji RP są organy władzy publicznej, na których spoczywa obowiązek poszanowania wolności komunikowania się jednostek między sobą oraz obowiązek ochrony tajemnicy komunikowania się. Obowiązek przestrzegania tajemnicy komunikowania się spoczywa również na podmiotach prywatnych, do których komunikat nadawcy jest kierowany, a także innych podmiotach prywatnych, do których komunikat ten zgodnie z intencją nadawcy nie powinien dotrzeć[14]. Podmiotem uprawnionym do powoływania się na ochronę jaką daje treść art. 49 Konstytucji RP jest każdy człowiek niezależnie od jego statusu wynikającego z przynależności państwowej lub sytuacji prawnej, a zatem ochrona tajemnicy komunikacji przysługuje również obcokrajowcom. Mogą na tajemnicę komunikowania się również powoływać osoby niepełnoletnie i ubezwłasnowolnione, choć oczywiście wykonują swoje uprawnienie w tym zakresie poprzez swoich przedstawicieli oraz niekiedy jednostki organizacyjne.

---

[11] L. Garlicki, K. Wojtyczek, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom II, wyd. II*, red. M. Zubik, LEX 2016, art. 31.

[12] Wyrok TK z 30 lipca 2014 r., sygn. akt K 23/11, „Orzecznictwo Trybunału Konstytucyjnego" („OTK") 2014, nr 7, poz. 80.

[13] Przykładem jest wykorzystanie danych z portali społecznościowych zgromadzonych przez przedsiębiorstwo Cambridge Analytica do wpływania na decyzje wyborców w latach 2015–2016, por. S. Czubkowska, *Afera Cambridge Analitica. Facebook wybrał Amerykanom prezydenta. Czy nam też wybierze? I jeszcze na tym zarobi*, https://wyborcza.pl/7,156282,23182834,afera-cambridge-analytica-facebook-wybral-amerykanom.html (dostęp: 15.03.2021).

[14] M. Florczak-Wątor, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, LEX 2019, art. 49.

Zakres przedmiotowy tajemnicy komunikowania się obejmuje, jak podniósł TK, wszelkie sposoby przekazywania wiadomości, w każdej formie komunikowania się, bez względu na fizyczny ich nośnik (są to np. rozmowy osobiste i telefoniczne, korespondencja pisemna, faks, wiadomości tekstowe i multimedialne, poczta elektroniczna). Ochrona konstytucyjna obejmuje dane osobowe uczestników komunikacji, informacje o wybieranych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze IMEI[15]. Ze sformułowania art. 49 Konstytucji RP wyraźnie wynika objęcie tajemnicą nie tylko treści przekazów, lecz także faktu i okoliczności komunikowania się[16]. Z tajemnicy komunikowania się wynikają m.in.: „zakaz stosowania podsłuchu telefonicznego, wprowadzania cenzury korespondencji czy też wchodzenia w inny sposób w krąg wiadomości dotyczących życia, interesów i działań innych osób"[17]. Zakres konstytucyjnej tajemnicy komunikowania się musi być uwzględniany przy formułowaniu ustawowych ograniczeń w zakresie wolności komunikowania się[18].

Ustawodawca, ograniczając tajemnicę komunikowania się, powinien postępować ostrożnie, ponieważ jego ingerencja nie dotyczy niejako kwestii technicznej związanej z ochroną pewnego rodzaju tajemnicy, ale narusza ważny element chroniący wolność człowieka. Stąd przewidziane przez prawo możliwości naruszenia tego rodzaju tajemnicy powinny być wyjątkowe[19].

## OCHRONA PRYWATNOŚCI W EUROPEJSKIEJ KONWENCJI O OCHRONIE PRAW CZŁOWIEKA I PODSTAWOWYCH WOLNOŚCI ORAZ KARCIE PRAW PODSTAWOWYCH

Zgodnie z art. 8 ust. 1 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności, przyjętej w Rzymie 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej protokołem nr 2 („EKPCPW")[20], każdy ma

---

[15] Wyrok TK z 30 lipca 2014 r., sygn. akt K 23/11, OTK 2014, nr 7, poz. 80.

[16] Zob. B. Opaliński, *Tajemnica komunikowania się w Konstytucji RP*, w: *Gromadzenie i udostępnianie danych telekomunikacyjnych*, red. P. Brzeziński, B. Opaliński, M. Rogalski, Warszawa 2016, s. 7 i n.

[17] W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz, wyd. VII*, LEX 2013, art. 49.

[18] Por. wyrok TK z 20 czerwca 2005 r., sygn. akt K 4/04, OTK 2005, nr 6, poz. 64. Zob. także wyrok TK z 2 lipca 2007 r., sygn. akt K 41/05, OTK ZU 2007/7A, poz. 72, cz. III, pkt 5.2.

[19] Zob. szerzej na temat art. 31 ust. 3 Konstytucji: P. Sarnecki (red.), *Prawo konstytucyjne RP*, Warszawa 2011, s. 100; L. Garlicki (red.), *Konstytucja Rzeczpospolitej Polskiej. Komentarz*, t. II, Warszawa 2002, s. 22–28. Zob. także wyrok TK z 18 lutego 2004 r., sygn. akt P. 21/02, OTK 2004/2A, poz. 9, cz. III, pkt 4; wyrok TK z 26 kwietnia 1999 r., sygn. akt K 33/98, OTK 1999/4, poz. 71; wyrok TK z 11 maja 1999 r., sygn. akt K 13/98, OTK 1999, nr 4, poz. 74; wyrok TK z 25 lutego 1999 r., sygn. akt K 23/98, OTK 1999/2, poz. 25; wyrok TK z 12 listopada 1995 r., sygn. akt K 12/95, OTK 1995/3, poz. 15, LEX nr 25568.

[20] Dz.U. z 1993 r., nr 61, poz. 284 ze zm.

prawo do poszanowania swojego życia prywatnego, w tym swojej korespondencji. Warunki ograniczania tego prawa przewiduje art. 8 ust. 2 EKPCPW, zgodnie z którym niedopuszczalna jest ingerencja władzy publicznej w korzystanie z prawa wyrażonego w art. 8 ust. 1 EKPCPW, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób. Przepis art. 8 ust. 1 EKPCPW dotyczy szeroko rozumianego prawa do poszanowania prywatnej sfery życia człowieka, gwarantując autonomię jednostce w zakresie kształtowania aspektów jej życia oraz własnej osobowości. Istotą tego prawa jest zapewnienie każdej jednostce sfery prywatności (autonomii) chronionej przed ingerencją zewnętrzną, pochodzącą zarówno od państwa, jak i podmiotów prywatnych[21].

Przepis art. 8 ust. 1 EKPCPW wskazuje cztery podstawowe dziedziny podlegające ochronie prawnej, a mianowicie: życie prywatne, życie rodzinne, mieszkanie i korespondencję. Sfery prywatności wymienione w tym przepisie nie mogą być ujmowane rozłącznie, gdyż nakładają się na siebie, tworząc tym samym wiele szczegółowych praw i odpowiadających im negatywnych i pozytywnych obowiązków władzy publicznej. Ich celem jest w konsekwencji ochrona godności człowieka i jego wolności[22]. Karta Praw Podstawowych Unii Europejskiej, w art. 7 także stanowi, że każda osoba ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się.

Zgodnie z art. 87 ust. 1 Konstytucji RP źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia. Ratyfikowane umowy międzynarodowe są źródłem prawa w Polsce. Państwo powinno gwarantować przyjęte przez siebie prawa nie tylko swoim obywatelom, ale także wszystkim osobom podlegającym jego jurysdykcji, niezależnie od obywatelstwa[23]. Postanowienia wskazanych aktów prawa międzynarodowego powinny być także uwzględniane w tworzonych nowych regulacjach prawnych, w tym w ustawie Prawo komunikacji elektronicznej. W szczególności, że przepisy prawa międzynarodowego ustanawiają jedynie minimalne standardy ochrony praw człowieka. Nie jest więc możliwe przyjmowanie w przepisach krajowych dotyczących ochrony praw człowieka zmian ograniczających lub znoszących gwarancje tylko z tego powodu, że postanowienia konwencji przewidują węższy niż prawo krajowe zakres[24].

---

[21] Zob. L. Garlicki, uwaga 21 do art. 8, w: *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1–18*, red. L. Garlicki, P. Hofmański, A. Wróbel, Warszawa 2010, s. 491; wyrok TK z 30 lipca 2014 r., sygn. K 23/11, OTK ZU 2014, nr 7, poz. 180; K. Szczechowicz, *Podsłuch telefoniczny w polskim procesie karnym*, Olsztyn 2009, s. 22–23.

[22] Zob. L. Garlicki, w: *Konwencja o Ochronie Praw Człowieka…*, op. cit., uwaga 21 do art. 8; wyrok TK z 30 lipca 2014 r., sygn. K 23/11, OTK ZU 2014, nr 7, poz. 180.

[23] F. Sudre, *Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności*, Warszawa 1993, s. 12. Zob. także M.A. Nowicki, *Wokół Konwencji Europejskiej*, Warszawa 1992, s. 13.

[24] D. Gajdus, B. Gronowska, *Stosowanie podsłuchu telefonicznego w ocenie Europejskiej Komisji i Europejskiego Trybunału Praw Człowieka. (Refleksje na tle rozwiązań polskich)*, „Palestra" 1994, nr 11, s. 122.

## DEFINICJA TAJEMNICY KOMUNIKACJI ELEKTRONICZNEJ

W obowiązującej obecnie ustawie prawo telekomunikacyjne używane jest pojęcie tajemnicy telekomunikacyjnej, zdefiniowane w art. 159 ust. 1 p.t. Tajemnicy telekomunikacyjnej poświęcony jest dział VII p.t. zatytułowany *Tajemnica telekomunikacyjna i ochrona danych użytkowników końcowych* (art. 159–174d p.t.). PKE wprowadza nową nazwę tej tajemnicy – to „tajemnica komunikacji elektronicznej", której poświęcony jest rozdział 4 zatytułowany *Tajemnica komunikacji elektronicznej oraz dane użytkowników końcowych* (art. 381–400 PKE) w dziale VII zatytyłowanym *Publicznie dostępne usługi komunikacji elektronicznej.*

Definicję tajemnicy komunikacji elektronicznej zawiera art. 381 PKE, który implementuje art. 5 dyrektywy o prywatności. W przepisie art. 381 PKE jest mowa o poufności komunikacji i związanych z nią danych o ruchu za pośrednictwem sieci telekomunikacyjnej. Tajemnica komunikacji elektronicznej odnosi się nie tylko do usług świadczonych przez przedsiębiorców telekomunikacyjnych, ale również przez dostawców usług komunikacji interpersonalnej niewykorzystującej numeracji.

Zgodnie z art. 381 ust. 1 PKE tajemnica komunikowania się w sieciach telekomunikacyjnych (tajemnica komunikacji elektronicznej) obejmuje:

1) dane dotyczące użytkownika;

2) komunikat elektroniczny;

3) dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów elektronicznych w sieciach telekomunikacyjnych lub naliczania opłat za usługi komunikacji elektronicznej, i mogą obejmować dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej lub w ramach usług komunikacji elektronicznej wskazujące położenie geograficzne telekomunikacyjnego urządzenia końcowego użytkownika usług komunikacji elektronicznej;

4) dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu elektronicznego lub wystawienia rachunku;

5) dane o próbach uzyskania połączenia pomiędzy zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń.

Tajemnica komunikacji elektronicznej występuje tylko w przypadku, gdy następuje wykorzystanie sieci telekomunikacyjnych w celu komunikowania. Pojęcie sieci telekomunikacyjnej zostało określone w PKE w sposób szeroki. Obejmuje systemy transmisyjne, a także urządzenia telekomunikacyjne, oprócz telekomunikacyjnych urządzeń końcowych, oraz inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają przekazywanie sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od rodzaju przekazywanej informacji (art. 2 pkt 59 PKE). Komunikowanie się w sieciach telekomunikacyjnych jest przedmiotem ochrony nie tylko w zakresie przesyłania informacji i danych, ale również w zakresie innych zda-

rzeń towarzyszących tym transmisjom[25]. Artykuł 381 ust. 1 PKE ogranicza pojęcia tajemnicy komunikacji elektronicznej do komunikowania w sieciach publicznych (art. 2 pkt 44 PKE).

## DANE UŻYTKOWNIKA

Tajemnica komunikacji elektronicznej obejmuje dane dotyczące użytkownika (art. 381 ust. 1 pkt 1 PKE). W wypadku przetwarzania danych dotyczących użytkownika, jeżeli mają charakter danych osobowych, a więc dotyczą osób fizycznych, powinno być ono zgodne z przepisami o ochronie danych osobowych. Ochrona danych o użytkownikach, którzy nie są osobami fizycznymi (użytkowników instytucjonalnych), jest uregulowana w przepisach PKE. Dane osobowe mogą również występować w treściach i danych, o których mowa w art. 381 ust. 1 pkt 2–5 (treść indywidualnych komunikatów, dane lokalizacyjne, dane o lokalizacji i próbach uzyskania połączenia). Dane te powinny podlegać ochronie przewidzianej w PKE zarówno w przypadku, gdy dotyczą osób fizycznych, jak i gdy są związane z podmiotami instytucjonalnymi[26].

Zgodnie z art. 2 pkt 86 PKE użytkownikiem jest podmiot korzystający z publicznie dostępnej usługi komunikacji elektronicznej lub żądający świadczenia takiej usługi, bez konieczności pozostawania stroną umowy o świadczenie usług telekomunikacyjnych. Tajemnicą są objęte dane dotyczące użytkowników przekazywane w sieci telekomunikacyjnej, a także dane o użytkownikach występujące w związku z ustanowieniem stosunku prawnego pomiędzy użytkownikiem a przedsiębiorcą oraz w związku z korzystaniem z usług[27]. Przepis art. 2 pkt 1 PKE definiuje z kolei abonenta jako użytkownika, który jest stroną umowy o świadczenie usług komunikacji elektronicznej zawartej z dostawcą usług komunikacji elektronicznej. Zgodnie więc z definicją przyjętą w PKE każdy abonent jest użytkownikiem. Wszystkie zatem regulacje w zakresie tajemnicy komunikacji elektronicznej, dotyczące użytkownika, odnoszą się także do abonenta. PKE używa także pojęcia użytkownik końcowy, którym jest podmiot korzystający z publicznie dostępnej usługi komunikacji elektronicznej lub żądający świadczenia takiej usługi dla zaspokojenia własnych potrzeb (art. 2 pkt 87 PKE). Pojęcie użytkownika jest szersze niż użytkownika końcowego i ochrona tajemnicy komunikacji elektronicznej obejmuje także użytkowników końcowych.

## KOMUNIKAT ELEKTRONICZNY

Zgodnie z art. 2 pkt 19 PKE komunikat elektroniczny obejmuje każdą informację wymienianą lub przekazywaną między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług komunikacji elektronicznej. W związku z tym, że ochrona obejmuje użytkowników, to nie ma znaczenia, czy są oni stroną

[25] S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2019, s. 1097.
[26] Ibidem, s. 1098.
[27] Ibidem.

umowy z dostawcą usług komunikacji elektronicznej (art. 2 pkt 77 PKE). Komunikat jest informacją przekazywaną za pośrednictwem publicznie dostępnych usług komunikacji elektronicznej, co zawęża przedmiot ochrony. Zgodnie bowiem z art. 2 pkt 45 PKE publicznie dostępna usługa komunikacji elektronicznej oznacza usługę komunikacji elektronicznej dostępną dla ogółu użytkowników.

## DANE TRANSMISYJNE

Tajemnicą komunikacji elektronicznej objęte są dane transmisyjne (art. 381 ust. 1 pkt 3 PKE). W związku z komunikatami elektronicznymi przekazywane są informacje towarzyszące, niezbędne do zestawienia połączenia lub transmisji komunikatu w sposób bezpołączeniowy, ustalenia sposobu zestawienia połączenia lub kierowania komunikatu, stosowanego protokołu komunikacyjnego oraz formatu komunikatu, identyfikacji abonentów, identyfikacji zakończeń sieci (numery, nazwy, inne znaki identyfikujące), identyfikacji urządzeń końcowych (np. numer IMEI), ustalenia należności za usługę telekomunikacyjną (termin rozpoczęcia i zakończenia, czas trwania połączenia lub przekazu, objętość informacji), a także inne informacje w zależności od rodzaju sieci i usługi komunikacji elektronicznej. Zakres przetwarzanych danych transmisyjnych jest pochodną funkcjonalności wykonywanej usługi komunikacji elektronicznej oraz technologii wykorzystywanej do jej świadczenia. Wśród danych transmisyjnych występują dane lokalizacyjne, wskazujące położenie geograficzne telekomunikacyjnego urządzenia końcowego należącego do użytkownika usług komunikacji elektronicznej. Chodzi o wszelkie dane przetwarzane w sieci telekomunikacyjnej lub w ramach wykonywania usług telekomunikacyjnych. Dane lokalizacyjne obejmują szerokość, długość geograficzną i wysokość nad poziomem morza, które można ustalić w odniesieniu do konkretnego terminala[28].

## DANE O LOKALIZACJI

Kategorię danych o lokalizacji wyróżniono w celu uregulowania spraw związanych z wykonywaniem usług o wartości wzbogaconej, opartych na lokalizacji (art. 2 pkt 80 PKE). Przepis art. 381 ust. 1 PKE wyróżnia więc dane lokalizacyjne (art. 381 ust. 1 pkt 3 PKE) oraz dane o lokalizacji (art. 381 ust. 1 pkt 4 PKE). Podział ten opiera się na różnym celu przetwarzania. Dane o lokalizacji mogą być gromadzone na podstawie różnych technologii występujących w sieciach telekomunikacyjnych lub w urządzeniach, którymi posługuje się użytkownik urządzenia[29].

---

[28] Ibidem, s. 1100. Zob. także K. Kawałek, M. Rogalski (red.), *Prawo telekomunikacyjne. Komentarz*, Warszawa 2010, s. 861.

[29] S. Piątek, *Prawo telekomunikacyjne…*, op. cit., s. 1100.

## DANE O PRÓBACH UZYSKANIA POŁĄCZENIA

Tajemnicą komunikacji elektronicznej objęte są dane o próbie uzyskania połączenia między określonymi zakończeniami sieci, w tym dane o nieudanych próbach połączeń (art. 381 ust. 1 pkt 5 PKE). Zarejestrowane dane tego rodzaju są chronione tajemnicą komunikacji elektronicznej na takich samych zasadach, jak dane o zrealizowanych połączeniach. Źródłem wymagań dotyczących zatrzymywania danych o próbach połączeń była dyrektywa Parlamentu Europejskiego i Rady 2006/24/WE z 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE. Trybunał Sprawiedliwości UE („TSUE") w wyroku z 8 kwietnia 2014 r., sprawy połączone C293/12 i C594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications i in.*[30], orzekł o nieważności tej dyrektywy[31], co jednak nie spowodowało uchylenia przepisów implementujących ją w krajowym porządku prawnym. Wyrok TSUE nie kwestionował bowiem dopuszczalności retencji danych telekomunikacyjnych w przepisach krajowych[32]. TSUE sformułował wytyczne w zakresie retencji danych[33]. Wątpliwości budzi natomiast charakter prawny tych wytycznych, tj. czy posiadają charakter bezwzględnych nakazów, czy też część z nich można uznać za niewiążące sugestie [34].

Dokonując wykładni przepisu art. 381 ust. 1 pkt 5 PKE, należy stwierdzić, że nieudaną próbą połączenia jest takie połączenie, które zostało zestawione pomiędzy zakończeniem sieci abonenta wywołującego oraz abonenta wywoływanego, ale z jakiegoś powodu nie zostało odebrane lub po zestawieniu zostało przerwane przez system. W praktyce oznaczać to będzie, że nieudaną próbą połączenia jest połączenie zestawione, lecz nieodebrane przez abonenta wywoływanego. Podobnie w przypadku połączenia przerwanego przez abonenta wywołującego lub wywoływanego podczas sygnału dzwonienia[35].

---

[30] European Case Law Identifier:EU:C:2014:238.

[31] Zob. szerzej w sprawie rozstrzygnięcia z dnia 8 kwietnia 2014 r. TSUE i jego uzasadnienia: A. Roberts, *Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications*, „Modern Law Review" 2015, nr 78 (3), s. 547 i n.; J. Milaj, *Invalidation of the Data Retention Directive – Extending the Proportionality Test*, „Computer Law & Security Review" 2015, nr 31, s. 606 i n.; S. Tracey, *The Fall of the Data Retention Directive*, „Communications Law" 2015, nr 20 (2), s. 54 i n.; M.P. Granger, K. Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, „European Law Review" 2014, nr 39 (6), s. 848.

[32] Zob. M. Tomkiewicz, *Sądowa kontrola pozyskiwania danych telekomunikacyjnych, internetowych i pocztowych*, „Państwo i Prawo" 2018, nr 4, s. 69.

[33] S. Piątek, *Prawo telekomunikacyjne…*, op. cit., s. 1101.

[34] Zob. szerzej M. Husovec, *First European Constitutional Court Suspends Data Retention after the Decision of the Court of Justice of EU*, The Center for Internet and Society, 8 April 2014, http://cyberlaw.stanford.edu/blog/2014/04/first-european-constitutional-court-suspends-data-retention-after-decision-court (dostęp: 20.12.2020). Zob. także S. Peers, *The Data Retention Judgment: The CJEU Prohibits Mass Surveillance*, EU Law Analysis, 8 April 2014, http://eulawanalysis.blogspot.fi/2014/04/the-data-retention-judgment-cjeu.html (dostęp: 11.10.2020).

[35] S. Piątek, *Prawo telekomunikacyjne…*, op. cit., s. 1101. Zob. także K. Kawałek, M. Rogalski (red.), *Prawo telekomunikacyjne…*, op. cit., s. 861–862.

## ZAKRES PODMIOTOWY TAJEMNICY KOMUNIKACJI ELEKTRONICZNEJ

Postanowienia art. 381 PKE obejmują wszystkie osoby, które mają dostęp do danych objętych tajemnicą komunikacji elektronicznej. Przepisy art. 382 PKE, które bezpośrednio odnoszą się do zakresu podmiotowego obowiązku zachowania tajemnicy komunikacji elektronicznej, wiążą ten obowiązek z uczestnictwem w wykonywaniu działalności elektronicznej (art. 382 ust. 1 PKE). Obowiązek zachowania tajemnicy obciąża więc wszystkie osoby, które funkcjonują w podmiotach uczestniczących w wykonywaniu działalności komunikacji elektronicznej w publicznych sieciach telekomunikacyjnych oraz podmiotach z nim współpracujących. Pojęcie „działalności komunikacji elektronicznej" obejmuje świadczenie publicznie dostępnych usług telekomunikacyjnych, dostarczanie publicznych sieci telekomunikacyjnych, w tym sieci i usług służących rozpowszechnianiu lub rozprowadzaniu programów radiofonicznych i telewizyjnych, lub świadczenie powiązanych usług oraz świadczenie publicznie dostępnych usług komunikacji interpersonalnej niewykorzystujących numerów (art. 1 ust. 1 PKE). PKE poszerza więc zakres podmiotowy uregulowań na przedsiębiorców świadczących publicznie dostępne usługi komunikacji interpersonalnej niewykorzystujące numeracji. Usługi te są określane jako usługi *Over the Top* (OTT). Wskazane wcześniej podmioty są obowiązane do zachowania należytej staranności w zakresie uzasadnionym względami technicznymi lub ekonomicznymi, przy zabezpieczaniu urządzeń telekomunikacyjnych, publicznych sieci telekomunikacyjnych oraz danych przed ujawnieniem tajemnicy komunikacji elektronicznej (art. 382 ust. 2 PKE).

Poszerzenie zakresu przedmiotowego i podmiotowego usług łączności elektronicznej w PKE (OTT) wpłynie na zakres stosowania dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[36]. W konsekwencji obowiązki wynikające z tej dyrektywy będą miały również zastosowanie do dostawców usług OTT-1, do których zalicza się usługi łączności elektronicznej, które nie mają formalnie takiego charakteru, ale są lub mogą być dla nich substytucyjne. W większości przypadków przetwarzanie informacji zawartych w łączności elektronicznej i powiązanych metadanych wygenerowanych w trakcie świadczenia usług OTT-1 będzie wymagać zgody użytkownika. Jedyne wyjątki mogą być prawnie dozwolone zgodnie z art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej[37].

Obecnie trwają prace nad Rozporządzeniem Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)[38]. Zakres stosowania tego rozporządzenia

---

[36] Dz. Urz. UE 2002 L 201.37 z dnia 31 lipca 2002.

[37] X. Konarski, *Wpływ Europejskiego kodeksu łączności elektronicznej na ochronę danych osobowych i prywatności użytkowników usług OTT-1 (usług łączności interpersonalnej)*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2020, nr 1, s. 75–76, 79–80, 82–83.

[38] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52017PC0010&from=PL (dostęp: 15.12.2021).

obejmie także dostawców usług OTT (por. punkt 1.3 tego rozporządzenia). Podtrzymuje także treść obecnego art. 15 dyrektywy o prywatności i łączności elektronicznej.

## PRZESŁANKI LEGALNEGO DOSTĘPU DO TAJEMNICY TELEKOMUNIKACYJNEJ

Informacje, o których mowa w art. 381 ust. 1 pkt 2–5, objęte tajemnicą komunikacji elektronicznej mogą być przetwarzane wyłącznie na potrzeby świadczonej usługi komunikacji elektronicznej. Przetwarzanie w innych celach jest dopuszczalne jedynie na podstawie przepisów ustawowych (art. 384 ust. 1 PKE). Przepis art. 384 ust. 2 PKE pozwala dostawcy usług komunikacji elektronicznej zanonimizować informacje, o których mowa w art. 381 ust. 1 pkt 2–5. Z kolei przepis art. 387 ust. 1 pkt 2 PKE stanowi, że w celu wykorzystania danych o lokalizacji dostawca usług komunikacji elektronicznej jest obowiązany dokonać anonimizacji tych danych. Dostawcy usług komunikacji elektronicznej będą mogli więc dokonywać operacji na zanonimizowanych danych. W motywie 26 RODO wyjaśniono, że anonimizacja danych osobowych oznacza czynności, który rezultatem jest to, że danych osób, których te dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować[39].

Przepis art. 384 ust. 3 PKE, zezwala także operatorowi przetwarzać dane osobowe użytkowników końcowych w zakresie niezbędnym do realizacji obowiązków, o których mowa w art. 21a Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Zgodnie z art. 21a ust. 3 tej ustawy operator jest obowiązany, na żądanie dyrektora Centrum, do niezwłocznego, nieodpłatnego wysłania komunikatów do wszystkich lub określonych przez dyrektora Rządowego Centrum Bezpieczeństwa grup użytkowników końcowych, w szczególności przebywających na określonym przez niego obszarze, jednorazowo lub przez wskazany przez dyrektora tego Centrum okres.

Warto zwrócić także uwagę na obowiązujące obecnie przepisy dotyczące zwalczania epidemii COVID-19, a tyczące się tajemnicy telekomunikacyjnej. Zgodnie z art. 11f Ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. z 2021 r., poz. 2095 ze zm.), podczas stanu zagrożenia epidemicznego, stanu epidemii albo stanu klęski żywiołowej operator jest obowiązany do udostępniania ministrowi właściwemu do spraw informatyzacji danych lokalizacyjnych, obejmujących okres ostatnich 14 dni, telekomunikacyjnego urządzenia użytkownika końcowego chorego na chorobę zakaźną COVID-19 lub objętego kwarantanną, na żądanie oraz

[39] Szerzej na temat istoty i charakteru prawnego anonimizacji danych objętych tajemnicą telekomunikacyjną zob. S. Piątek, P. Piątek, *Anonimizacja danych objętych tajemnicą telekomunikacyjną*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2014, nr 8, s. 51–59.

w sposób i w formie ustalonej przez ministra właściwego do spraw informatyzacji. Operator na żądanie ministra właściwego do spraw informatyzacji jest obowiązany do przekazania w sposób i w formie ustalonej przez tego ministra, w celu przeciwdziałania COVID-19, podczas stanu zagrożenia epidemicznego, stanu epidemii albo stanu klęski żywiołowej zanonimizowanych danych lokalizacyjnych urządzeń końcowych użytkowników końcowych. Zgoda użytkownika końcowego na przetwarzanie i udostępnianie tych danych nie jest wymagana. Z kolei zgodnie z art. 11g wskazanej ustawy podczas stanu zagrożenia epidemicznego, stanu epidemii albo stanu klęski żywiołowej anonimizacja danych lokalizacyjnych w celu przeciwdziałania COVID-19 nie stanowi czynności przetwarzania, o której mowa w art. 161 ust. 1 p.t.

Zgodnie z art. 382 ust. 5 PKE podmioty uczestniczące w wykonywaniu działalności komunikacji elektronicznej w publicznych sieciach telekomunikacyjnych oraz podmioty z nim współpracujące, działając na zlecenie organów administracji publicznej, mogą wysyłać komunikaty elektroniczne w interesie publicznym do użytkowników końcowych. Przepis ten przewiduje kolejny wyjątek w zakresie zachowania tajemnicy komunikacji elektronicznej, który jest uzasadniony interesem publicznym.

Wreszcie wskazać należy na postanowienia art. 393 PKE. Zgodnie ust. 1 tego przepisu zakazane jest używanie: 1) automatycznych systemów wywołujących lub 2) telekomunikacyjnych urządzeń końcowych, w szczególności w ramach korzystania z usług komunikacji interpersonalnej – dla celów przesyłania niezamówionej informacji handlowej w rozumieniu Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, w tym marketingu bezpośredniego, do abonenta lub użytkownika końcowego, chyba że uprzednio wyraził on na to zgodę. Zgoda ta może być wyrażona przez udostępnienie przez abonenta lub użytkownika końcowego identyfikującego go adresu elektronicznego w rozumieniu Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, w celu przesyłania niezamówionej informacji handlowej (art. 393 ust. 2 PKE).

W tym miejscu przypomnieć należy treść art. 31 ust. 3 Konstytucji RP, według którego ograniczenia w zakresie konstytucyjnych wolności i praw, a więc wolności komunikowania się i tajemnicy komunikowania się, mogą być ustanawiane tylko wtedy, gdy są konieczne w demokratycznym państwie, w szczególności dla jego bezpieczeństwa lub porządku publicznego, zdrowia i moralności publicznej albo wolności i praw innych osób. Przepis ten formułuje zasadę proporcjonalności, którą kształtują trzy przesłanki o charakterze materialnym: przydatność, konieczność oraz proporcjonalność[40]. Przepis ten określa dwie przesłanki (formalną i materialną), które muszą zostać spełnione łącznie, aby uznać, że możliwe jest naruszenie tajemnicy komunikowania się. Przesłanka formalna określa formę aktu prawnego, który zezwala na naruszenie rodzaju tajemnicy określonego w art. 49 Konstytucji – dopuszczalne jest tylko ograniczenie tajemnicy dokonane w ustawie. Przesłanka materialna z kolei wskazuje na wartości, które powinny być brane pod

[40] Zob. szerzej P. Sarnecki (red.), *Prawo konstytucyjne RP*, Warszawa 2011, s. 100; L. Garlicki (red.), *Konstytucja Rzeczpospolitej Polskiej. Komentarz*, t. II, Warszawa 2002, s. 22–28.

uwagę w demokratycznym państwie, jeżeli decyduje się ona na ingerencję w tajemnicę komunikowania się. Należą do nich bezpieczeństwo, porządek publiczny lub ochrony środowiska, zdrowia i moralności publicznej, albo ochrona wolności i praw innych osób, przy czym naruszanie tajemnicy komunikowania się nie może w powodować, że przestanie ona faktycznie istnieć. W PKE została określona jedynie PKE przesłanka formalna, ponieważ art. 384 ust. 1 PKE wskazuje wprost, że przetwarzanie danych objętych tajemnicą komunikacyjną w celach innych niż związanych z świadczonymi usługami może nastąpić tylko na podstawie przepisów ustawy. Natomiast PKE nie określa przesłanek materialnych udostępnienia danych objętych tajemnicą korespondencji, te bowiem są określone w innych ustawach określających prawo dostępu do danych objętych tajemnicą komunikacyjną.

## DOSTĘP DO TAJEMNICY TELEKOMUNIKACYJNEJ – ORZECZNICTWO SĄDÓW POWSZECHNYCH

Przepis art. 381 ust. 2 PKE zakazuje przetwarzanie informacji objętych tajemnicą komunikacji elektronicznej, o których mowa w art. 381 ust. 1 pkt 2–5 PKE, przez osoby inne niż nadawca i odbiorca komunikatu, ale jednocześnie określa wyjątki, kiedy przetwarzanie takie będzie możliwe. Operacje na treściach i danych objętych tajemnicą komunikacji elektronicznej są dozwolone dla nadawcy i odbiorcy komunikatu. Z przepisu art. 381 ust. 2 PKE nie wynika jednak uprawnienie dla nadawcy i odbiorcy komunikatu do żądania dostępu do wszystkich danych objętych tajemnicą, w szczególności do wszelkich danych transmisyjnych i danych o lokalizacji. Nadawca i odbiorca komunikatów uzyskują dostęp do poszczególnych treści i danych na podstawie umowy lub z mocy przepisów prawa. Pewne ograniczenia w zakresie dostępu do tych danych mogą jednak wynikać z treści innych stosunków publiczno- lub prywatnoprawnych. Przepis art. 381 ust. 2 pkt 4 PKE wprost wskazuje, że wkroczenie w sferę tajemnicy komunikacji elektronicznej jest możliwe tylko w przypadkach ściśle określonych ustawą oraz w przepisach odrębnych[41].

Przepis art. 381 ust. 2 PKE dotyczy różnych kategorii treści i danych, które podlegają odrębnym zasadom ochrony, co może w praktyce powodować trudności. W sposób jednolity potraktowano bowiem treści komunikatów, dane użytkowników oraz inne dane objęte tajemnicą komunikacji elektronicznej. Przepisy art. 381 ust. 2 PKE posiadają charakter szczególny w stosunku do przepisów chroniących dane osobowe. Zakresy czynności podejmowanych w związku z treściami i danymi objętymi tajemnicą komunikacji elektronicznej krzyżują się z czynnościami regulowanymi przepisami o ochronie danych osobowych.

Pod rządami Prawa telekomunikacyjnego orzecznictwo sądowe zmierzało w kierunku ograniczenia dopuszczalności żądania przez sądy danych objętych tajemnicą telekomunikacyjną, w szczególności danych objętych retencją, dla celów

[41] Zob. także S. Hoc, *Glosa do uchwały SN z 22.1.2003 r., I KZP 45/02*, „Przegląd Sądowy" 2003, nr 11–12, s. 203; J. Misztal-Konecka, J. Konecki, *Billing jako dowód w postępowaniu w sprawach o wykroczenia*, „Państwo i Prawo" 2010, nr 7, s. 84; A. Bojańczyk, *Karnoprawne aspekty ochrony praw pracownika do tajemnicy komunikowania się, cz. I*, „Palestra" 2003, nr 1–2, s. 49.

postępowania innego niż w sprawach karnych[42]. SA w Białymstoku w postanowieniu z dnia 6 kwietnia 2011 r., sygn. akt I ACz 279/11, wyjaśnił, że „ani prawo telekomunikacyjne, ani przepisy Kodeksu postępowania cywilnego nie stwarzają podstawy uzasadniającej wydanie przez sąd w sprawie cywilnej postanowienia dowodowego obligującego operatora do przetworzenia i przekazania temu sądowi danych objętych tajemnicą telekomunikacyjną. Zarówno bowiem w ustawie prawo telekomunikacyjne, jak i w Kodeksie postępowania cywilnego brak jest uregulowań przewidujących taką możliwość. Wprowadzenie przez ustawodawcę ochrony tajemnicy telekomunikacyjnej powoduje natomiast, że odjęta została możliwość pozyskania danych dotyczących użytkownika numeru i danych tzw. transmisyjnych w postępowaniu w sprawach cywilnych jedynie na podstawie imperium przysługującego organowi procesowemu. Dowód taki może natomiast być przeprowadzony na podstawie zgody strony lub osoby, której te dane dotyczą (art. 159 ust. 2 pkt 2)"[43]. W wyroku tym SA wyjaśnił także, że art. 248 i 251 k.p.c. odnoszą się do dowodów z dokumentów i nie mogą być stosowane wprost do dowodów z informacji, a w szczególności dotyczących informacji o połączeniach telefonicznych z określonych numerów telefonów oraz danych dotyczących użytkownika tych numerów[44].

W uchwale z dnia 6 sierpnia 2020 r., III CZP 78/19, SN stwierdził jednak, że sąd jest uprawniony na podstawie art. 159 ust. 2 pkt 4 p.t. – „do żądania od podmiotu związanego tajemnicą telekomunikacyjną informacji pozwalających zweryfikować twierdzenia powoda, że czynu naruszającego dobra osobiste dopuścił się pozwany w sprawie"[45].

## DOSTĘP DO TAJEMNICY KOMUNIKACJI ELEKTRONICZNEJ A OCHRONA DANYCH OSOBOWYCH

W okresie obowiązywania Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[46], zagadnieniem analizowanym w orzecznictwie sądów administracyjnych była możliwość wykorzystania przepisów tej ustawy jako podstawy przekazywania danych osobowych objętych tajemnicą telekomunikacyjną. Zagadnienie to wystąpiło w dwóch sytuacjach:

– w sprawach o udostępnianie danych użytkownika adresu IP dla potrzeb innego postępowania (cywilnego lub karnego),

---

[42] Zob. szerzej M. Rogalski, *Udostępnianie danych telekomunikacyjnych*, „Przegląd Prawa Publicznego" 2019, nr 7–8, s. 31–32.

[43] „Orzecznictwo Sądów Apelacyjnych Apelacji Białostockiej" 2011, nr 1, s. 36. Zob. także M. Janik, *Kwalifikacja dowodowa danych objętych tajemnicą telekomunikacyjną w postępowaniu cywilnym*, „Monitor Prawniczy" 2015, nr 3, s. 158.

[44] Zob. także uchwałę SN z 29 marca 1990 r., sygn. akt III CZP 102/89, „Orzecznictwo Sądu Najwyższego" 1990, nr 10–11, poz. 127; postanowienie SA we Wrocławiu z 30 sierpnia 2010 r., sygn. akt I Acz 1032/10 niepublikowane.

[45] OSNC 2021, nr 2, poz. 7. Zob. krytyczną glosę do tej uchwały K. Sobolewski, *Dopuszczalność uchylenia tajemnicy komunikacyjnej przez sąd cywilny. Glosa do uchwały SN z dnia 6 sierpnia 2020 r., III CZP 78/19*, „Glosa" 2021, nr 3, s. 51–57.

[46] Dz.U. z 2016 r., poz. 922, dalej jako: u.o.d.o.

– w sprawach o udostępnienie straży gminnej (miejskiej) danych osobowych użytkowników telekomunikacji w celu wykonywania określonych prawem zadań realizowanych dla dobra publicznego w związku ze ściganiem wykroczeń.

W pierwszym aspekcie orzecznictwo sądów ewoluowało od uznania, że nie można na podstawie art. 29 ust. 2 a po jego uchyleniu art. 23 ust. 1 pkt 2 lub pkt 5 u.o.d.o. żądać udostępnienia danych osobowych objętych tajemnicą telekomunikacyjną, gdyż wskazany przepis nie zawierał jednoznacznych dyrektyw pozwalających na odkodowanie zakresu znaczeniowego użytego w tym przepisie zwrotu, „jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych". Tymczasem istotą wyjątku od przestrzegania tajemnicy telekomunikacyjnej określonego w p.t. jest właśnie dookreśloność celu czy powodu, przewidzianego jednocześnie w przepisie szczególnym innego aktu prawnego[47]. Podnoszono również, że przepis art. 159 ust. 2 p.t. jest przepisem przewidującym silniejszą ochronnę danych niż przepis art. 23 ust. 1 u.o.d.o. i dlatego to on znajdzie zastosowanie jako podstawa legalizująca przetwarzanie danych objętych tajemnicą telekomunikacyjną. W takiej sytuacji doszłoby więc do częściowego wyłączenia przepisów ustawy o ochronie danych osobowych[48]. Uznano więc, że ochrona przewidziana w przepisach statuujących tajemnicę telekomunikacyjną jest dalej idąca niż rozwiązanie zawarte w u.o.d.o.

Z czasem jednak, być może pod wpływem niezwykle szybkiego rozwinięcia się zjawiska hejtu w internecie, które faktycznie stawało się bezkarne i jednocześnie bardzo dotkliwie, a dotyczyło zarówno pojedynczych osób, jak i całych środowisk, w orzecznictwie NSA zaczął dominować podgląd zawarty m.in. w wyroku z 21 lutego 2014 r., sygn. akt I OSK 2324/12, w którym na tle stosowania przepisów art. 159 ust. 2 pkt 4 p.t. w zw. z art. 23 ust. 1 pkt 2 u.o.d.o. uznano, że „tajemnica telekomunikacyjna, nie jest nieograniczona. Nie sięga przede wszystkim takich działań w sieci, które naruszają obowiązujący porządek prawny. Umożliwienie zatem podejmowania działań zmierzających do naprawy tej sytuacji, w tym też ścigania, i to nie tylko z urzędu, ale i w drodze prywatnego aktu oskarżenia czy domaganie się ochrony dóbr osobistych na drodze cywilnej, jest działaniem w granicach prawa, pozwalającym na zwolnienie z tej ochrony"[49]. W sytuacji więc, gdy po pierwsze, istnieje zarówno w Prawie telekomunikacyjnym lub innym akcie prawnym przepis pozwalający na uchylenie tajemnicy telekomunikacyjnej, a po drugie, takie uchylenie omawianego rodzaju tajemnicy nie budzi wątpliwości – przedsiębiorca telekomunikacyjny powinien ujawnić dane osobowe[50].

Uwzględniając powyższą argumentację, sądy administracyjne akceptowały szeroką możliwość uzyskiwania danych objętych omawianym rodzajem tajemnicy. Podejście to było krytykowane w doktrynie, gdyż pozwalało na „uzyskiwanie danych identyfikujących abonentów i użytkowników usług telekomunikacyjnych

---

[47] Por. wyrok WSA w Warszawie z 28 listopada 2011 r, sygn. akt II SA/Wa 1875/11, Legalis.

[48] Wyrok NSA z 26 stycznia 2009 r, sygn. akt I OSK 174/08, LEX nr 478301.

[49] Centralna Baza Orzeczeń Sądów Administracyjnych („CBOSA"), podobnie wyrok NSA z 29 kwietnia 2020 r., sygn. akt I OSK 4332/18, CBOSA.

[50] Zob. uzasadnienie wyroku NSA z 29 kwietnia 2020 r., I OSK 4332/18, LEX nr 3034351.

oraz świadczonych drogą elektroniczną przez podmioty prywatne nie tylko w sprawach o przestępstwa, lecz także w przypadku dochodzenia roszczeń cywilnych w postępowaniu cywilnym, do czego podstawy prawnej nie mają nawet sądy"[51]. Umożliwienie dostępu do tych danych jest jednak obwarowane dwoma warunkami. Po pierwsze, „umożliwienie podjęcia czynności prawnych zmierzających do ochrony swoich dóbr osobistych na drodze cywilnej jest działaniem w granicach prawa, pozwalającym na odstępstwo od zasady ochrony danych osobowych. Zauważa się przy tym, że w celu udostępnienia danych na potrzeby wniesienia pozwu do sądu przez jednostkę wnioskującą konieczne jest wnikliwe przeanalizowanie i zweryfikowanie przez organ, że zamiar tej jednostki skorzystania z prawa do sądu w konkretnej sprawie jest realny i rzeczywisty"[52]. Pierwszy warunek leży po stronie podmiotu, który złożył wniosek o udostępnienie danych objętych tajemnicą komunikacyjną. Wniosek o udostępnienie danych, aby był skuteczny, powinien być poprzedzony działaniami, które zmierzają do realizacji uprawnień wynikających z prawa karnego lub prawa cywilnego[53] w zakresie obrony dóbr podlegających ochronie prawnej, a wola wszczęcia przez dany podmiot postępowania sądowego nie ma charakteru pozornego[54].

W toku postępowania administracyjnego powinno więc zostać ustalone, „czy u podstaw żądania uczestnika postępowania istotnie leżał cel, jakim było wystąpienie na drogę sądową, a który cechowała aktualność i pewność. O powyższym mogłyby zaś świadczyć podjęte przez uczestnika postępowania konkretne, określone działania, polegające np. na występowaniu do Policji lub Prokuratury z prośbą o udzielenie mu stosownej pomocy w uzyskaniu ochrony dóbr osobistych naruszonych przez autora komentarzy. Wyłącznie tylko deklarowanie, że dane osobowe osoby trzeciej są wnioskodawcy niezbędne, gdyż zamierza on wystąpić z pozwem w stosunku do tej osoby, w obowiązującym stanie prawnym, jest niewystarczające"[55].

Po drugie, warunkiem udostępnienia danych jest zastosowaniem zasady proporcjonalności. Sądy administracyjne uważają, że udostępnienie danych użytkownika Internetu jest możliwe, ale tylko po wyważeniu przeciwstawnych interesów, stosownie do okoliczności każdego przypadku oraz przy należytym uwzględnieniu wymogów wynikających z zasady proporcjonalności. Organy orzekające w tego rodzaju sprawach powinny zatem z urzędu wziąć pod uwagę zarówno interesy podmiotu wnioskującego o żądane informacje, jak i administratora danych oraz – co istotne – podmiotów, których te informacje dotyczą, a które z istoty postępowania o wyjawienie ich danych nie są i nie mogą być czynnie działającymi stronami tego postępowania administracyjnego[56]. Podjęte środki powinny być przede

---

[51] A. Lach, *Uzyskiwanie przez osoby prywatne danych telekomunikacyjnych oraz danych internetowych*, „Państwo i Prawo" 2018, nr 6, s. 72.

[52] Wyrok NSA z 11 grudnia 2018 r., sygn. akt I OSK 398/17, LEX nr 2614892, podobnie wyrok z 10 listopada 2015 r., sygn. akt I OSK 1173/14, CBOSA.

[53] Por. wyrok NSA z 4 grudnia 2014 r., sygn. akt I OSK 978/13, CBOSA.

[54] Por. wyrok NSA z 22 marca 2018 r., sygn. akt I OSK 454/16, CBOSA.

[55] Wyrok NSA z 3 czerwca 2016 r., sygn. akt I OSK 2496/13, CBOSA.

[56] Por. wyrok NSA z dnia 21 sierpnia 2013 r., sygn. akt I OSK 1666/12 CBOSA.

wszystkim adekwatne do celu i nie naruszać innych gwarancji ochronnych, przy których ocenie należy uwzględnić przepisy rangi konstytucyjnej[57].

Kwestią sporną było również przetwarzanie danych osobowych użytkowników usług telekomunikacyjnych w celu wykonywania określonych prawem zadań realizowanych dla dobra publicznego w związku ze ściganiem wykroczeń np. przez straże miejskie i gminne. W tym zakresie orzecznictwo sądów administracyjnych również uległo zmianie. Początkowo w orzecznictwie sądowym wykluczano możliwość udostępnienia danych telekomunikacyjnych w ramach postępowania w sprawach o wykroczenia. W wyroku z dnia 30 sierpnia 2006 r., II SA/Wa 809/05, WSA w Warszawie stwierdził, że ustawodawca nie przewidział możliwości zwolnienia z tajemnicy telekomunikacyjnej w ramach postępowania dotyczącego wykroczenia[58]. Analogicznie w wyroku z 10 października 2006 r., II SA/Wa 642/05, WSA w Warszawie stwierdził, że brak jest podstawy prawnej dopuszczającej przetwarzanie danych osobowych objętych tajemnicą telekomunikacyjną przez straż gminną w toku czynności wyjaśniających prowadzonych w sprawach o wykroczenia[59]. Podobnie w wyroku z 23 kwietnia 2008 r., II SA/Wa 1552/06, WSA w Warszawie stwierdził, że wykładnia celowościowa ostatniego zdania art. 161 p.t. nie przemawia za możliwością udostępnienia tajemnicy telekomunikacyjnej na podstawie art. 23 ust. 1 pkt 2 i 4 u.o.d.o.[60]

W wyroku z 5 lutego 2008 r., I OSK 37/07, NSA uznał jednak, że pomiędzy p.t. a u.o.d.o. nie zachodzi relacja wyłączenia, lecz uzupełnienia. Zdaniem NSA okolicznością usprawiedliwiającą przetwarzanie danych osobowych abonenta przez straż miejską jest niezbędność tej czynności do wykonania określonych prawem zadań realizowanych dla dobra publicznego, związanych z wykryciem sprawcy fałszywych alarmów pożarowych[61]. Ten kierunek wykładni podtrzymał NSA w wyrokach z 19 stycznia 2015 r., I OSK 1099/13[62], oraz z 6 marca 2019 r., sygn. akt I OSK 2677/16, w którym stwierdzono, że „wprawdzie przepisy ustawy o ochronie danych osobowych, prawa telekomunikacyjnego, ustawy o strażach gminnych czy kodeksu postępowania w sprawach o wykroczenia nie stanowią wprost o uprawnieniu straży gminnej do żądania, w przypadku prowadzenia postępowania w sprawie popełnienia wykroczenia, od operatora sieci danych osobowych jej abonenta, takich jak: imię, nazwisko i adres zamieszkania, który jest potencjalnym sprawcą czynu, tym niemniej nie ulega wątpliwości, iż takie uprawnienie straż gminna/miejska jednak posiada"[63]. Zdaniem NSA wykładnia przepisów regulujących omawianą materię nie może bowiem prowadzić do paraliżu organu,

---

[57] Zob. analizę prawnych podstaw dostępu do danych objętych tajemnicą telekomunikacyjną na podstawie przepisów o ochronie danych osobowych w artykule: A. Lach, *Uzyskiwanie przez osoby prywatne danych telekomunikacyjnych oraz danych internetowych*, „Państwo i Prawo" 2018, nr 6, s. 67 i n.

[58] Wyrok WSA w Warszawie z dnia 30 sierpnia 2006 r., II SA/Wa 809/05, Legalis.

[59] Wyrok WSA w Warszawie z 10 października 2006 r., II SA/Wa 642/05, Legalis.

[60] Wyrok WSA w Warszawie z 23 kwietnia 2008 r., II SA/Wa 1552/06, Legalis.

[61] Wyrok NSA z 5 lutego 2008 r., I OSK 37/07, Legalis.

[62] Wyrok NSA z 19 stycznia 2015 r., I OSK 1099/13, Legalis.

[63] Wyrok NSA z 6 marca 2019 r., sygn. akt I OSK 2677/16, CBOSA.

mającego ustawowe kompetencje do m.in. ścigania sprawców wykroczeń. Zgodnie bowiem z art. 11 Ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych[64] straż jest powoływana przez samorząd gminny m.in. w celu: ochrony spokoju i porządku w miejscach publicznych, a także ochrony obiektów komunalnych i urządzeń użyteczności publicznej  Dla zrealizowania tych zadań straż posiada wiele uprawnień, do których należy m.in. prawo do legitymowania osób w uzasadnionych przypadkach w celu ustalenia tożsamości osób, w stosunku co do których zachodzi podejrzenie popełnienia przez nie czynu zabronionego (art. 12 u.s.g.). Oczywiście powyższe uprawnienia nie odnoszą się wprost do prawa żądania ujawnienia przez operatora sieci danych osobowych abonenta, który jest potencjalnym sprawcą wykroczenia, ale zakres tych uprawnień straży gminnej (miejskiej) ewidentnie dowodzi, że jest to podmiot mający – z mocy ustawy – prawo do naruszania w określonych sytuacjach wolności i prywatności osób, a więc praw chronionych konstytucyjnie. Wyższość dobra publicznego w określonych sytuacjach wymaga bowiem podporządkowania praw przysługujących jednostce. Z kolei w myśl treści art. 17 Ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia[65] straż gminna jest jednym z wymienionych w katalogu oskarżycieli publicznych w sprawach o wykroczenia, a więc przyznano jej również uprawnienie do przeprowadzenia czynności wyjaśniających w celu ustalenia, czy istnieją podstawy do wystąpienia z wnioskiem o ukaranie oraz zebrania danych niezbędnych do sporządzenia wniosku o ukaranie (art. 54–56a k.p.w.). Przy czym – w myśl art. 54 ust. 1 *in fine* k.p.w. – wskazane czynności wyjaśniające powinny być w miarę możności podejmowane w miejscu popełnienia czynu bezpośrednio po jego ujawnieniu i zakończone w ciągu miesiąca. W sprawach o ściganie wykroczeń niezmiernie ważnym czynnikiem jest więc czas, który wpływa na skuteczność działania. Wykonywanie przez straż gminną lub miejską zadań i obowiązków wymaga zatem wykorzystywania informacji o osobach, których działania te dotyczą. Prowadzi to do wniosku, że przepisy ustawy o strażach gminnych stanowią o uprawnieniu straży do przetwarzania danych w związku z wykonywaniem powierzonych temu organowi zadań, bez konieczności uzyskiwania na to zgody osoby, której dane te dotyczą. Tym bardziej że, zgodnie z rt.. 10a ust. 1 u.s.g., straż w celu realizacji ustawowych zadań może przetwarzać dane osobowe, z wyłączeniem danych sensytywnych. Stąd sądy administracyjne przyjęły, że straże gminne są uprawnione do pozyskiwania danych objętych klauzula tajemnicy komunikacyjnej w sprawach o wykroczenia na podstawrt.art. 23 ust. 1 pkt 2 u.o.d.o.

Podkreślić należy, że wobec takiego samego brzemienia poprzednio obowiązujących art. 23 ust. 1 pkt 2 i pkt 5 u.o.d.o. oraz obecnie obowiązujących art. 6 ust. 1 lit. c i f RODO przytoczone wyżej poglądy sądów administracyjnych nadal zachowują swoją aktualność[66], a zatem znajdą one zastosowanie w obecnym stanie prawnym.

---

[64] Tj. Dz. U. z 2019 r. poz. 1795 ze zm., dalej jako: u.s.g.

[65] Dz.U. z 2021 r., poz. 457 ze zm., dalej jako: k.p.w.

[66] Por. wyrok NSA z dnia 20 kwietnia 2021 r., sygn. akt III OSK 161/21, LEX nr 3169386, podobnie uważa P. Fajgielski, w: *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób*

Przepis art. 381 ust. 2 PKE zezwala na przetwarzanie danych z innych powodów określonych ustawą lub przepisami odrębnymi, a przepis art. 381 ust. 3 PKE zezwala tylko w przypadkach określonych w ustawie[67]. Przepis art. 381 ust. 2 pkt 4 PKE dopuszcza nie tylko przetwarzanie danych osobowych na podstawie przepisów PKE, ale także na podstawie innych przepisów, w tym RODO. W zakresie przetwarzania danych osobowych przepisy art. 381 ust. 2 pkt 4 i ust. 3 PKE oraz przepisy art. 6 ust. 1 lit. c i e w zw. z ust. 3 RODO zawierają podobne odesłania określające dozwolony zakres przetwarzania danych, poprzez odwołanie się do uprawnień, obowiązków i zadań realizowanych w interesie publicznym wynikających z innych przepisów prawa.

Zbieg przepisów PKE i RODO w sprawie przetwarzania danych osobowych został uregulowany w RODO. Zgodnie z art. 95 RODO rozporządzenie nie nakłada dodatkowych obowiązków na osoby fizyczne ani prawne co do przetwarzania w związku ze świadczeniem ogólnodostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii w sprawach, w których podmioty te podlegają szczegółowym obowiązkom mającym ten sam cel, określonym w dyrektywie o prywatności. W sprawach, które nie zostały uregulowane w RODO, odpowiedni przepis rozporządzenia stanowi dostateczną podstawę przetwarzania danych osobowych przez przedsiębiorcę telekomunikacyjnego. Zauważa się, że z treści tego przepisu wynika, iż w zakresie, w jakim przepisy te regulują materię uregulowaną w dyrektywie, nie powinny ulegać zmianie, nawet gdyby w drodze wykładni wskazywać miała na to treść RODO. Mówiąc jeszcze inaczej, można wskazać, że konsekwencją wskazanej w komentowanym przepisie relacji RODO do dyrektywy 2002/58/WE jest to, że przepisy implementujące tę dyrektywę nie będą mogły zostać uznane za niezgodne z RODO, nawet jeżeli dotyczą przetwarzania danych osobowych objętych RODO[68], a zatem można uznać, że relacja pomiędzy RODO a przepisami implementującymi dyrektywę 2002/58/WE jest jak między *lex generali* a *lex specialis*[69]. Przepisy krajowe, a zatem i projektowanego PKE, powinny mieć pierwszeństwo w stosowaniu przed rozwiązaniami przyjętymi w RODO.

Pomimo, wydawałoby się, dość jasnej regulacji zawartej w art. 95 RODO, granica pomiędzy danymi osobowymi w rozumieniu RODO a danymi telekomunikacyjnymi określonymi w art. 381 ust. 1 pkt 3–5 PKE nie jest jednoznaczna. Wiele danych telekomunikacyjnych umożliwia przedsiębiorcy telekomunikacyjnemu łatwe zidentyfikowanie abonenta lub użytkownika końcowego, co w świetle art. 4 pkt 1 RODO przemawia za traktowaniem takich danych jako danych osobowych[70].

---

*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)*, w: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, wyd. II*, LEX 2022, art. 6.

[67] Zob. także P. Fajgielski, *Ochrona danych osobowych w telekomunikacji – aspekty prawne*, Lublin 2003, s. 235.

[68] Por. M. Górski, w: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Legalis 2018, kom. do art. 95.

[69] Por. W. Chomiczewski, M. Czerniawski, w: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 1128.

[70] Zob. na gruncie wcześniejszych przepisów: P. Litwiński, *Ochrona prywatności i tajemnicy telekomunikacyjnej w nowym Prawie telekomunikacyjnym*, w: *Vademecum nowego prawa telekomunikacyjnego*, Warszawa 2004, s. 69.

Zgodnie z wyrokiem WSA w Warszawie z 3 lutego 2010 r., II SA/Wa 1598/09[71], adres IP stanowi dane osobowe, gdy jest na stałe przypisany do określonego urządzenia, użytkowanego przez określony podmiot. NSA w wyroku z 19 maja 2011 r., I OSK 1079/10[72], wskazał, że tam, gdzie adres IP jest na dłuższy okres przypisany do konkretnego urządzenia, a urządzenie to przypisane jest konkretnemu użytkownikowi, należy uznać, że stanowi on dane osobowe, jest to bowiem informacja umożliwiająca identyfikację konkretnej osoby fizycznej. Zależność ta powoduje, że w określonych sytuacjach istnieje możliwość identyfikacji tego podmiotu. Podobnie TSUE w wyroku z 19 października 2016 r., sygn. akt C-582/14, *Breyer v. Bundesrepublik Deutschland*, jednoznacznie przesądził, że „dynamiczny adres protokołu internetowego (adres IP) zarejestrowany przez dostawcę usług medialnych online przy okazji przeglądania przez daną osobę strony internetowej, którą dostawca ten udostępnia publicznie, stanowi, wobec tego dostawcy dane osobowe"[73].

## DOSTĘP DO DANYCH OBJĘTYCH TAJEMNICĄ TELEKOMUNIKACYJNĄ NA PODSTAWIE PRZEPISÓW O DOSTĘPIE DO INFORMACJI PUBLICZNEJ

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej[74] statuuje w art. 1 ust. 1, że każda informacja o sprawach publicznych jest informacja publiczną. Przepis ten wraz z art. 6 u.d.i.p. określa bardzo szeroki zakres przedmiotowy pojęcia „informacja publiczna" i choć budzi on pewne kontrowersje i spory[75] – to wydaje się, że w pełni akceptuje się stanowisko, iż dotyczy on działalności organów władzy publicznej osób pełniących funkcje publiczne w zakresie wykonywania przez nie spraw publicznych – to zarówno „działalność organów władzy publicznej, jak i wskazanych wcześniej samorządów oraz osób i jednostek organizacyjnych w zakresie wykonywania zadań władzy publicznej oraz gospodarowania mieniem komunalnym lub mieniem Skarbu Państwa"[76]. Treść art. 1 ust. 1 wskazuje zatem, że intencją ustawodawcy było takie określenie informacji publicznej, aby każdy sposób wykonywania władztwa państwowego zarówno w sferze społecznej, politycznej, jak i gospodarczej mógł zostać poddany kontroli społecznej za pomocą narzędzi określonych w ustawie o dostępie do informacji publicznej.

W orzecznictwie sądów administracyjnych wskazuje się, że przedsiębiorcy telekomunikacyjni są zobowiązani w obszarze prowadzonej przez nich działalności do udostępnienia danych na zasadach określonych w przepisach określających obowiązki związane z obronnością, bezpieczeństwem państwa oraz bezpieczeń-

[71] Wyrok WSA w Warszawie z 3 lutego 2010 r., II SA/Wa 1598/09, Legalis.

[72] Wyrok NSA z 19 maja 2011 r., I OSK 1079/10, Legalis.

[73] https://curia.europa.eu/juris/liste.jsf?num=C-582/14&language=PL (dostęp: 22.12.2021).

[74] Dz.U. z 2020 r., poz. 2176, dalej jako: u.d.i.p.

[75] Por. P. Szustakiewicz, *Problemy dostępu do informacji publicznej na tle orzecznictwa sądów administracyjnych*, „Samorząd Terytorialny" 2015, nr 4, s. 58–71.

[76] I. Kamińka, M. Rozbicka-Ostrowska, *Ustawa o dostępie do informacji publicznej. Komentarz*, Warszawa 2016, s. 23.

stwem i porządkiem publicznym (art. 176 i n. p.t.)[77]. Rynek telekomunikacyjny jest rynkiem regulowanym, na którym rolę regulatora pełni Prezes Urzędu Komunikacji Elektronicznej. Poza wskazanymi wcześniej obowiązkami przedsiębiorcy telekomunikacyjni realizują jeszcze wiele innych obowiązków wynikających z prawa telekomunikacyjnego lub na żądanie Prezesa UKE. W zakresie realizacji tych obowiązków, przy uwzględnieniu przepisów p.t., Prezes UKE może być zobowiązany do udostępnienia informacji w trybie dostępu do informacji publicznej.

Prawo dostępu do informacji publicznej nie ma jednak charakteru nieograniczonego. Wynika to wprost z art. 5 ust. 1 u.d.i.p., według którego podlega ono ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych. Do takich tajemnic zalicza się również tajemnicę telekomunikacyjną[78]. Niewątpliwie zatem w sytuacji, gdy w ramach dostępu do informacji publicznej żądane dane dotyczą informacji objętych tajemnicą telekomunikacyjną, Prezes UKE powinien zgodnie z art. 16 ust. 1 u.d.i.p. wydać decyzję o odmowie dostępu do informacji publicznej. Decyzja taka podlega kontroli instancyjnej i sądowej.

## SANKCJE ZA NARUSZENIE OBOWIĄZKU ZACHOWANIA TAJEMNICY TELEKOMUNIKACYJNEJ

Zgodnie z art. 441 ust. 1 pkt 79 PKE, kto narusza obowiązek zachowania tajemnicy komunikacji elektronicznej, podlega karze pieniężnej. Kara pieniężna przewidziana jest także za używanie automatycznych systemów wywołujących lub używanie telekomunikacyjnych urządzeń końcowych dla celów przesyłania niezamówionej informacji handlowej bez uprzedniego uzyskania zgody abonenta lub użytkownika końcowego (art. 441 ust. 1 pkt 83 PKE). Kary pieniężne nakłada Prezes UKE, w drodze decyzji, w wysokości do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym. Decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności (art. 442 ust. 1 PKE). Niezależnie od kar pieniężnych Prezes UKE może nałożyć na kierującego przedsiębiorstwem telekomunikacyjnym, w szczególności osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy telekomunikacyjnego lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy (art. 441 ust. 4 PKE).

Kara może zostać nałożona także na podstawie innych niż PKE przepisów. Kara grzywny za przesyłanie za pomocą środków komunikacji elektronicznej niezamówionych informacji handlowych może być nałożona na podstawie art. 24 ust. 1

[77] Wyrok NSA z 4 grudnia 2015 r. sygn. akt I OSK 1898/14, CBOSA podobnie wyrok NSA z 2 grudnia 2015 r., sygn. akt I OSK 289/15, CBOSA oraz wyrok WSA w Warszawie z 16 października 2015 r., sygn. akt II SAB/Wa 718/15, CBOSA.

[78] Por. wyrok NSA z 10 stycznia 2014 r., sygn. akt I OSK 2075/13, LEX nr 1456978, wyroki WSA w Warszawie z 5 grudnia 2013 r., sygn. akt VIII SA/Wa 621/13, LEX nr 1408050 i z 23 maja 2012 r., sygn. akt VIII SA/Wa 160/12, LEX nr 1276055.

Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r., poz. 344 ze zm.), w sytuacji braku zgody abonenta lub użytkownika końcowego na przesyłanie takich informacji.

## WNIOSKI

Skonstruowane w PKE postanowienia w zakresie tajemnicy komunikacji elektronicznej są generalnie zgodne ze standardem konstytucyjnej zasady ochrony tajemnicy komunikowania się. Nie zachodzi konflikt pomiędzy postanowieniami PKE a RODO. Brak także takiego konfliktu pomiędzy tajemnicą komunikacji elektronicznej a prawem dostępu do informacji publicznej. Nie budzi bowiem wątpliwości, że dane objęte tajemnicą komunikacji elektronicznej nie mogą podlegać ujawnieniu w trybie określonym przez ustawę o dostępie do informacji publicznej.

## BIBLIOGRAFIA

Bojańczyk A., *Karnoprawne aspekty ochrony praw pracownika do tajemnicy komunikowania się, cz. I*, „Palestra" 2003, nr 1–2.

Chomiczewski W., Czerniawski M., w: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Czubkowska S., *Afera Cambridge Analitica. Facebook wybrał Amerykanom prezydenta. Czy nam też wybierze? I jeszcze na tym zarobi*, https://wyborcza.pl/7,156282,23182834,afera-cambridge-analytica-facebook-wybral-amerykanom.html.

Fajgielski P., w: *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*, w: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, wyd. II*, LEX 2022.

Fajgielski P., *Ochrona danych osobowych w telekomunikacji – aspekty prawne*, Lublin 2003.

Florczak-Wątor M., w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, LEX 2019.

Garlicki L. (red.), *Konstytucja Rzeczpospolitej Polskiej. Komentarz*, t. II, Warszawa 2002.

Garlicki L., Wojtyczek K., w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom II, wyd. II*, red. M. Zubik, LEX 2016.

Górski M., w: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Legalis 2018.

Granger M.P., Irion K., *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, „European Law Review" 2014, nr 39 (6).

Hoc S., *Glosa do uchwały SN z 22.1.2003 r., I KZP 45/02*, „Przegląd Sądowy" 2003, nr 11–12.

Husovec M., *First European Constitutional Court Suspends Data Retention after the Decision of the Court of Justice of EU*, The Center for Internet and Society, 8 April 2014, http://cyberlaw.stanford.edu/blog/2014/04/first-european-constitutional-court-suspends-data-retention-after-decision-court.

Janik M., *Kwalifikacja dowodowa danych objętych tajemnicą telekomunikacyjną w postępowaniu cywilnym*, „Monitor Prawniczy" 2015, nr 3.

Kamińka I., Rozbicka-Ostrowska M., *Ustawa o dostępie do informacji publicznej. Komentarz*, Warszawa 2016.

Kawałek K., Rogalski M. (red.), *Prawo telekomunikacyjne. Komentarz*, Warszawa 2010.

Konarski X., *Wpływ Europejskiego kodeksu łączności elektronicznej na ochronę danych osobowych i prywatności użytkowników usług OTT-1 (usług łączności interpersonalnej)*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2020, nr 1.

Mednis A., *Ochrona danych osobowych w świetle dyrektywy UE z 12 lipca 2002 roku o prywatności w komunikacji elektronicznej*, „Prawo i Ekonomia w Telekomunikacji" 2002, nr 4.

Misztal-Konecka J., Konecki J., *Billing jako dowód w postępowaniu w sprawach o wykroczenia*, „Państwo i Prawo" 2010, nr 7.

Lach A., *Uzyskiwanie przez osoby prywatne danych telekomunikacyjnych oraz danych internetowych*, „Państwo i Prawo" 2018, nr 6.

Litwiński P., *Ochrona prywatności i tajemnicy telekomunikacyjnej w nowym Prawie telekomunikacyjnym*, w: *Vademecum nowego prawa telekomunikacyjnego*, Warszawa 2004.

Milaj J., *Invalidation of the Data Retention Directive – Extending the Proportionality Test*, „Computer Law & Security Review" 2015, nr 31.

Opaliński B., *Tajemnica komunikowania się w Konstytucji RP*, w: *Gromadzenie i udostępnianie danych telekomunikacyjnych*, red. P. Brzeziński, B. Opaliński, M. Rogalski, Warszawa 2016.

Peers S., *The Data Retention Judgment: The CJEU Prohibits Mass Surveillance*, EU Law Analysis, 8 April 2014, http://eulawanalysis.blogspot.fi/2014/04/the-data-retention-judgment-cjeu.html.

Piątek S., Piątek P., *Anonimizacja danych objętych tajemnicą telekomunikacyjną*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2014, nr 8.

Piątek S., *Prawo telekomunikacyjne. Komentarz*, Warszawa 2019.

Roberts A., *Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications*, „Modern Law Review" 2015, nr 78 (3).

Rogalski M., *Udostępnianie danych telekomunikacyjnych*, „Przegląd Prawa Publicznego" 2019, nr 7–8.

Safjan M., Bosek L. (red.), *Konstytucja RP, t. I, Komentarz do art. 1–86*, Legalis 2016.

Sarnecki P. (red.), *Prawo konstytucyjne RP*, Warszawa 2011.

Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej. Komentarz, wyd. VII*, LEX 2013.

Sobolewski K., *Dopuszczalność uchylenia tajemnicy komunikacyjnej przez sąd cywilny. Glosa do uchwały SN z dnia 6 sierpnia 2020 r., III CZP 78/19*, „Glosa" 2021, nr 3.

Szustakiewicz P., *Problemy dostępu do informacji publicznej na tle orzecznictwa sądów administracyjnych*, „Samorząd Terytorialny" 2015, nr 4.

Tomkiewicz M., *Sądowa kontrola pozyskiwania danych telekomunikacyjnych, internetowych i pocztowych*, „Państwo i Prawo" 2018, nr 4.

Tracey S., *The Fall of the Data Retention Directive*, „Communications Law" 2015, nr 20 (2).

## POJĘCIE I ZAKRES TAJEMNICY KOMUNIKACJI ELEKTRONICZNEJ

Streszczenie

W polskim prawie funkcjonuje od kilkunastu lat pojęcie tajemnicy telekomunikacyjnej, które zostało zdefiniowane w ustawie prawo telekomunikacyjne. Przedmiotem artykułu będzie ana-

liza, czy uregulowania w tym zakresie spełniają wymagania konstytucyjnej zasady ochrony tajemnicy komunikowania się oraz jaka jest ich relacja do przepisów o ochronie danych osobowych. Analiza w szczególności dotyczyć będzie postanowień poświęconych tajemnicy komunikacji elektronicznej w projekcie ustawy prawo komunikacji elektronicznej, który został przygotowany w związku z wejściem w życie Europejskiego kodeksu łączności elektronicznej.

Słowa kluczowe: tajemnica komunikowania się, tajemnica telekomunikacyjna, tajemnica komunikacji elektronicznej, ochrona danych osobowych, dostęp do informacji publicznej

## THE DEFINITION AND SCOPE OF ELECTRONIC COMMUNICATIONS SECRET

Summary

The concept of telecommunications secret, defined in the Telecommunications Act, has been in use in Polish law for several years. In connection with the entry into force of the European Electronic Communications Code, a draft Act on Electronic Communications was prepared, which includes provisions on the secrecy of electronic communications. The subject of the article will be to analyze whether the proposed regulations meet the requirements of the constitutional principle of the protection of confidentiality of communication and what is their relation to the provisions on the protection of personal data.

Keywords: communication secret, telecommunications secret, electronic communication secret, personal data protection, access to public information

Cytuj jako: Rogalski M., Szustakiewicz P., *Pojęcie i zakres tajemnicy komunikacji elektronicznej*, „Ius Novum" 2022 (16) nr 1, s. 59–82. DOI: 10.26399/iusnovum.v16.1.2022.4/m.rogalski/p.szustakiewicz

Cite as: Rogalski M., Szustakiewicz P. (2022) 'The definition and scope of electronic communications secret'. *Ius Novum* (Vol. 16) 1, 59–82. DOI: 10.26399/iusnovum.v16.1.2022.4/m.rogalski/p.szustakiewicz