MATERIAŁY SZKOLENIOWE

Beata Rodak[1]

Pozaprocesowe i procesowe uzyskiwanie danych internetowych

Streszczenie

W artykule poruszono kwestię uzyskiwania danych internetowych w trybie pozaprocesowym oraz procesowym. Przedstawiono główne problemy związane z udostępnianiem tych danych, omówiono przesłanki uzyskiwania danych oraz wskazano podmioty legitymowane do uzyskiwania danych internetowych. Przedstawiono także standardy konstytucyjne oraz europejskie uzyskiwania danych z powołaniem się na najważniejsze orzeczenia.

Słowa kluczowe

Dane internetowe, cyberprzestrzeń, cyberbezpieczeństwo, Internet.

1. Wstęp

Dane internetowe stanowią źródło istotnych informacji, które mogą okazać się pomocne w toku czynności operacyjno-rozpoznawczych oraz w procesie karnym. Pojęcie danych internetowych mieści w swym zakre-

[1] Beata R o d a k, mgr prawa, absolwentka Wydziału Prawa i Administracji UMK w Toruniu, aplikant adwokacki III roku przy ORA w Łodzi. Autorka pracy magisterskiej pt. „Pozaprocesowe i procesowe uzyskiwanie danych internetowych", przedstawionej do Konkursu o nagrodę I Zastępcy Prokuratora Generalnego – Prokuratora Krajowego w 2021 r. ORCID: 0000-0003-3114-5061.

sie dane osobowe oraz tzw. dane eksploatacyjne, które odnoszą się do sposobu korzystania z usługi przez usługobiorcę.

Zagadnienie uzyskiwania danych internetowych wzbudza kontrowersje. Z jednej strony należy zważyć, że odebranie służbom możliwości pozyskiwania danych internetowych prowadziłoby do trudnych do rozwiązania sytuacji, z drugiej zaś strony należy mieć na uwadze, iż możliwość uzyskiwania danych internetowych stanowi ingerencję w prawa i wolności jednostki, gwarantowane jej na gruncie Konstytucji RP oraz prawa europejskiego. Orzecznictwo i praktyka wykształciły standardy, które demokratyczne państwo musi spełniać, aby efektywnie chronić takie wartości, jak chociażby bezpieczeństwo i porządek publiczny, a jednocześnie w jak najmniejszym stopniu i w sposób najmniej dotkliwy ingerować i naruszać prawo do prywatności jednostki.

2. Gwarancje konstytucyjne i europejskie a uzyskiwanie danych internetowych

Konstytucja RP nie odnosi się wprost do funkcjonowania człowieka w wirtualnej rzeczywistości[2]. *De lege lata* nie istnieje przepis rangi konstytucyjnej, który statuowałby szczególne regulacje przewidziane dla usługobiorców korzystających z sieci Internet. Ustrojodawca zrezygnował z wyodrębnienia przepisów dotyczących użytkowników Internetu. Nie oznacza to jednak, że ochrona konstytucyjnych praw i wolności jednostki w związku z korzystaniem z sieci Internet podlega zróżnicowaniu w stosunku do ochrony przewidzianej dla tradycyjnych form komunikowania się. Tym samym, nie sposób traktować danych przekazywanych internetowo jako funkcjonujących niejako obok konstytucyjnej ochrony praw i wolności jednostki.

Ustrojodawca konkretyzuje, które sfery życia podlegają ochronie na gruncie ustawy zasadniczej. Wśród wskazanych w Konstytucji sfer podlegających ochronie, znajdują się m.in.: tajemnica komunikowania się oraz autonomia informacyjna, stanowiące komponent prawa do prywatności[3]. Wspomniane gwarancje mają niebagatelne znaczenie również dla uzyskiwania danych internetowych, bowiem zakres omawianych wolności i dopuszczalne ingerencje oraz ograniczenia tych gwarancji, stanowią wyznacznik legalnego uzyskiwania danych internetowych oraz determinują możliwość ich gromadzenia przez uprawnione do tego podmioty.

[2] Wyrok TK z dnia 30 lipca 2014 r., sygn. K 23/11, Legalis nr 994752.
[3] *Ibidem*.

Zasada wykreowana przez art. 49 Konstytucji RP polega na zapewnieniu wolności i ochrony tajemnicy komunikowania się każdej jednostki. Ta wolność implikuje jednocześnie istnienie zakazu zmuszania adresatów do ujawnienia treści korespondencji, jak również zakazu podejmowania prób ingerencji w tajemnicę komunikowania się bez zgody osób komunikujących się[4]. Ponadto tajemnica ta zakresem swym obejmuje poufność co do faktu bycia adresatem określonych treści oraz przekazów[5]. Warto przy tym wskazać, że omawiana gwarancja chroni nie tylko treść przekazywanych informacji, ale także wszelkie dane uczestników procesu komunikowania się, dane o wybieranych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń oraz umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP[6], a zatem również dane internetowe. Z konstrukcji ochrony tajemnicy komunikowania się można wyinterpretować zasadę, w myśl której żaden podmiot poza osobami, które się komunikują, nie powinien mieć dostępu do informacji stanowiących przedmiot komunikatu, jak również co do informacji dotyczących samego faktu komunikowania się przez określone osoby, jak również nie powinien czynić z tych informacji użytku[7]. Władza publiczna jest obowiązana do stworzenia mechanizmów zapewniających gwarancję tej ochrony.

Wolność i ochrona tajemnicy komunikowania się nie ma jednak charakteru bezwzględnego. Wynika to z drugiego zdania analizowanego przepisu, choć stanowi ono *superfluum*, ponieważ już z brzmienia art. 31 ust. 3 Konstytucji RP wynika, że prawa i wolności jednostek gwarantowane przez Konstytucję mogą podlegać ograniczeniom. Ustrojodawca nie zdecydował się na uczynienie z tej wolności *ius infinitum.* Ograniczenie wskazanej wolności może nastąpić jedynie w przypadkach wskazanych w ustawie oraz w sposób w niej określony.

W szczególności uzasadnione jest wprowadzenie ograniczeń w sytuacji, w której korzystanie z wolności prowadziłoby do naruszenia innych praw i wolności oraz wartości, które chroni Konstytucja[8]. Podkreśla się

[4] P. Sarnecki, Komentarz do art. 49, (w:) L. Garlicki, M. Zubik (red.), Konstytucja Rzeczypospolitej Polskiej, Komentarz. Tom II, Warszawa 2016, s. 260–263.
[5] *Ibidem*.
[6] Wyrok TK z dnia 30 lipca 2014 r., sygn. K 23/11…
[7] B. Opaliński, Tajemnica komunikowania się w Konstytucji RP, (w:) P. Brzeziński (red.), Gromadzenie i udostępnianie danych telekomunikacyjnych, Warszawa 2016, s. 7.
[8] B. Banaszak, Konstytucja RP. Komentarz do art. 49, Warszawa 2012, s. 306. Zob. też: W. Skrzydło, Komentarz do art. 49 KRP, (w:) W. Skrzydło (red.), Konstytucja Rzeczypospolitej Polskiej. Komentarz, SIP LEX 2019.

również, że regulacje mające za przedmiot ograniczanie praw i wolności jednostek, powinny być poddawane kontroli ze strony sądu[9].

Kolejną gwarancją konstytucyjną, istotną z uwagi na możliwość uzyskiwania danych internetowych jest autonomia informacyjna określona w art. 51 ust. 1–2 Konstytucji RP, statuująca z jednej strony wolność jednostki do decydowania o tym, czy, komu i jakie dane dotyczące swojej osoby ujawni, a z drugiej kreująca zakaz po stronie innych podmiotów do żądania udzielenia informacji na temat danej jednostki bez podstawy prawnej. *Expressis verbis* wskazano władze publiczne, zakazując im pozyskiwania, gromadzenia oraz udostępniania innych informacji niż niezbędne w demokratycznym państwie.

Uwzględnienia wymaga różnica zakresu podmiotowego. Artykuł 51 ust. 1 Konstytucji stanowi bowiem, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania danych o sobie. Oznacza to, że beneficjentem omawianej gwarancji jest w istocie każda jednostka niezależnie od tego, czy posiada obywatelstwo polskie, czy status cudzoziemca. Jest to rozwiązanie znamienne dla właściwie każdej z wolności gwarantowanych konstytucyjnie. Wyjątek stanowi regulacja art. 51 ust. 2 KRP. Ustrojodawca wskazał, że władze publiczne nie mogą zbierać danych dotyczących obywateli. Nie sposób jednakże wysnuwać z treści przepisu przyzwolenia na pozyskiwanie, gromadzenie i udostępnianie informacji przez władze publiczne o cudzoziemcach. Ochrony należy wszak upatrywać w regulacji art. 47 KRP. Przyjąć należy, że cudzoziemcom również przysługiwać będzie gwarancja niemożności pozyskiwania zbędnych danych dotyczących wskazanych wyżej osób. Ograniczenia omawianej wolności, podobnie jak w odniesieniu do art. 49 KRP, muszą czynić zadość wymogom określonym w przepisie artykułu 31 Konstytucji RP. Ograniczenia te nie mogą jednakże naruszać istoty wolności i praw. Przepisy powinny określać przypadki, w jakich może nastąpić ograniczenie, a także wskazywać, w jaki sposób ograniczenie to należałoby realizować[10]. Jest to związane z optymalizacyjnym charakterem zasad konstytucyjnych[11]. Nietrudno bowiem wyobrazić sobie sytuację, w której ochrona praw i wolności określonych osób może wymagać ingerencji w tożsame prawa i wolności innych osób.

[9] *Ibidem*.

[10] Wyrok TK z dnia 12 stycznia 2000 r., sygn. P 11/98, OTK 2000, nr 1, poz. 3.

[11] Opinia RPO do projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy nr 154), https://www.rpo.gov.pl/sites/default/files/Do_Marszalka_Sejmu.pdf (dostęp: 11 lutego 2022 r.).

Rzecznik Praw Obywatelskich, dalej: Rzecznik, zakwestionował zgodność z Konstytucją przepisów dotyczących uzyskiwania przez służby danych abonenckich. Zarzucił im przede wszystkim brak precyzji, co do celu gromadzenia danych. Rzecznik podnosił ponadto, że regulacje te nie odnoszą się do kategorii osób, co do których warunkiem koniecznym jest respektowanie tajemnicy zawodowej. Rzecznik zwrócił również uwagę, że przepisy regulujące pracę służb nie czynią zadość zasadzie subsydiarności, adekwatności i proporcjonalności. Krytykował ponadto brak wystarczającej kontroli nad uzyskiwaniem danych. RPO zwrócił uwagę również na nieokreśloność regulacji dotyczących uzyskiwania danych przez służby, które – jako ingerujące w sferę prywatności jednostki – muszą być unormowane w sposób właściwy w ustawie. Ponadto, słusznie zauważono, że uzyskiwanie danych internetowych przez służby powinno stanowić *ultima ratio.* Kwestionowanie zgodności z Konstytucją RP przepisów dotyczących uzyskiwania danych abonenckich przez służby było również przedmiotem wniosku Prokuratora Generalnego[12], który, podobnie jak Rzecznik, zarzucał przepisom regulującym pracę służb nieproporcjonalną ingerencję w podstawowe prawa i wolności jednostek.

Trybunał Konstytucyjny w wyroku z dnia 30 lipca 2014 r., sygn. K 23/11 stwierdził niezgodność z Konstytucją przepisów dotyczących uzyskiwania danych przez uprawnione służby. Przede wszystkim swoje rozstrzygnięcie oparł na braku niezależnej kontroli nad uzyskiwaniem danych internetowych. Trybunał nie zakwestionował konieczności uzyskiwania danych, podkreślając, że stanowi to istotne narzędzie w walce z przestępczością, jednak regulacja nie jest regulacją bez wad i konieczne są zmiany[13].

W systemie prawa Rady Europy również nie przewidziano przepisów odnoszących się odrębnie do funkcjonowania jednostki w Internecie. Europejska Konwencja Praw Człowieka, dalej: EKPC[14] gwarantuje w ramach prawa do prywatności, prawo do poszanowania korespondencji prywatnej. Wolność ta, wyrażona w art. 8 EKPC interpretowana jest jako gwarancja niezakłóconej i niecenzurowanej komunikacji między jednost-

[12] Wniosek Prokuratora Generalnego do TK w sprawie stwierdzenia niezgodności z Konstytucją przepisów dotyczących uzyskiwania danych telekomunikacyjnych przez służby, dołączony do sprawy o sygn. K 23/11, https://ipo.trybunal.gov.pl/ipo/dok?dok=F1770459731% 2FK_29_11_Wns_2011_08_01.pdf (dostęp: 11 lutego 2022 r.).

[13] Wyrok TK z dnia 30 lipca 2014 r., sygn. K 23/11…

[14] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r., Nr 61, poz. 284).

kami[15]. Konwencja ustanowiła niezwykle wysoki próg ochrony poszanowania korespondencji, ponieważ nie obowiązuje w tym zakresie reguła *de minimis* i każda ingerencja stanowi naruszenie wolności komunikowania się[16]. Prawo, które statuuje art. 8 EKPC, ma przede wszystkim za zadanie ochronę jednostek przed arbitralną ingerencją władz[17].

Prawo do prywatności oraz związane z nim prawo do poszanowania korespondencji, nie mają jednakże na gruncie EKPC charakteru absolutnego i mogą podlegać ograniczeniom. Wynika to wprost z brzmienia art. 8 ust. 2 EKPC. Na gruncie art. 8 ust. 1 EKPC ukształtowało się bogate orzecznictwo. Analiza judykatów dotyczących wskazanej regulacji pozwala ustalić zakres oraz treść tajemnicy korespondencji w systemie prawa Rady Europy. Warto zwrócić uwagę, że Europejski Trybunał Praw Człowieka (dalej: ETPC) nie zanegował dopuszczalności niejawnego pozyskiwania przez władze publiczne informacji o jednostkach[18], dostrzegł konieczność ingerowania w tę wolność z uwagi na ochronę bezpieczeństwa oraz instytucji demokratycznego państwa prawa[19]. Trybunał jednocześnie wskazał, że regulacje ingerujące w prawo wykreowane na gruncie art. 8 EKPC powinny być wysoce precyzyjne, zarówno w odniesieniu do podstaw, jak i zakresu ingerencji. Co więcej, ETPC podniósł, że państwa powinny regulować omawiane kwestie w sposób klarowny. Bogate orzecznictwo ETPC wykreowało minimalne standardy dotyczące ingerowania przez władze publiczne w proces komunikowania się[20].

Po pierwsze, ETPC podkreślił, że elementem koniecznym do ingerowania w prawo do poszanowania prywatności, jest wskazanie rodzaju przestępstw, w odniesieniu do których możliwe jest uzyskiwanie danych dotyczących jednostki[21]. W sprawie Iordachi i in. przeciwko Mołdawii[22], ETPC stwierdził naruszenie art. 8 EKPC, ponieważ na gruncie mołdawskiego prawodawstwa niejawne uzyskiwanie danych było możliwe w celu zapobiegania poważnym, bardzo poważnym i wyjątkowo poważnym przestępstwom. W ocenie ETPC rozwiązanie to było niewystarczające z uwagi

[15] I. R o a g n a, Ochrona prawa do poszanowania życia prywatnego i rodzinnego w Europejskiej Konwencji o Ochronie Praw Człowieka, Strasburg 2012, s. 34.
[16] *Ibidem*.
[17] M. N o w i c k i, Komentarz do Konwencji o ochronie praw człowieka i podstawowych wolności. Komentarz do art. 8, (w:) M. N o w i c k i (red.), Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka, Warszawa 2017, s. 625.
[18] M. R o g a l s k i, Kontrola…, s. 62.
[19] *Ibidem*.
[20] *Ibidem*.
[21] *Ibidem*.
[22] Wyrok ETPC z dnia 10 lutego 2009 r., skarga nr 25198/02, Legalis nr 129445.

na jakość regulacji[23]. Trybunał w przywołanym wyroku podkreślił, że niewystarczającym jest wskazanie, iż chodzi o poważne przestępstwa, nawet jeśli ustawa definiuje to pojęcie[24]. ETPC postulował, by regulacje możliwie jak najdokładniej określały katalog przestępstw, których popełnienie uzasadnia sięganie po dane przez służby oraz niejawną inwigilację jednostek.

ETPC wskazał również, że koniecznym jest określenie kategorii podmiotów, w odniesieniu do których możliwe jest pozyskiwanie informacji. W sprawie Amman przeciwko Szwajcarii[25], Trybunał zwrócił uwagę na to, że choć ustawa wskazywała, jakie podmioty mogą być objęte kontrolą, to nie zawierała jakichkolwiek środków ostrożności, co stanowiło naruszenie konwencyjnego wymogu zgodności z prawem. W ocenie ETPC konieczne jest uregulowanie procedury dotyczącej uzyskiwania danych przez służby w taki sposób, by uniemożliwiała ona ingerencję w prawa i wolności osób, co do których uzyskiwanie danych nie jest możliwe. Z całą pewnością może być tu mowa o podmiotach, które związane są tajemnicą zawodową, jak chociażby adwokaci, radcowie prawni czy lekarze. Ponadto, ETPC wskazał, że należy dokładnie określić maksymalny czas stosowania niejawnej kontroli wobec jednostki.

Ponadto, ETPC zwrócił uwagę na konieczność prawidłowego uregulowania procedury wyrażenia zgody na stosowanie środka niejawnej kontroli, która powinna mieć charakter aprioryczny i nie może ograniczać się jedynie do kwestii statystycznych czy *stricte* formalnych. Zgoda powinna pochodzić od niezależnego organu. Kontrola o charakterze aposteriorycznym nie jest wystarczająca i nie czyni zadość wymogom stawianym przez ETPC. Trybunał podniósł także konieczność wprowadzenia regulacji określających środki ostrożności, które wykluczą dowolne i niekompletne przekazywanie danych przez uprawnione służby.

W sprawie Association for European Integration and Human Rights and Ekimdzhiev przeciwko Bułgarii[26], ETPC stwierdził, że ustawodawstwo Bułgarii nie spełniało konwencyjnego wymogu jakości prawa, ponieważ nie regulowało w dostatecznym stopniu kwestii dotyczących postępowania z zebranymi danymi i informacjami, jak również należytego ich zabezpieczania i sposobu niszczenia.

[23] Decyzja ETPC z dnia 5 kwietnia 2005 r. w sprawie Iordachi i in. przeciwko Mołdawii, skarga nr 25198/02.
[24] *Ibidem*.
[25] Wyrok Wielkiej Izby z dnia 16 lutego 2000 r., nr skargi 27798/95, https://www.legal-tools.org/doc/6e49ed/pdf/ (dostęp: 17 lutego 2022 r.).
[26] Wyrok ETPC z dnia 28 czerwca 2007 r., nr skargi 62540/00, Legalis nr 122649.

Minimalny standard konwencyjny to również konieczność poinformowania osoby, której dane uzyskano o tym fakcie. Zwraca się jednak uwagę, że poinformowanie o prowadzonych działaniach może nastąpić wówczas, gdy nie stanowi zagrożenia dla celów stosowanego środka, często więc będzie możliwe *ex post*, aczkolwiek rozwiązanie takie należy ocenić pozytywnie, gdyż uprzednie poinformowanie o prowadzonych działaniach przez służby wobec konkretnej osoby, może uniemożliwić realizację celu, dla którego działania są prowadzone.

Warto zauważyć, że w ocenie ETPC, ochrona wynikająca z art. 8 ust. 1 EKPC, rozciąga się również na informacje dotyczące dat oraz długości przychodzących połączeń. W sprawie Malone przeciwko Zjednoczonemu Królestwu[27], ETPC stwierdził, że bezprawne użycie danych z billingu może być postrzegane jako naruszenie prawa wynikającego z art. 8 ust. 1 EKPC, gdyż dane tam zawarte stanowią integralny element procesu komunikowania się.

Warto poświęcić uwagę również tzw. Cyberkonwencji[28], dalej: Konwencja, umowa międzynarodowa, regulującej szereg zagadnień związanych z danymi internetowymi. Przywołana Konwencja została ratyfikowana przez Polskę w 2015 r. Cyberkonwencja ma na celu utworzenie jednolitych rozwiązań dotyczących przeciwdziałania cyberprzestępczości. Omawiana umowa międzynarodowa nie tylko kreuje katalog przestępstw komputerowych, ale zawiera też rozwiązania procesowe, w tym, w szczególności, precyzuje zasady współpracy międzynarodowej. Cyberkonwencja ogranicza przeszkodę podwójnej karalności przy stosowaniu pomocy prawnej między państwami. Ma to ogromne znaczenie z uwagi na fakt, że w przypadku niespełnienia wymogu podwójnej karalności, uzyskanie dowodów od innego państwa, w którym czyn nie jest penalizowany, jest często utrudnione[29]. Rozwiązaniem zasługującym na szczególną uwagę, jest zawarty w umowie wymóg dotyczący utworzenia czynnych 24/7 ośrodków, których celem ma być zapewnienie pomocy w sprawach dotyczących cyberprzestępczości. Co interesujące, również na gruncie tej umowy deklaruje się konieczność prowadzenia niezależnej kontroli nad zabezpieczonymi danymi oraz należycie uzasadniać ingerencję w podstawowe wolności obywatelskie w procesie zabezpieczania i gromadzenia danych cyfrowych. Konwencja nie przesądza, jakiego rodzaju środki mają przedsię-

[27] Decyzja ETPC z dnia 23 maja 2002 r., nr skargi 39026/97, Legalis nr 201560.

[28] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r., poz. 728).

[29] A. Lach, Karnoprocesowe instrumenty zwalczania pedofilii i pornografii dziecięcej w Internecie, Prok. i Pr. 2005, nr 10, s. 52–62.

wziąć państwa będące jej stronami. Stanowi jedynie o „odpowiednich środkach", pozostawiając dużą swobodę państwom.

Na gruncie prawa UE zagwarantowano jednostce ochronę życia prywatnego, w tym komunikowania się oraz ochronę danych osobowych.

W myśl art. 16 ust. 1 Traktat o Funkcjonowaniu Unii Europejskiej, dalej: TFUE[30] każda jednostka ma prawo do ochrony danych osobowych. Przepis ten dotyczy przetwarzania danych osobowych zarówno w sektorze prywatnym, jak i publicznym, w tym także w zakresie policyjnej współpracy[31]. Regulacja ta koresponduje z uregulowaniem art. 8 Karty Praw Podstawowych Unii Europejskiej, dalej: KPPUE[32] stojącym na straży ochrony danych osobowych jednostki, których przetwarzanie jest możliwe za zgodą osoby, której dane dotyczą lub na uzasadnionej podstawie przewidzianej przez przepis ustawy. Ponadto, na gruncie art. 7 KPPUE prawodawca unijny zapewnia każdemu prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się.

W odniesieniu do prawa wtórnego UE, na szczególną uwagę zasługuje dyrektywa z dnia 12 lipca 2002 r.[33] Dyrektywa ta zapewnia ochronę podstawowych praw i wolności, w szczególności życia prywatnego, poufności komunikacji oraz ochrony danych osobowych w sektorze łączności elektronicznej. Gwarantuje ona również swobodny przepływ danych związanych z łącznością elektroniczną w UE. W myśl art. 5 ust. 1 dyrektywy o łączności, państwa członkowskie zapewniają na gruncie ustawodawstwa krajowego poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. W szczególności zakazuje się słuchania, nagrywania, jak również przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatów i związanych z nimi danymi o ruchu bez zgody użytkowników. Z kolei art. 6 dyrektywy o łączności kreuje nakaz usunięcia lub zanonimizowania danych zbędnych. Od przywołanych regulacji istnieje jednakże wyjątek, który statuuje art. 15

[30] Traktat o Funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 326/47).

[31] A. Grzelak, Prawo do ochrony danych osobowych a konieczność walki z przestępczością. Uwagi na tle art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, (w:) S. Dudzik, N. Półtorak (red.), Prawo Unii Europejskiej a prawo konstytucyjne państw członkowskich, Warszawa 2013, s. 407.

[32] Karta Praw Podstawowych Unii Europejskiej z dnia 7 grudnia 2000 r. (Dz. Urz. UE C Nr 83 z 2010 r. ze zm.).

[33] Dyrektywa o łączności, dyrektywa z dnia 12 lipca 2002 r. – Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz UE. L 201 z 2002 r., s. 37–47).

ust. 1 tego aktu prawnego, a mianowicie państwom członkowskim zostało przyznane uprawnienie do ograniczenia ustawowego zakresu praw i obowiązków wynikających z regulacji art. 5 i 6 dyrektywy pod warunkiem, że ograniczenia są niezbędne oraz proporcjonalne a ponadto właściwe dla społeczeństwa demokratycznego do zapewnienia bezpieczeństwa państwa, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej. Artykuł 15 ust. 1 upoważnia ponadto państwa członkowskie do uchwalenia środków ustawodawczych, na podstawie których możliwe będzie przechowywanie danych przez uzasadniony czas. Jednocześnie wskazuje się, że środki te powinny być zgodne z ogólnymi zasadami prawa UE[34].

Duże znaczenie należy przypisać wyrokowi w sprawie Digital Rights Ireland[35]. Na kanwie przywołanej sprawy Trybunał Sprawiedliwości Unii Europejskiej, dalej: TSUE stwierdził nieważność dyrektywy retencyjnej. Podstawą takiego rozstrzygnięcia było przede wszystkim to, że zdaniem TSUE dyrektywa nie respektowała w sposób należyty zasady subsydiarności[36]. TSUE podkreślił w wyroku szereg mankamentów dyrektywy retencyjnej, zwróciwszy uwagę na zbyt szeroki zakres zarówno podmiotowy dyrektywy i gromadzonych na jej podstawie danych, a tym samym brak wyłączeń podmiotowych wobec osób, które są objęte tajemnicą zawodową, przez brak kryteriów określenia najpoważniejszych przestępstw, które uzasadniałyby dostęp do danych oraz wymogów dotyczących apriorycznej kontroli, co implikowało w istocie brak gwarancji ochrony przed nadużyciami[37]. W Zjednoczonym Królestwie do brytyjskiego Sądu Najwyższego wpłynął wniosek o zbadanie zgodności z przepisami regulacji dotyczącej obowiązku retencyjnego. Decyzją Prezesa TSUE sprawę tę połączono ze sprawą C-203/15. Wyrok ten ma duże znaczenie, ponieważ aktualizuje on konieczność zweryfikowania, jakie przestępstwa powinny legalizować i umożliwiać korzystanie ze zgromadzonych danych. Konieczność ta jest wynikiem wymogu proporcjonalności. Kluczowym okazuje się przeanali-

[34] Opinia w sprawie zgodności z prawem UE poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw, http://orka.sejm.gov.pl/Druki8ka.nsf/0/B30BB05699C73CE8C1257F310040516D/%24File/154-001.pdf (dostęp: 11 lutego 2022 r.), s. 5.

[35] Wyrok TSUE z dnia 8 kwietnia 2014 r., https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN (dostęp: 11 lutego 2022 r.).

[36] A. L a c h, Obowiązek retencji danych telekomunikacyjnych i udostępniania tych danych organom ścigania, MoP 2017, nr 11, s. 612.

[37] Uwagi Helsińskiej Fundacji Praw Człowieka, *op. cit*.

zowanie przydatności uzyskiwania danych internetowych, gromadzonych przez służby i organy.

TSUE wskazał ponadto, że ustawodawstwo krajowe musi spełniać szereg warunków, by móc ingerować w prawo do prywatności jednostek. W ocenie Trybunału ustawodawstwo krajowe powinno opierać się na obiektywnych dowodach, które są powiązane z daną grupą osób i służą zwalczaniu poważnej przestępczości i poważnych zagrożeń. TSUE w sposób stanowczy odniósł się również do konieczności uregulowania przesłanek materialnych i formalnych dotyczących postępowania z danymi. Za niewystarczające uznano odwołanie się wyłącznie do jednego z celów wykreowanych na gruncie art. 15 dyrektywy o łączności. TSUE zwrócił szczególną uwagę na kwestię zagwarantowania organom państwowym dostępu do danych. W ocenie Trybunału, aby warunki te zostały spełnione, dostęp do danych uzyskiwanych przez te organy powinien być poddawany uprzedniej kontroli sądu. Obowiązek kontroli dezaktualizuje się wyłącznie w wypadkach niecierpiących zwłoki. Ponadto TSUE podkreślił, że należy informować osobę, której dane zgromadzono, możliwie jak najszybciej, by zagwarantować należytą ochronę jej praw[38].

3. Pozaprocesowe uzyskiwanie danych internetowych

Ustawodawca legitymował do uzyskiwania danych internetowych w ramach czynności operacyjno-rozpoznawczych służby o charakterze wywiadowczym, kontrwywiadowczym, policyjnym, skarbowym i specjalnym, a uprawnienie to zostało każdorazowo wykreowane na gruncie poszczególnych pragmatyk. Możliwość uzyskiwania danych internetowych, oprócz Policji (art. 20c ustawy o Policji[39]) przysługuje jeszcze Straży Granicznej (art. 10b ustawy o Straży Granicznej[40]), Krajowej Administracji Skarbowej (art. 114 ust. 1 ustawy o Krajowej Administracji Skarbowej[41]), Żandarmerii Wojskowej (art. 30 ust. 1 Ustawy o Żandarmerii Wojskowej[42]), Agencji Bezpieczeństwa Wewnętrznego oraz

[38] A. L a c h, Obowiązek…, s. 613.

[39] Ustawa z dnia 6 kwietnia 1990 r. o Policji (tekst jedn. Dz. U. z 2021 r., poz. 1882, 2333, 2447, 2448).

[40] Ustawa z dnia 12 października 1990 r. o Straży Granicznej (tekst jedn. Dz. U. z 2021 r., poz. 1486, 1728, 1898, 2191, 2333).

[41] Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (tekst jedn. Dz. U. z 2021 r., poz. 422, 464, 694, 802, 815, 954, 1003, 1005, 1718, 2076, 2105).

[42] Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (tekst jedn. Dz. U. z 2021 r., poz. 1214).

Agencji Wywiadu (art. 28 ust. 1 Ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[43]), Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (art. 32 ust. 1 Ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego[44]), Centralnemu Biurowi Antykorupcyjnemu (art. 18 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym[45]), Służbie Ochrony Państwa (art. 57 ust. 1 ustawy o Służbie Ochrony Państwa[46]).

W piśmiennictwie wskazuje się, że tryb uzyskiwania danych internetowych w toku czynności operacyjno-rozpoznawczych wymaga od Policji rzetelności, sumienności, ale również postuluje się szybkość działania ze strony usługodawców świadczących usługi drogą elektroniczną[47].

Artykuł 20c ustawy o Policji był przedmiotem częstych nowelizacji. Początkowo, na gruncie analizowanego przepisu, ustawodawca statuował wyłącznie przesłankę zapobiegania i wykrywania przestępstw[48]. Przesłanka wykrywania i zapobiegania przestępstwom skarbowym pojawiła się dopiero w wyniku wejścia w życie ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[49].

Już *prima facie*, daje się zauważyć ogólny charakter tych przesłanek oraz – przede wszystkim – brak zamkniętego katalogu przestępstw, których popełnienie uzasadniałoby sięgnięcie przez Policję po dane internetowe. Przyjąć zatem należy, że na gruncie art. 20c ustawy o Policji, mowa jest o każdym przestępstwie, jakie zostało stypizowane w k.k. oraz w k.k.s. Bez znaczenia pozostaje ustawowe zagrożenie karą, jak również to, czy przestępstwo stanowi występek, czy jest ono zbrodnią. Uzyskiwa-

[43] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jedn. Dz. U. z 2021 r., poz. 2333).
[44] Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (tekst jedn. Dz. U. z 2021 r., poz. 2333).
[45] Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (tekst jedn. Dz. U. z 2021 r., poz. 1671, 2333).
[46] Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (tekst jedn. Dz. U. z 2019 r., poz.
[47] W. K o t o w s k i, Ustawa o Policji. Komentarz praktyczny, Warszawa 2004, s. 409.
[48] J. W ó j c i k, Przeciwdziałanie przestępczości zorganizowanej. Zagadnienia prawne, kryminologiczne i kryminalistyczne, Warszawa 2011, s. 195.
[49] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r., poz. 125 ze zm.).

nie danych internetowych nie jest jednakże możliwe w celu zapobiegania lub wykrywania wykroczeń[50].

Analiza pierwszej z przesłanek prowadzi do konkluzji, że uzyskanie danych internetowych przez Policję na podstawie art. 20c ustawy o Policji musi być celowe i prowadzić do wykrycia lub zapobieżenia przestępstwu. Przepis nie statuuje wymogu uzyskiwania danych internetowych wyłącznie w uzasadnionych przypadkach obawy popełnienia przestępstwa.

Kolejna przesłanka wprowadzona przez ustawodawcę na gruncie art. 20c to przesłanka ratowania życia lub zdrowia ludzkiego. I w tym przypadku ustawodawca zastosował alternatywę łączną i rozwiązanie to należy ocenić pozytywnie, gdyż, gdyby przyjąć dla analizowanej treści alternatywę rozłączną, rozwiązanie to dotknięte byłoby błędem logicznym. Przez czasownik „ratować', którego użyto w omawianej regulacji, należy rozumieć udzielanie komuś pomocy w niebezpieczeństwie lub trudnej sytuacji[51]. Ponadto, przesłanka ta zazębia się w pewnym zakresie z przesłanką zapobiegania przestępstwom, gdyż ratowanie życia lub zdrowia ludzkiego może polegać na odparciu niebezpieczeństwa polegającego na popełnieniu przestępstwa. Jednakże przesłanka ta ma w istocie szerszy zakres, gdyż należy mieć na względzie, iż ratowanie życia lub zdrowia ludzkiego może również polegać na odparciu niebezpieczeństwa, które nie zostało spowodowane w wyniku popełnienia przestępstwa.

Regulacja przepisu art. 20c ustawy o Policji kreuje jeszcze jedną przesłankę, zgodnie z którą Policja może żądać udostępnienia danych internetowych w celu wsparcia działań poszukiwawczych lub ratowniczych. Warto podkreślić, że ustawa o Policji nie definiuje pojęcia takich działań, jak również nie odsyła w tym zakresie do innych przepisów. Definicja działań ratowniczych została zawarta w ustawie o ochronie przeciwpożarowej[52]. Zgodnie z art. 2 pkt 2 wspomnianej ustawy, działania ratownicze stanowią każdą czynność podjętą w celu ochrony życia, zdrowia, mienia lub środowiska, a także likwidację przyczyn powstania pożaru, wystąpienia klęski żywiołowej lub innego miejscowego zagrożenia. Z kolei działania poszukiwawcze, są prowadzone w sprawach poszukiwania osób ukrywających się przed organami ścigania i wymiaru sprawiedliwości w postępowaniach prowadzonych przez ABW oraz zaginionych w niewyjaśnionych okoliczno-

[50] Z. G ą d z i k, Tajemnica telekomunikacyjna, (w:) Ł. C z e b o t a r i in. (red.), Komentarz. Ustawa o Policji, Warszawa 2015, s. 286–292.

[51] S. D u b i s z, Uniwersalny słownik języka polskiego, t. 3, P–Ś, Warszawa 2003, s. 889–890.

[52] Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (tekst jedn. Dz. U. 2021, poz. 869, 2490).

ściach, jeżeli zaginięcie może stwarzać zagrożenie dla bezpieczeństwa państwa (§ 1 pkt 2 zarządzenia Szefa ABW[53]).

Warto zwrócić uwagę, że ustawodawca nie przewidział w omawianym przepisie jakichkolwiek ograniczeń podmiotowych, oznacza to, że Policja może uzyskiwać dane internetowe dotyczące każdej osoby, nie wyłączając osób związanych tajemnicą zawodową, jak np. adwokaci czy radcowie prawni oraz lekarze.

Ustawodawca wykreował na gruncie omawianego przepisu dwa sposoby uzyskiwania danych internetowych przez Policję. Szczegółowe wymagania co do wniosków, sprzętu oraz oprogramowania są przedmiotem decyzji KGP[54].

Konkretyzując, pierwszy ze sposobów polega na tym, że usługodawca udostępnia dane internetowe policjantowi wskazanemu w pisemnym wniosku jednego z komendantów albo osoby przez nich upoważnionej bądź na ustne żądanie policjanta posiadającego pisemne upoważnienie wskazanych wyżej osób[55].

Ponadto uzyskiwanie danych internetowych może odbywać się za pomocą sieci telekomunikacyjnej, w sposób zdalny poza siedzibą usługodawcy, bez udziału pracowników usługodawcy bądź przy ich niezbędnym udziale, który winien być ograniczony do minimum[56]. W ten sposób uzyskiwać dane może policjant wyposażony w pisemne upoważnienie KGP, Komendanta CBŚP, Komendanta BSWP i komendanta wojewódzkiego.

Przepisy nie precyzują, w jakim terminie udostępnienie ma nastąpić, jednakże należy przyjąć, że powinno to nastąpić bez zbędnej zwłoki, w możliwie najkrótszym czasie, tak, by nie narazić danych na zniekształcenie bądź ich utratę, tak by skutecznie zwalczyć przestępczość oraz udzielić pomocy osobom znajdującym się w niebezpieczeństwie. Co więcej, przepis wskazuje, że usługodawca udostępnia dane na żądanie organu Policji, oznacza to zatem obligatoryjne udostępnienie tych danych. Ustawodawca uniemożliwił usługodawcy odmowę udostępnienia danych.

Zgodnie z treścią art. 20c ust. 8 ustawy o Policji, udostępnienie tej formacji danych internetowych za pośrednictwem sieci telekomunikacyj-

[53] Zarządzenie nr 5 Szefa ABW z dnia 17 marca 2010 r. w sprawie form i metod wykonywania przez Samodzielną Sekcję Poszukiwawczą Departamentu Postępowań Karnych ABW czynności poszukiwawczych (Dz. Urz. ABW.2010.1.3).

[54] Decyzja nr 34 KGP z dnia 19 lutego 2018 r. zmieniająca decyzję w sprawie uzyskiwania i przetwarzania przez Policję danych telekomunikacyjnych, pocztowych oraz internetowych (Dz. Urz. poz.27).

[55] B. Opaliński i in., Zakres uprawnień Policji. Komentarz do art. 20c, (w:) B. Opaliński i in. (red.), Ustawa o Policji. Komentarz, Warszawa 2015, s. 156–164.

[56] B. Opaliński i in., Zakres…, s. 156–164.

nej jest możliwe, jeśli możliwość taką przewiduje porozumienie zawarte między KGP a usługodawcą.

Ponadto, by uzyskanie danych mogło odbyć się za pomocą bezpiecznego łącza, wymagane jest, by sieci zapewniały możliwość ustalenia tożsamości osoby uzyskującej dane, rodzaj uzyskiwanych danych oraz czas, w którym zostały pobrane. Wymaga się również, by sieci te były odpowiednio zabezpieczone, tak technicznie, jak i organizacyjnie. Zabezpieczenie powinno uniemożliwiać osobie nieuprawnionej dostęp do danych. Dostęp do danych za pomocą sieci telekomunikacyjnej jest ponadto możliwy, jeżeli jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Policji albo prowadzonych przez nie czynności[57].

Ustawodawca nałożył obowiązek na KGP, Komendanta CBŚP, Komendanta BSWP i komendanta wojewódzkiego Policji prowadzenia w formie elektronicznej rejestrów wystąpień o uzyskanie danych internetowych. Rejestry muszą być prowadzone z zachowaniem przepisów o ochronie informacji niejawnych.

Kontrolę nad uzyskanymi danymi internetowymi sprawuje sąd okręgowy właściwy miejscowo dla siedziby organu Policji, który dane uzyskał. W ramach kontroli, organ Policji, któremu udostępniono dane składa sądowi sprawozdanie. Takie sprawozdanie organ Policji jest zobligowany przedkładać sądowi w półrocznych okresach. W sprawozdaniu należy wskazać liczbę przypadków pozyskania danych internetowych oraz rodzaj tych danych, a także kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych. Sąd okręgowy może jednakże zapoznać się z materiałami w ramach kontroli, gdy uzna to za konieczne. Sąd w ciągu 30 dni informuje organ Policji o wynikach kontroli. Przepisy jednakże nie konkretyzują, czy i jakiego rodzaju konsekwencje ponieść może organ Policji, który zwrócił się po dane lub je wykorzystał w sytuacji, gdy kontrola zakończy się wynikiem negatywnym.

4. Uzyskiwanie danych internetowych w trybie procesowym

Analiza przepisów ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego[58] pokazuje, że ustawodawca nie poświęcił należytej

[57] M. R o g a l s k i, Kontrola…, s. 208–232.
[58] Tekst jedn. Dz. U. z 2021 r., poz. 534 ze zm., dalej k.p.k.

uwagi kwestii uzyskiwania danych internetowych na potrzeby procesu karnego. Próżno bowiem szukać w k.p.k. przepisu, który mógłby odnosić się do omawianej kwestii. Oczywistym jest jednak, że pewna ułomność regulacji nie może oznaczać, iż uzyskiwanie danych internetowych w toku procesu karnego jest niemożliwe. Warto jednak zwrócić uwagę na istnienie luki prawnej w tej materii. Dla porównania, kwestia uzyskiwania danych telekomunikacyjnych została uregulowana przez ustawodawcę wprost w przepisie art. 218 k.p.k. Ustawodawca zawarł tam zamknięty katalog podmiotów obowiązanych do udostępnienia danych, pomijając usługodawców w rozumieniu ustawy o świadczeniu usług drogą elektroniczną[59].

Należy zatem podjąć rozważania, czy odpowiednie stosowanie art. 218 k.p.k. w zw. z art. 236a k.p.k., mogłoby stanowić podstawę do wystąpienia z żądaniem udostępnienia danych internetowych. Przepis art. 218 k.p.k. wprost wskazuje na obowiązek udostępnienia danych przez enumeratywnie wskazane w nim podmioty. Z uwagi na powyższe, nie ma możliwości odpowiedniego zastosowania tego przepisu w zw. z art. 236a k.p.k. do danych internetowych. Stosowanie takiej podstawy uzyskiwania danych internetowych prowadziłoby do niedopuszczalnego rozszerzenia zamkniętego katalogu podmiotów obowiązanych do ich udostępnienia. Obecnie najwłaściwszym wydaje się więc upatrywanie podstawy do uzyskiwania danych internetowych w oparciu o przepis art. 217 k.p.k. w zw. z art. 236a k.p.k. Przepis art. 217 k.p.k. stanowi wprost o rzeczach, jednakże jego zastosowanie w zw. 236a k.p.k., w odniesieniu do danych internetowych, jawi się jako trafne rozwiązanie.

Na gruncie regulacji art. 217 k.p.k. ustawodawca jako główną przesłankę zatrzymania rzeczy przewidział aspekt dowodowy[60], a zatem uzyskiwanie danych możliwe jest w przypadku posiadania przez uprawniony organ informacji, że mają one znaczenie dla ustaleń faktycznych w toczącym się postępowaniu karnym. Należy przy tym zaznaczyć, że w omawianej regulacji nie zapisano, iż zachodzi uzasadniona podstawa do twierdzenia, że dane podlegające zatrzymaniu mają pożądany walor dowodowy. Warto, dla porównania wskazać chociażby regulację art. 219 k.p.k., gdzie ustawodawca napisał wprost, że przeprowadzenie przeszukania może mieć miejsce w przypadku zaistnienia uzasadnionej podstawy pozwalającej przypuszczać, że rzeczy znajdują się w konkretnym

[59] Ustawa z dnia 18 lipca 2004 r. o świadczeniu usług drogą elektroniczną (tekst jedn. Dz. U. z 2020 r., poz. 344).

[60] D. Jagiełło, Taktyka kryminalistycznych czynności dowodowych, Warszawa 2019, s. 145.

miejscu[61]. Zupełna dowolność w gromadzeniu danych niepowiązanych ze śledztwem groziłaby odpowiedzialnością dyscyplinarną lub karną osobie, która działałaby w taki sposób.

Należy jednak zwrócić uwagę, że przed uzyskaniem danych internetowych organy procesowe *de facto* nie mają pełnej wiedzy dotyczącej ich treści, jak również brak im pewności, czy konkretne dane internetowe będą mogły stanowić dowód w sprawie. Na podstawie innych środków lub źródeł dowodowych zakładają natomiast, że konkretne informacje mają znaczenie dla sprawy. W przypadku uzyskiwania danych internetowych na potrzeby procesu karnego, będzie konieczna dwuetapowa ocena ich przydatności. Pierwsza – aprioryczna, gdy organ poweźmie informację, że dane internetowe mogą pomóc w ustaleniu istotnych okoliczności popełnienia przestępstwa, a nawet doprowadzić do ujęcia sprawcy i jego skazania oraz druga – ocena aposterioryczna, polegająca na wnikliwej analizie uzyskanych danych oraz stwierdzeniu ich przydatności, jeśli posiadają walor dowody lub chociażby wykrywczy[62].

Z uwagi na regulację zawartą w art. 217 k.p.k., warunkiem *sine qua non* wystąpienia przez uprawnione podmioty z żądaniem udostępnienia danych internetowych, jest toczące się postępowanie karne oraz związek danych internetowych (nawet hipotetyczny) z tymże postępowaniem. Nieuzasadnione będzie wystąpienie z takim żądaniem przed wszczęciem postępowania, jak i po jego prawomocnym zakończeniu. Należy wskazać, że w chwili wystąpienia z żądaniem udostępnienia danych musi istnieć stan zawisłości sprawy (*lis pendens*). Bez znaczenia pozostaje jednakże, czy postępowanie jest w fazie *in rem*, czy *ad personam*.

Regulacja art. 227 k.p.k. przewiduje konieczność zachowania umiaru przy dokonywaniu czynności zatrzymania danych. Zatrzymanie powinno odbyć się zgodnie z celem tej czynności oraz w sposób, który nie wyrządzi niepotrzebnych szkód i dolegliwości. To pozytywne rozwiązanie, gdyż hołduje naczelnym zasadom, jakie powinny towarzyszyć ingerencji w prawa i wolności jednostki, tj. zasadzie celowości oraz adekwatności. Oznacza to, że podmioty uprawnione do uzyskiwania danych internetowych powinny mieć na uwadze te wytyczne i nie stosować instytucji uzyskiwania danych internetowych, gdy nie jest to podyktowane sytuacją konieczną.

W aspekcie podjętego tematu wspomnieć należy o rudymentarnych zasadach, tj. zasadzie subsydiarności i proporcjonalności. Dane internetowe mogące mieć znaczenie dla sprawy powinny być pozyskiwane do-

[61] R. Z d y b e l, Funkcja wykrywcza i dowodowa postępowania karnego, Warszawa 2016, s. 216.
[62] M. R o g a l s k i, Kontrola…, s. 91.

piero w przypadku, gdy okoliczności faktyczne badanego zdarzenia nie sposób ustalić bez ich wykorzystania[63]. Ponadto, działanie takie musi charakteryzować celowość, która oznacza, że udostępnienie wspomnianych danych jest dokonywane wyłącznie dla realizacji celu ustawowego, jakim jest wykrycie sprawcy i pociągnięcie go do odpowiedzialności za popełnione przestępstwo. Oprócz celowości, uzyskiwanie danych internetowych charakteryzować musi konieczność i adekwatność. Konieczność oznacza, że bez uzyskania takich informacji osiągnięcie realizacji opisanego ustawowego celu nie jest możliwe; adekwatność zachodzi wtedy, gdy działanie jest dopuszczalne, bowiem mniej inwazyjne środki uniemożliwiają rozstrzygnięcie o przedmiocie postępowania[64].

Konsekwencją przyjęcia jako podstawy prawnej do uzyskiwania danych internetowych w trybie procesowym art. 217 k.p.k. w zw. z art. 236a k.p.k., jest poszerzenie katalogu podmiotów uprawnionych do uzyskiwania danych internetowych w porównaniu do art. 218 k.p.k., statuującego podstawę do uzyskiwania m.in. danych telekomunikacyjnych. Ustawodawca wskazał wprost w przepisie art. 217 k.p.k., że podmiotami uprawnionymi do żądania wydania rzeczy są sąd i prokurator. Uprawnienie do wystąpienia z żądaniem udostępnienia danych przez sąd i prokuratora nie jest skorelowane z koniecznością wystąpienia wypadku niecierpiącego zwłoki. Z kolei w wypadkach niecierpiących zwłoki, uprawnienie to przysługuje także Policji i innym organom. Należy zaznaczyć, że w przypadku uzyskiwania danych internetowych, uprawnienie Policji będzie aktualizowało się często, z uwagi na podatność danych internetowych na manipulację oraz łatwość ich utraty, co niejednokrotnie będzie stanowiło ów wypadek niecierpiący zwłoki. Dodać należy, że przypadek niecierpiący zwłoki będzie równie często podyktowany celami wykrywczymi, tj. dążeniem do niezwłocznego ujęcia sprawcy po popełnieniu przez niego przestępstwa, a przynajmniej jego ustalenia.

Należy jednak z całą stanowczością podkreślić, że uprawnienie to jest uprawnieniem ograniczonym i ma charakter warunkowy. Legitymacja ta dotyczy zatem ekstraordynaryjnych sytuacji. Za wypadek niecierpiący zwłoki uznać należy sytuację, w której zachodzi niebezpieczeństwo utraty lub zniekształcenia dowodu. Oprócz Policji, uprawnienie to przysługiwać będzie, w oparciu o art. 312 § 1 k.p.k., również następującym organom: Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Krajowej Administracji Skarbowej, Centralnemu Biurowi Antykorupcyjnemu,

[63] J. S k o r u p k a, Komentarz do art. 217 k.p.k., (w:) J. S k o r u p k a (red.), Kodeks postępowania karnego. Komentarz, SIP Legalis 2019.
[64] *Ibidem*.

Żandarmerii Wojskowej. Ponadto, oprócz wskazanych *expressis verbis* organów, należy wskazać, że uprawnienia te przysługują również innym podmiotom na podstawie ustaw szczególnych.

De lege lata uzyskiwanie danych internetowych w trybie procesowym jest możliwe przez odpowiednie stosowanie przepisów rozdziału 25 k.p.k. i może mieć miejsce w odniesieniu do dysponenta i użytkownika systemu informatycznego na podstawie art. 236a k.p.k.[65]

Przepis art. 217 k.p.k. przewiduje dwie formy wydania rzeczy: dobrowolne wydanie rzeczy przez osobę, w której władztwie się znajduje oraz przymusowe odebranie rzeczy w razie odmowy wydania[66]. Z uwagi jednakże na odpowiednie stosowanie tej regulacji w zw. z art. 236a k.p.k. oraz mając na względzie ustawowy obowiązek udostępnienia danych internetowych organom prowadzącym postępowanie, należy przyjąć, iż w praktyce dochodzi najczęściej do dobrowolnego udostępnienia danych przez usługodawcę.

Procedurę uzyskiwania danych internetowych w procesie karnym inicjuje powzięcie informacji, że dane takie istnieją i kto jest w ich posiadaniu, co skwitowane zostaje wydaniem stosownego postanowienia skierowanego do dostawcy usługi sieciowej.

Żądanie to, w omawianej sytuacji będzie przybierać formę postanowienia. W wypadkach niecierpiących zwłoki z żądaniem może wystąpić Policja lub inny uprawniony organ[67], niebędący uprawnionym do wydawania postanowień. Wówczas usługodawca może żądać niezwłocznego sporządzenia i doręczenia mu postanowienia o zatwierdzeniu uzyskania danych. Usługodawcę należy pouczyć o przysługującym mu prawie. Niemniej, w razie wystąpienia przez usługodawcę z żądaniem wydania postanowienia, jego doręczenie powinno nastąpić w ciągu 14 dni (art. 217 § 4 k.p.k.). Postanowienie to jest zaskarżalne. Zażalenie przysługuje stronom na zasadach ogólnych oraz osobom, których prawa zostały na-

[65] A. Lach, Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego, PiP 2003, nr 25, s. 16-25.

[66] J. Skorupka, *op. cit*., (w:) J. Skorupka (red.), Kodeks postępowania karnego. Komentarz, SIP Legalis.

[67] W myśl regulacji § 66 pkt 3 wytycznych nr 1 KGP (Dz. Urz. KGP z dnia 24 lipca 2015 r.): „W razie konieczności dokonania na podstawie art. 217 § 1 k.p.k. w zw. z art. 236a k.p.k. zatrzymania rzeczy, danych informatycznych lub nośników zawierających dane informatyczne (…) kierownik jednostki Policji może wystawić nakaz wydania rzeczy lub nośników zawierających dane informatyczne (…), w którym wskazuje: 1) cel czynności, ze wskazaniem rzeczy lub nośników zawierających dane informatyczne, które mają być odnalezione lub zatrzymane (…) 3) nazwę i adres instytucji, w której ma być przeprowadzona czynność".

ruszone. Oznacza to w istocie, że możliwość zaskarżenia postanowienia o zatrzymaniu danych internetowych powinien mieć zarówno usługobiorca (nawet jeśli nie ma statusu strony w postępowaniu), jak i usługodawca. Zażalenie jest rozpoznawane przez sąd rejonowy, w którego okręgu prowadzone jest postępowanie. Jeżeli uzyskanie danych internetowych zostało dokonane bez polecenia sądu lub prokuratora oraz nie zatwierdzono tej czynności w ciągu 7 dni, organ, który dane uzyskał jest obowiązany do ich zwrócenia bądź zniszczenia, chyba, że usługodawca nie złożył wniosku o sporządzenie postanowienia.

Postanowienie powinno zawierać dokładne określenie danych internetowych, których wydania żąda organ, podmiotu dysponującego artefaktami, określić należy przedział czasowy ich wytworzenia. Decyzja musi spełniać ponadto ogólne wymogi, które określa kodeks postępowania karnego, tj. wskazanie organu, który wydał postanowienie, datę jego wydania, sygnaturę sprawy i krótki opis, czego dotyczy śledztwo/dochodzenie. Postanowienie wymaga uzasadnienia, a więc wskazania okoliczności uzasadniające przypuszczenie, że dane te mogą służyć jako dowód w sprawie i mają znaczenie dla toczącego się postępowania. Postanowienie w przedmiocie żądania udostępnienia danych internetowych doręcza się użytkownikowi, którego dane dotyczą. Co istotne, doręczenie można wstrzymać na czas oznaczony, jednakże nie później niż do prawomocnego zakończenia postępowania[68].

Udostępnienie przez usługodawcę danych wskazanych w postanowieniu może w praktyce napotkać na trudności. UŚUDE nie nakłada bowiem na usługodawcę obowiązku retencji danych w taki sposób, jak przedsiębiorca telekomunikacyjny musi gromadzić metadane w zakresie połączeń telefonicznych. Taki stan rzeczy w sposób oczywisty może utrudniać pracę organów ścigania, bowiem od wewnętrznych ustaleń (regulaminów) poszczególnych usługodawców oraz przepisów RODO będzie uzależniona retencja danych internetowych. Zatem usługodawca może udostępnić na żądanie organu tylko takie dane, które posiada w chwili zgłoszenia żądania przez sąd lub prokuratora[69].

Z uwagi na specyfikę danych internetowych, ich zatrzymanie może polegać także na skopiowaniu śladów cyfrowych[70]. Decyzja o formie przekazania danych internetowych leży w kompetencji organu występującego z żądaniem. Sąd, prokurator lub inny uprawniony organ może żą-

[68] J. Skorupka, *op. cit*., (w:) J. Skorupka (red.), Kodeks postępowania karnego. Komentarz, SIP Legalis 2019.
[69] K. Chałubińska-Jentkiewicz, J. Taczkowska-Olszewska, *op. cit*.
[70] A. Lach, Gromadzenie…

dać udostępnienia danych w formie elektronicznej na nośniku bądź w formie wydruku. Forma przekazania danych będzie istotna z punktu widzenia możliwości ich późniejszego wykorzystania przy czym uzyskanie śladów w formie cyfrowej jest najbardziej pożądane, bowiem umożliwia dalsze, efektywne ich wykorzystanie (np. wprowadzenie do bazy danych i przetwarzanie w ramach analizy kryminalnej). Po otrzymaniu postanowienia usługodawca jest obowiązany udostępnić dane na nośniku lub zapewnić warunki dostępu i utrwalania tych danych[71]. W ostatnim z wymienionych przypadków uprawniony podmiot będzie mógł samodzielnie skopiować dane, których wydania żąda.

Kluczowym zagadnieniem dotyczącym procedury uzyskiwania danych internetowych jest ich zabezpieczenie. Zgodnie z art. 218a § 1 k.p.k. urzędy, instytucje i podmioty prowadzące działalność telekomunikacyjną lub świadczące usługi drogą elektroniczną oraz dostawcy usług cyfrowych obowiązani są niezwłocznie zabezpieczyć, na żądanie sądu lub prokuratora zawarte w postanowieniu, na czas określony, nieprzekraczający jednak 90 dni, dane informatyczne przechowywane w urządzeniach zawierających te dane na nośniku lub w systemie informatycznym. W sprawach o przestępstwa określone w art. 200b k.k. (propagowanie pedofilii), art. 202 § 3, 4, 4a, 4b k.k. (publiczne prezentowanie treści pornograficznych) lub art. 255a k.k. (rozpowszechnianie lub publiczne prezentowanie treści mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym) oraz w rozdziale 7 ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii[72] przewidziano dla organu prowadzącego postępowanie możliwość połączenia zabezpieczenia danych informatycznych z obowiązkiem usunięcia tych danych[73]. W art. 218b k.p.k. znajduje się ustawowa delegacja dla właściwych ministrów do określenia sposobu technicznego przygotowania systemów i sieci oraz zabezpieczania danych informatycznych. Kwestia ta została uregulowana w rozporządzeniu Ministra Sprawiedliwości z dnia 18 czerwca 2021 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji, do gromadzenia danych informatycznych oraz danych niestanowiących treści rozmowy telefonicznej lub innego przekazu informacji, a także sposobów ich zabezpieczania w urządzeniach zawierających te dane oraz w systemach i na informatycznych nośnikach danych[74].

[71] *Ibidem*.
[72] Tekst jedn. Dz. U. z 2020 r., poz. 2050 ze zm.
[73] K. Eichstaedt, (w:) D. Świecki (red.), Kodeks postępowania karnego. Tom I. Komentarz aktualizowany, LEX/el. 2022, art. 218(a).
[74] Dz. U., poz. 1101.

Zgodnie z tym rozporządzeniem usługodawca jest obowiązany do zapewnienia stałej gotowości, polegającej na możliwości sporządzania wykazów danych niezwłocznie w ciągu doby (§ 2). Zabezpieczenia danych dokonuje się przy użyciu środków technicznych, w sposób umożliwiający ich późniejsze odtworzenie przy użyciu urządzeń odtwarzających. (§ 4 ust. 1). Zabezpieczenie to musi być dokonane przez osobę uprawnioną przez usługodawcę, przy użyciu środków technicznych podmiotu obowiązanego, w urządzeniach zawierających te dane, w systemie lub na nośniku informatycznym (§ 4 ust. 2). Z czynności zabezpieczenia danych sporządza się notatkę (§ 5 ust. 1). Określone dane przechowuje się w warunkach zabezpieczających przed ich utratą, zniekształceniem lub nieuprawnionym ujawnieniem oraz zniszczeniem lub uszkodzeniem nośnika informatycznego (§ 7). W przypadku stwierdzenia nieprzydatności danych, należy je niezwłocznie zwolnić spod zabezpieczenia lub dokonać ich zniszczenia w sposób uniemożliwiający ich odtworzenie. Należy przy tym pamiętać, że instytucja zwrotu rzeczy (uzyskanych danych internetowych) nie będzie miała zastosowania w omawianym przypadku. Zwrot taki nie jest konieczny, ponieważ usługodawca wciąż posiada dane, które udostępnił, zbędnym więc wydaje się zwrócenie mu kopii. Tym bardziej bezzasadnym byłoby zwrócenie danych usługobiorcy niebędącemu właścicielem kopii[75].

5. Podsumowanie

Celem niniejszego artykułu było przedstawienie problematyki uzyskiwania danych internetowych w trybie pozaprocesowym oraz procesowym. Analiza regulacji prowadzi do kilku wniosków. Przede wszystkim, dane internetowe stanowią źródło cennych informacji o człowieku, zatem kwestia ich uzyskiwania, zarówno w toku procesu, jak i w ramach czynności operacyjno-rozpoznawczych powinna być uregulowana w sposób konkretny i precyzyjny. Czynności pozyskiwania opisanych informacji wkraczają bowiem w podstawowe prawa i wolności osoby ludzkiej, takie jak przede wszystkim prawo do prywatności, ochrony tajemnicy korespondencji, czy wreszcie prawo do autonomii informacyjnej. Taki stan rzeczy wymaga, aby ingerencja w prawa i wolności jednostki stanowiła *ultima ratio*, a regulacje czyniły zadość zasadom proporcjonalności, subsydiarności oraz celowości i adekwatności.

[75] M. R o g a l s k i, Kontrola…, s. 298.

Nie można wszak zrezygnować z możliwości uzyskiwania danych internetowych przez określone podmioty. Należy skupić się w pierwszej kolejności na precyzyjnym określeniu przesłanek legitymujących służby do uzyskiwania danych internetowych oraz zrewidować system kontroli nad uzyskiwaniem danych internetowych w toku czynności operacyjno-rozpoznawczych. Warto mieć również na uwadze, że uzyskiwanie danych internetowych w toku procesu jest możliwe przez odpowiednie stosowanie przepisu art. 217 k.p.k. w zw. z art. 236a k.p.k.

Bibliografia

1. Banaszak B., Konstytucja RP. Komentarz, wyd. 2., Warszawa 2012.
2. Chałubińska-Jentkiewicz K., Taczkowska-Olszewska J., Świadczenie usług drogą elektroniczną. Komentarz, Warszawa 2019.
3. Eichstaedt K., (w:) D. Świecki (red.), Kodeks postępowania karnego. Tom I. Komentarz aktualizowany, LEX/el. 2022, art. 218(a).
4. Fleszer D., Zakres przetwarzania danych osobowych w działalności gospodarczej, Warszawa 2008.
5. Gądzik Z., Tajemnica telekomunikacyjna, (w:) Ł. Czebotar i in. (red.), Komentarz. Ustawa o Policji, Warszawa 2015.
6. Gołaczyński J., Ustawa o świadczeniu usług drogą elektroniczną. Komentarz, wyd. 1, Warszawa 2009.
7. Grzelak A., Prawo do ochrony danych osobowych a konieczność walki z przestępczością. Uwagi na tle art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, (w:) S. Dudzik, N. Półtorak (red.), Prawo Unii Europejskiej a prawo konstytucyjne państw członkowskich, Warszawa 2013.
8. Grzeszczyk W., Kodeks postępowania karnego. Komentarz, Warszawa 2014.
9. Jagiełło D., Problematyka dowodów elektronicznych, (w:) T. Gardocka, D. Jagiełło (red.), Zagadnienia dowodowe w procesie karnym, Warszawa 2017.
10. Kakarenko K., Sobczak J., Odpowiedzialność za przestępstwa popełnione w sieci a kwestia prywatności, (w:) Sobczak J. i in. (red.), Prawo prywatności jako reguła społeczeństwa informacyjnego, Warszawa 2017.
11. Klafkowska-Waśniowska K., Komentarz do art. 18 ustawy o świadczeniu usług drogą elektroniczną, (w:) Lubasz D., Namysłowska M. (red.), Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw, Warszawa 2011.

12. Kotowski W., Ustawa o Policji. Komentarz praktyczny, wyd. 1, Warszawa 2004.
13. Lach A., Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego, Prok. i Pr. 2003, nr 25.
14. Lach A., Obowiązek retencji danych telekomunikacyjnych i udostępniania tych danych organom ścigania, MoP 2017, nr 11.
15. Lach A., Uzyskiwanie dowodów w ramach kontroli korespondencji w procesie karnym, (w:) Opaliński B., Rogalski M. (red.), Kontrola korespondencji. Zagadnienia wybrane, Warszawa 2018.
16. Nowicki M. (red.), Wokół Konwencji europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka, wyd. 7., Warszawa 2017.
17. Opaliński B., Tajemnica komunikowania się w Konstytucji RP, (w:) P. Brzeziński (red.), Gromadzenie i udostępnianie danych telekomunikacyjnych, Warszawa 2016.
18. Opaliński B. i in. (red.), Ustawa o Policji. Komentarz, wyd. 1, Warszawa 2015.
19. Roagna I., Ochrona prawa do poszanowania życia prywatnego i rodzinnego w Europejskiej Konwencji o Ochronie Praw Człowieka, Strasburg 2012.
20. Rogalski M., Kontrola korespondencji, Warszawa 2016.
21. Rogalski M., Obowiązujące w Polsce przepisy w zakresie gromadzenia i udostępniania danych telekomunikacyjnych, (w:) P. Brzeziński, B. Opaliński, M. Rogalski (red.), Gromadzenie i udostępnianie danych telekomunikacyjnych, Warszawa 2016.
22. Sarnecki P., Komentarz do art. 49, (w:) L. Garlicki, M. Zubik (red.), Konstytucja Rzeczypospolitej Polskiej, Komentarz. Tom II, Warszawa 2016.
23. Skorupka J. (red.), Kodeks postępowania karnego. Komentarz, SIP Legalis.
24. Skrzydło W. (red.), Konstytucja Rzeczypospolitej Polskiej. Komentarz, SIP LEX.
25. Wójcik J., Przeciwdziałanie przestępczości zorganizowanej. Zagadnienia prawne, kryminologiczne i kryminalistyczne, Warszawa 2011.
26. Zdybel R., Funkcja wykrywcza i dowodowa postępowania karnego, Warszawa 2016.

Internet data acquisition in judicial or extrajudicial proceedings

Abstract

This paper deals with the Internet data acquisition that is done as part of, or outside the course of regular judicial proceedings. Major issues in providing access to such data are presented, prerequisites for obtaining data are discussed, and bodies entitled to acquire Internet data are specified. Constitutional and European standards for obtaining data are also presented, with reference to key rulings.

Key words

Internet data, cyberspace, cyber security, Internet.