Ius Novum
4/2016

ZAŁOŻENIA MODELU ZBIERANIA I UDOSTĘPNIANIA DANYCH TELEKOMUNIKACYJNYCH

MACIEJ ROGALSKI

WPROWADZENIE

1. Zakres ingerencji państwa w prawa i wolności obywateli jest jednym z fundamentalnych zagadnień w państwach demokratycznych. Obszarem ingerencji państwa w sferę praw i wolności obywateli, a w szczególności prawo do prywatności, jest dostęp poprzez uprawnione do tego podmioty do danych telekomunikacyjnych obywateli. Uzasadnieniem dla pozyskiwania przekazów i danych telekomunikacyjnych jest konieczność zapewnienia skutecznego zwalczania przestępczości. Zatrzymywanie (retencja) danych telekomunikacyjnych jest ważnym narzędziem wykorzystywanym przez organy ścigania i wymiaru sprawiedliwości w sprawach karnych.

Artykuł przedstawia wyniki prac zespołu w ramach realizacji projektu badawczego nr 2015/17/B/HS5/00472 pt. *Gromadzenie i udostępnianie danych telekomunikacyjnych* finansowanego przez Narodowe Centrum Nauki. Celem prowadzonych badań w ramach tego projektu badawczego było dokonanie analizy istniejących obecnie obowiązków wynikających z postanowień ustawy Prawo telekomunikacyjne oraz uprawnień podmiotów działających na podstawie odrębnych ustaw, a także sądu i prokuratury, żądających udostępnienia danych telekomunikacyjnych, dla ustalenia:

– czy obowiązujące w Polsce przepisy dotyczące pozyskiwania i udostępniania danych telekomunikacyjnych chronią dostatecznie prawa i wolności obywatelskie przed nadmierną ingerencją państwa;
– czy obecne uregulowania prawne, w zakresie udostępniania danych telekomunikacyjnych są właściwe, zgodne z prawem Unii Europejskiej, czy też pozwalają na pozyskiwanie tych danych nieadekwatnie do celów jakim służą, zarówno pod względem ilościowym jak i zakresu danych telekomunikacyjnych, w szczególności tzw. billingów;
– czy proces pozyskiwania i przetwarzania przez uprawnione podmioty danych z bilingów oraz innych danych jest prawidłowy, czy też powinien on ulec zmianie;

– czy obecnie funkcjonujące mechanizmy prawne i rozwiązania organizacyjne zapewniają wystarczającą kontrolę nad udostępnianiem danych telekomunikacyjnych, czy też powinna być ona lepiej rozwinięta i bardziej ścisła, aby ograniczyć liczbę i zakres udostępnianych danych;
– czy obecnie, po stwierdzeniu nieważności dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 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 zmieniającą dyrektywę 2002/58/WE[1] istnieją podstawy prawne do zbierania i udostępniania danych telekomunikacyjnych[2];
– czy powinien być stworzony nowy model zbierania i udostępniania danych telekomunikacyjnych;
– jakie powinny być założenia i jak powinien wyglądać nowy model zbierania i udostępniania danych telekomunikacyjnych.

2. W oparciu o przeprowadzone analizy zostały wypracowane założenia do modelu gromadzenia i udostępniania danych telekomunikacyjnych. Obowiązujące rozwiązania w zakresie gromadzenia i udostępnia danych telekomunikacyjnych opierają się dyrektywie 2006/24/WE Parlamentu Europejskiego i Rady z dnia 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. Ocena postanowień dyrektywy 2006/24/WE z prawami podstawowymi stała się przedmiotem postępowania przed Trybunałem Sprawiedliwości UE, na skutek pytań prejudycjalnych skierowanych do Trybunału przez sądy krajowe z Irlandii i Austrii, w trybie art. 267 TFUE. W wyroku z dnia 8 kwietnia 2014 r. w sprawach połączonych C-293/12 i C-594/12 *Digital Rights Ireland* Trybunał Sprawiedliwości stwierdził jednak nieważność dyrektywy 2006/24/

---

[1] Dz. Urz. UE L Nr 105, s. 54.

[2] W kwestii skutków wyroku Trybunału Sprawiedliwości UE stwierdzającego nieważność dyrektywy 2006/24/WE na prawo krajowe zob. P. Dąbrowska, *Skutki orzeczenia wstępnego Europejskiego Trybunału Sprawiedliwości*, Warszawa 2004, s. 89; A. Wilk, *Skutki orzeczenia wstępnego*, Przegląd Prawa Europejskiego 2006, nr 1–2, s. 56; D. Anderson, *References to the European Court*, London 1995, s. 304; P. Craig, *The Jurisdiction of the Community Courts* [w:] G. de Búrca, J.H.H. Weiler (red.), *The European Court of Justice*, Oxford New York 2001, s. 177–214; A. Roberts, *Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications*, Modern Law Review 2015, nr 78(3), s. 537; J. Milaj, *Invalidation of the data retention directive – Extending the proportionality test*, Computer Law & Security Review 2015, nr 31, s. 611; M. Górski, *Skutki wyroku Digital Rights Ireland w płaszczyźnie krajowej*, Radca Prawny 2014, nr 154, s. 40; S. Tracey, *The fall of the Data Retention Directive*, Communications Law 2015, nr 20(2), s. 55; A. Wróbel, *O niektórych problemach sądowego stosowania Karty Praw Podstawowych*, [w:] A. Wróbel (red.), *Karta Praw Podstawowych w europejskim i krajowym porządku prawnym*, Warszawa 2009, s. 84; X. Tracol, *Legislative Genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national law which enacted it*, Computer Law & Security Review 2014, nr 30, s. 744; K. Kowalik-Bańczyk, *Konsekwencje przyjęcia protokołu polsko-brytyjskiego dotyczącego stosowania Karty Praw Podstawowych*, [w:] A. Wróbel (red.), *Karta Praw Podstawowych w europejskim i krajowym porządku prawnym*, Warszawa 2009, s. 149; A. Wróbel, *Czy Karta Praw Podstawowych może być bezpośrednio stosowana przez sądy polskie*, Europejski Przegląd Sądowy 2008, nr 7, s. 1; T. Ojanen, *Privacy is more than just a seven-letter word: the Court of Justice of the European Union sets constitutional limits on mass surveillance*, European Constitutional Law Review 2014, nr 10(3), s. 528.

WE[3]. W pracy został także wykorzystany wyrok polskiego Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. akt K 23/11[4], który odnosi się wprost do problematyki objętej projektem badawczym.

Prowadzone w ramach projektu badawczego badania są badaniami podstawowymi. Przygotowane założenia modelu zbierania i udostępniania danych telekomunikacyjnych są wynikiem przeprowadzonych badań podstawowych.

ZAŁOŻENIA MODELU ZBIERANIA I UDOSTĘPNIANIA DANYCH TELEKOMUNIKACYJNYCH

1. Przyszły model zbierania i udostępniania danych telekomunikacyjnych powinien się opierać na głównych rozwiązaniach, które będą wyznaczać podstawowe jego założenia. Rozwinięcie tych założeń polegać powinno nie tylko na zmianach przepisów powszechnie obowiązujących, ale także na stworzeniu lub zmianie istniejących procedur, zmianach o charakterze organizacyjnym oraz istniejącej praktyki. Ważną cechą tego modelu jest dążenie do ograniczenie ilości i zakresu pozyskiwanych informacji telekomunikacyjnych, przy uwzględnieniu z jednej strony potrzeby uprawnionych podmiotów, a z drugiej – potrzeby ochrony praw obywateli.

Przede wszystkim nowy model zbierania i udostępniania danych telekomunikacyjnych musi spełniać wszystkie wymagania konstytucyjne. Niejawne pozyskiwanie przez organy władzy publicznej informacji o jednostce wymaga zachowania daleko idących gwarancji proceduralnych. Zawsze wtedy, gdy organ władzy publicznej jest uprawniony do pozyskiwania informacji o życiu prywatnym jednostek, w tym danych telekomunikacyjnych, konieczne jest bardzo precyzyjne określenie w ustawie przedmiotowego zakresu, w jakich te działania mogą być realizowane[5].

Zbieranie danych o ruchu i lokalizacji powinno być ograniczone do sytuacji, które stwarzają zagrożenie dla bezpieczeństwa publicznego. Wartość jaką jest zapewnienie bezpieczeństwa publicznego, a w którą wpisuje się walka z przestępczością (w tym terroryzmem), usprawiedliwia odstępstwo od obowiązku przestrzegania prawa do prywatności, jeżeli będzie przewidziane przepisami prawa, konieczne, proporcjonalne i poddane ciągłemu nadzorowi. W tych warunkach dopuszczalne jest nałożenie obowiązku zatrzymywania danych oraz umożliwienie dostępu do nich właściwym organom

---

[3] Digital Rights Ireland Ltd (C-293/12) przeciwko Minister for Communications, Marine and Natural Resources i inni oraz Kärntner Landesregierung (C-594/12) i inni, http://curia.europa.eu/juris/liste.jsf?num=C-293/12&language=pl. Zob. Także krytyczne oceny dyrektywy w doktrynie: D. Wright, P. de Hert, *Privacy Impact Assessment*, Springer 2012, s. 372.

[4] Dz.U. z 2014 r., poz. 1055. Zob. uzasadnienie: otk.trybunal.gov.pl/orzeczenia/teksty/otk/2014/K_23_11.doc

[5] Zob. K. Wojtyczek, *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP*, Kraków 1999, s. 110; L. Garlicki, *Uwaga nr 21, 22, 23, 24, 25, 26, 27 do art. 33 Konstytucji RP*, [w:] L. Garlicki (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. II, Warszawa 2002, s. 22–28; L. Wiśniewski, *Prawo a wolność człowieka – pojęcie i konstrukcja prawna*, [w:] L. Wiśniewski (red.), *Podstawowe prawa jednostki i ich sądowa ochrona*, Warszawa 1997, s. 54 i n.; wyrok TK z dnia 12 stycznia 2000 r., sygn. akt P 11/98, Orzecznictwo Trybunału Konstytucyjnego 2000, nr 1, poz. 3; wyrok TK z dnia 25 lutego 1999 r., sygn. akt K 23/98, Orzecznictwo Trybunału Konstytucyjnego 1999, nr 2, poz. 25.

krajowym, jako odstępstwo od systemu ochrony prawa do poszanowania prywatności w zakresie przetwarzania danych osobowych w sektorze łączności elektronicznej w UE, ustanowionego przez dyrektywę 2002/58/WE[6], która przewiduje obowiązek zagwarantowania poufności komunikacji oraz danych o ruchu, a także obowiązek usuwania lub anonimizacji tych danych w przypadku, gdy nie są już potrzebne do celów transmisji komunikatu, z wyjątkiem sytuacji, gdy są one potrzebne do celów naliczania opłat i tylko tak długo, jak taka potrzeba istnieje.

2. Konieczne jest precyzyjne określenie w ustawie katalogu organów państwa upoważnionych do gromadzenia oraz przetwarzania danych o jednostce[7]. Należy wystrzegać się przed takim zdefiniowaniem w przepisach pojęcia „właściwych organów", które może prowadzić do uznania, że w istocie przepisy wewnętrzne wprowadzają otwarty katalog podmiotów mogących mieć dostęp do danych o ruchu i lokalizacji. W przepisach należy określić nie tylko katalog organów, które będą uprawnione do domagania się od dostawców usług telekomunikacyjnych dostępu do danych w celu ich późniejszego wykorzystania w zakresie niezbędnym do wykrywania i ścigania poważnych przestępstw, lecz także wprowadzić mechanizm ograniczający dostęp do danych do ściśle określonej kategorii osób w ramach struktur tych organów.

3. W ustawie muszą być sprecyzowane przesłanki niejawnego pozyskiwania informacji o osobach[8]. Nie jest dopuszczalne gromadzenie ani przetwarzanie danych o jednostce przez organy władzy publicznej bez powodu, w nieokreślonych lub niemożliwych do osiągnięcia celach. Niejawne pozyskiwanie informacji o jednostkach w demokratycznym państwie prawa, jest dopuszczalne jedynie w celu zapobiegania poważnym przestępstwom, ich ścigania i wykrywania[9]. Pozyskanie danych telekomunikacyjnych może nastąpić tylko w takich wypadkach, w których prawdopodobieństwo popełnienia przestępstwa jest realne, a nie tylko hipotetyczne. Ciężar wykazania prawdopodobieństwa zagrożenia przestępstwem ma przy tym spoczywać na organach państwa wnoszących o umożliwienie im niejawnego gromadzenia informacji i podlegać ocenie sądu lub innego niezależnego organu.

4. W ustawie muszą być wskazane wyraźnie pod względem rodzajowym sprawy, w przypadku których możliwe jest gromadzenie danych telekomunikacyjnych. Precyzyjne określenie katalogu spraw, w których uprawnione organy mogą pozyskiwać dane telekomunikacyjne, ma kluczowe znaczenie dla oceny, czy obowiązujące przepisy nie naruszają zasady proporcjonalności, a tym samym są dopuszczalne w świetle obowiązujących przepisów chroniących prawa i wolności obywatelskie[10].

---

[6] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, Dz. Urz. WE L Nr 201, s. 37 ze zm.

[7] Wyrok TK z 30 lipca 2014 r., sygn. K 23/11, Dz.U. z 2014 r., poz. 1055, cz. III, pkt 5; http://trybunal.gov.pl; Legalis nr 994752.

[8] *Ibidem*.

[9] E. Kosta, P. Valcke, *Telecommunications – the EU data retention directive Retaining the data retention directive*, Computer Law & Security Report 2006, nr 22, s. 374.

[10] Wyrok TK z 30 lipca 2014 r., sygn. K 23/11, Dz.U. z 2014 r., poz. 1055, cz. III, pkt 5; http://trybunal.gov.pl; Legalis nr 994752.

Przyjąć należy, że gromadzenie i udostępnianie danych telekomunikacyjnych jest możliwe tylko w sprawach karnych. Nie jest to możliwe w sprawach cywilnych[11] czy nawet o wykroczenia[12]. Gromadzenie i udostępnianie danych telekomunikacyjnych oznacza wkraczanie w jedno z podstawowych praw obywatelskich i powinno być możliwe tylko w kategorii najpoważniejszych naruszeń prawa, do których należy zaliczyć przestępstwa.

5. Gromadzenie i udostępnianie danych może dotyczyć tylko przestępstw, w celu zapobiegania, wykrywania ich i ścigania. Ograniczenie tajemnicy komunikowania może bowiem dotyczyć tylko przestępstw. Nie można jednak poprzestać w ustawie określającej kompetencje uprawnionych podmiotów do pozyskiwania danych telekomunikacyjnych, na ogólnym pojęciu „przestępstw" czy też „poważnych przestępstw", bez wskazania poszczególnych typów czynów zabronionych pod groźbą kary[13]. W przeciwnym razie, takie sformułowanie umożliwi pozyskiwanie danych w przypadku wszystkich przestępstw, a nie tylko ściśle określonych, wymienionych w ustawie[14].

Gromadzenie i udostępnianie danych telekomunikacyjnych powinno być prowadzone tylko w celu zapobiegania, wykrywania i ścigania przestępstw. Nie może służyć realizacji innych zadań np. o charakterze analitycznym, przykładowo w celu uzyskiwania, analizowania, przetwarzania i przekazywania właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa.

Ustawa powinna wymagać istnienia związku pomiędzy danymi, które mają być zatrzymywane, a działalnością przestępczą stanowiącą zagrożenie dla bezpieczeństwa publicznego[15]. W szczególności, ustawa powinna ograniczać się do zatrzymywania danych związanych albo z określonym czasem, określonym obszarem geograficznym lub określonym kręgiem osób, które mogą mieć związek z poważnym przestępstwem, albo osobami, których zatrzymane dane z innych powodów mogłyby przyczynić się do zapobieżenia poważnym przestępstwom oraz ich wykrywania lub ścigania.

Ustawa powinna określać materialne i proceduralne przesłanki, w przypadku zaistnienia których właściwe organy będą mogły uzyskać dostęp do danych i następnie je wykorzystać[16]. Wskazanym jest sprecyzowanie w ramach przepisów wewnętrznych, jak należy rozumieć pojęcie dostępu do danych. Przepisy powinny stanowić wyraźnie, że możliwość dostępu do tych danych i ich późniejszego wykorzystania powinno być ściśle ograniczona celami zapobiegania i wykrywania dokładnie określonych poważnych przestępstw lub ich ścigania.

---

[11] Wyroku Sądu Apelacyjnego w Białymstoku z 6 czerwca 2011 r., I ACz 279/11, Orzecznictwo Sądów Apelacji Białostockiej 2011, nr 1, poz. 36; J. Misztal-Konecka, J. Konecki, *Billing jako dowód w postępowaniu w sprawach o wykroczenia*, Państwo i Prawo 2010, nr 7, s. 78.

[12] Por. wyroki Wojewódzkiego Sądu Apelacyjnego w Warszawie: z 30 sierpnia 2006, II SA/Wa 809/05, LEX nr 283565; z 10 października 2006, II SA/Wa 643/05, niepubl.

[13] Por. E. Stoeva, *The Data Retention Directive and the right to privacy*, ERA Forum 2014, nr 15, s. 583.

[14] E. Kosta, P. Valcke, *Telecommunications – the EU...*, s. 374.

[15] A. Roberts, *Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications*, Modern Law Review 2015, nr 78(3), s. 547.

[16] Wyrok TK z 30 lipca 2014 r., sygn. K 23/11, Dz.U. z 2014 r., poz. 1055, cz. III, pkt 5; http://trybunal.gov.pl; Legalis nr 994752.

Ustawa powinna przewidywać obiektywne kryterium, które pozwoliłoby ograniczyć liczbę osób uprawnionych do uzyskiwania dostępu i późniejszego wykorzystywania zatrzymanych danych do przypadków, gdy jest to ściśle konieczne do realizacji zamierzonego celu. Precyzyjne określenie przestępstw i wskazanie celu gromadzenia danych pozwoli wyznaczyć granice przedmiotowe zakresu stosowania tych przepisów. Stanowić będzie także jedno z obiektywnych kryteriów, które pozwoli zagwarantować, że właściwe organy krajowe będą miały dostęp do danych i będą mogły je wykorzystywać wyłącznie w celu zapobiegania, wykrywania i ścigania przestępstw.

6. Ustawa musi dokładnie określać rodzaje i zakres danych telekomunikacyjnych podlegających gromadzeniu i udostępnianiu[17]. Nie może być to zbiór duży. Musi to być zakres danych niezbędnych do wykrywania i zwalczania poważnych przestępstw.

7. Ustawa musi precyzować przedmiotowe przesłanki podjęcia decyzji w sprawie gromadzenia i udostępniania danych telekomunikacyjnych. Nie jest wystarczające odwołanie się np. do ogólnych zagrożeń dóbr prawnie chronionych, zwłaszcza przez zwroty niedookreślone. Ustawodawca zobowiązany jest zdefiniować zamknięty i możliwe wąski katalog poważnych przestępstw, uzasadniających tego rodzaju ingerencję w status jednostki. Należy wskazać konkretne, według artykułów ustawy karnej, przestępstwa. Nie można przyjąć, że sama penalizacja jakiegoś czynu w ustawach karnych, a nawet zobowiązanie do jego ścigania na mocy umów międzynarodowych, są wystarczającymi przesłankami uznania go za poważny w stopniu uzasadniającym dopuszczalność pozyskiwania danych telekomunikacyjnych.

8. Ustawa musi określać kategorie podmiotów, wobec których mogą być gromadzone i udostępniane dane telekomunikacyjne[18]. W ustawie powinny być wskazane wyjątki i ograniczenia w zakresie osób. W szczególności chodzi o osoby, w stosunku do których brak jakichkolwiek podstaw, zarówno faktycznych, jak i prawnych do wszczęcia postępowania karnego.

Obecnie obowiązujące przepisy nie wskazują kategorii osób, w stosunku do których nie można pozyskiwać danych telekomunikacyjnych ze względu na respektowanie ich tajemnicy zawodowej[19]. Ustawodawca nie wyłączył żadnej kategorii użytkowników

---

[17] *Ibidem*.

[18] 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. 848–849; wyrok TK z 30 lipca 2014 r., sygn. K 23/11, Dz.U. z 2014 r., poz. 1055, cz. III, pkt 5; http://trybunal.gov.pl; Legalis nr 994752.

[19] Por. F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Springer 2012, s. 44 i n.; M. Wąsek-Wiaderek, *Telegraaf Media Nederland Landelijke Media B.V. i inni przeciwko Niderlandom – wyrok z dnia 22 listopada 2012 r., skarga nr 39315/06 (kluczowe zagadnienia: ochrona tajemnicy dziennikarskiej (źródła informacji dziennikarskiej), stosowanie podsłuchu wobec dziennikarzy, ochrona tajemnicy państwowej, prawo do prywatności)*, Przegląd Orzecznictwa Europejskiego dotyczącego Spraw Karnych 2012, nr 4, s. 10–17; J. Długosz, *Obowiązki prawników wykonujących wolne zawody w zakresie przeciwdziałania praniu pieniędzy. Komentarz do wyroku ETS z 26 czerwca 2007 r. (sygn. C-305/05) i do wyroku TK z 2 lipca 2007 r. (sygn. K 41/05)*, Radca Prawny 2008, nr 4, s. 42–43; M.K. Kolasiński, *Dopuszczalność ograniczenia tajemnicy adwokacko-radcowskiej w imię zapewnienia skuteczności prawa konkurencji Unii Europejskiej*, Glosa 2012, nr 2, s. 111; G. Di Federico, *Case C-550/07 P, Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v. European Commission, Judgment of the European Court of Justice (Grand Chamber) of 14 September 2010*, Common Market Law Review 2011, nr 2, s. 581–602; T. Bruno, *Ciąg dalszy sporu o zakres zasady legal*

z kręgu podmiotów, których dane mogą być pozyskiwane, choć dane te mogą być objęte tajemnicą notarialną, adwokacką, radcy prawnego, lekarską lub dziennikarską. Przewidziany jest jedynie tryb dopuszczenia przez sąd do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji.

9. Pożądane jest określenie w ustawie rodzajów środków gromadzenia informacji, a także rodzajów informacji pozyskiwanych za pomocą poszczególnych środków. Niezbędne jest sprecyzowanie sposobu wkroczenia w sferę prywatności jednostki. Konieczne sprecyzowanie w przepisach prawa zamkniętego rodzajowo katalogu środków i metod działania, za pomocą których organy państwa mogą gromadzić informacje o jednostkach[20]. Zamknięty katalog takich środków i metod ogranicza arbitralność organów państwa. Umożliwia także sprawowanie efektywnej kontroli nad pozyskiwaniem informacji o osobach.

10. Ustawa musi precyzować maksymalny czas gromadzenia i udostępniania danych telekomunikacyjnych, po upływie którego dalsze ich gromadzenie jest już niedopuszczalne[21]. Chodzi tu o czas ich gromadzenia i udostępniania przez przedsiębiorców telekomunikacyjnych. Przepisy powinny w sposób jednoznaczny ustalać termin, po upływie którego uprawnione organy państwowe nie mogą domagać się dostępu do danych przechowywanych przez dostawców usług telekomunikacyjnych. Za nieprawidłowe działanie należy uznać żądania udostępnienia danych telekomunikacyjnych za okres wykraczający poza przewidziany prawem czas ich przetrzymywania. Dłuższy niż okres przewidziany w ustawie czas przechowywania danych przez przedsiębiorcę telekomunikacyjnego może być dopuszczalny tylko w przypadkach przewidzianych wyraźnie przez przepisy Prawa telekomunikacyjnego i co jest kluczowe, tylko w celu określonym w tych przepisach, np. na potrzeby postępowań reklamacyjnych.

Czas, przez który uprawnione podmioty mogą przetwarzać pozyskane dane, nie może być ani nadmiernie długi, ani zbyt krótki[22]. Ustawodawca musi mieć na uwadze, że w demokratycznym państwie prawa nie jest dopuszczalne – nawet za zgodą sądu i w sytuacji podejrzenia popełnienia poważnych przestępstw – prowadzenie czynności bezterminowo, choćby miało się to wiązać z bezpowrotną utratą dowodów. Wydaje się, że 12-miesięczny okres zatrzymania danych telekomunikacyjnych jest stosunkowo

---

professional privilege – glosa do wyroku SPI z dnia 17.09.2007 w połączonych sprawach: T-125/03 i T-253/03 Akzo Nobel Chemicals Ltd i Agros Chemicals Ltd przeciwko Komisji WE, EPS 2008, nr 6, s. 46; M. Bernatt, B. Turno, *Zasada Legal Professional privilege w projekcie zmiany ustawy o ochronie konkurencji i konsumentów*, Internetowy Kwartalnik Antymonopolowy i Regulacyjny 2013, nr 1(2), s. 17–30.

[20] Wyrok TK z 30 lipca 2014 r., sygn. K 23/11, Dz.U. z 2014 r., poz. 1055, cz. III, pkt 5; http://trybunal.gov.pl; Legalis nr 994752.

[21] *Ibidem*.

[22] S. Tracey, *The fall of the Data Retention Directive*, Communications Law 2015, nr 20(2), s. 54; 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; M. Wach, *Zatrzymywanie danych telekomunikacyjnych przez dwa lata w celach bliżej nieokreślonych a prawo do prywatności*, Radca Prawny. Dodatek naukowy 2011, nr 115–116, s. 22; D. Adamski, *Retencja danych telekomunikacyjnych – uwagi de lege ferenda wynikające z przepisów wspólnotowych*, Monitor Prawniczy 2007, nr 4 – dodatek Prawo Mediów Elektronicznych 2007, s. 6.

długi, wziąwszy pod uwagę istotną ingerencję w wolności i prawa konstytucyjne wynikające z zatrzymywania dotyczących ich danych telekomunikacyjnych. Dane statystyczne wskazują, że w połowie wypadków udostępnianie danych mieściło się w okresie pierwszych 2 miesięcy ich przechowywania[23]. Może to uprawdopodabniać tezę, że chociaż upoważnione organy mogły pozyskiwać dane telekomunikacyjne znacznie wcześniej, zwlekały z tym do ostatniego miesiąca. W kontekście tej statystyki oraz zasady proporcjonalności, wydaje się, że zatrzymywanie danych o ruchu i lokalizacji na czas nie dłuższy niż 6 miesięcy jest wystarczające. Ewentualnie można rozważyć zróżnicowania okresu przechowywania danych z uwagi na kategorie danych oraz ich potencjalne wykorzystanie przez uprawnione podmioty, sąd i prokuraturę. W takiej sytuacji koniecznym będzie uwzględnienie aspektów kosztowych związanych z zastosowanym rozwiązaniem.

11. W ustawie powinna być uregulowana procedura decydowania o udostępnianiu danych telekomunikacyjnych, włączywszy w to powierzenie kompetencji do zarządzenia tych czynności. Chodzi o zapewnienie niezależnej kontroli udostępniania danych telekomunikacyjnych w momencie, gdy zwraca się z wnioskiem o udostępnienie danych telekomunikacyjnych podmiot uprawniony na mocy przepisu ustawy do uzyskania takich danych[24]. Powinna to być zgoda sądu, wydawana np. w formie postanowienia wyrażającego zgodę lub nie na udostępnienie uprawnionym podmiotom danych telekomunikacyjnych.

Kwestią bardzo istotną jest to, czy kontrola ta jest uprzednią czy też następczą. Kontrola następcza jest dopuszczalnym rozwiązaniem z punktu widzenia zgodności z normami Konstytucji RP. W przypadku jednak kontroli następczej, należy zawsze uwzględnić m.in. specyfikę działania i ustawowy zakres zadań poszczególnych uprawnionych do pozyskania danych telekomunikacyjnych podmiotów, sytuacje niecierpiące zwłoki, w których szybkie pozyskanie danych telekomunikacyjnych może być niezbędne do zapobieżenia popełnieniu przestępstwa lub jego wykrycia. Zgodnie z konstytucyjną zasadą sprawności działania instytucji publicznych należy wykreować mechanizm, który umożliwiłby służbom odpowiedzialnym za bezpieczeństwo państwa i porządek publiczny efektywną walkę z zagrożeniami.

Lepszym jednak, z punktu widzenia ochrony praw i wolności obywatelskich, ale także uwzględniającym interesy służb, jest rozwiązanie, które co do zasady przewiduje kontrolę uprzednią sądu[25]. Kontrola uprzednia, czyli realizowana przed skierowaniem zapytania w sprawie udostępnienia danych telekomunikacyjnych, pozwoliłaby nie tylko na istotne zwiększenie nadzoru nad wykorzystaniem tego środka, ale prawdopodobnie

---

[23] Zob. komunikat Najwyższej Izby Kontroli pt. *NIK o billingach* oraz dokument pt. *Informacja o wynikach kontroli. Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne*, http://www.nik.gov.pl/aktualnosci/nik-o-billingach.html;

Dane statystyczne zebrane przez Urząd Komunikacji Elektronicznej, https://www.uke.gov.pl/informacja-o-rocznym-sprawozdaniu-dotyczacym-udostepniania-danych-telekomunikacyjnych-13495. Zob. także wyrok TK z 30 lipca 2014 r., sygn. K 23/11, Dz.U. z 2014 r., poz. 1055; http://trybunal.gov.pl; Legalis nr 994752, cz. III, pkt 6.

[24] Wyrok TK z 30 lipca 2014 r., sygn. K 23/11, Dz.U. z 2014 r., poz. 1055, cz. III, pkt 5; http://trybunal.gov.pl; Legalis nr 994752.

[25] *Ibidem*.

przyczyniłaby się również do ograniczenia skali jego wykorzystania. W przypadku kontroli uprzedniej sprawowanej przez sąd ważne jest precyzyjne określenie sytuacji, w których środek ten może być wykorzystany jako niezbędny warunek oceny zasadności wniosku. Sąd, dokonując kontroli uprzedniej, powinien przede wszystkim ocenić zasadność wniosku o udostępnienie danych telekomunikacyjnych, w szczególności pod względem zasady subsydiarności i proporcjonalności oraz sprawdzić jego poprawność pod względem formalnym.

Uprzednia kontrola, prowadzona przez sąd przyczyniłaby się zarówno do zwiększenia poprawności przygotowywanych przez organy służby wniosków, jak i ich liczby. Konieczne jest bowiem zapewnienie efektywności przyjmowanych w praktyce rozwiązań. Innymi słowy, zapewnienie aby kontrola sprawowana przez sąd była rzeczywistą, a nie tylko pozorną kontrolą. Prowadzenie kontroli powinno być obligatoryjne, a nie tylko fakultatywne.

Sąd lub niezależny organ administracyjny powinien kontrolować, aby udostępnianie i wykorzystywanie danych ograniczało się do przypadków, gdy jest to ściśle konieczne do realizacji zamierzonego celu. Sąd lub odpowiedni organ orzekałby lub decydowałby wyłącznie na uzasadniony wniosek przedstawiony w związku z postępowaniem, którego celem jest zapobieganie, wykrywanie lub ściganie przestępstw.

W przypadku kontroli następczej, która realizowana jest po skierowaniu zapytania w sprawie udostępnienia danych telekomunikacyjnych, powinna ona przede wszystkim zapewnić weryfikację poprawności wykorzystania tego środka.

Możliwe są także rozwiązania, gdy kontrola następcza funkcjonuje łącznie z kontrolą uprzednią albo samodzielnie. Różny jest w takich sytuacjach jej zakres. W pierwszym przypadku może zostać ograniczona do kontroli wykorzystania tego środka pod kątem przestrzegania obowiązujących przepisów i procedur, w szczególności prawidłowości przetwarzania pozyskanych danych, ochrony przed ich utratą lub udostępnieniem nieuprawnionym osobom, a także ich niezwłocznym zniszczeniem, gdy nie są już potrzebne dla realizacji celu, dla którego zostały pozyskane. W przypadku natomiast, gdy występuje tylko kontrola następcza, jej zakres powinien być znacznie szerszy i obejmować również kontrolę zasadności wykorzystania tego środka dowodowego.

12. Powinno być także zapewnione badanie legalności udostępnienia danych telekomunikacyjnych przez zewnętrzny i niezależny od organów władzy wykonawczej podmiot, najlepiej przez sąd[26]. Kontrola ta uruchamiana byłaby przede wszystkim na wniosek jednostki, której dane telekomunikacyjne były udostępniania.

Abonent lub użytkownik, których dane telekomunikacyjne są zatrzymywane i wykorzystywane przez właściwe organy w celu wykrywania i ścigania poważnych przestępstw, powinien być o tym poinformowany[27]. Obowiązek poinformowania jed-

---

[26] *Ibidem*.

[27] Por. A. Rzepliński, *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 26 marca 1987 r., Seria A nr 116. Sprawa Leander przeciwko Szwecji (cz. I)*, Prokuratura i Prawo 1998, nr 1, s. 121–142; A. Rzepliński, *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 26 marca 1987 r., Seria A nr 116. Sprawa Leander przeciwko Szwecji (cz. II)*, Prokuratura i Prawo 1998, nr 2, s. 141–156; F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Springer 2012, s. 40–41 i 78; A. Lach, *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, Prokuratura i Prawo 2003, nr 10, s. 16.

nostki o pozyskaniu informacji na jej temat powinien istnieć bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne oraz bez względu na to, w związku z jakim postępowaniem dane te uzyskano. Szczególnego znaczenia nabiera to w odniesieniu do osób, wobec których nie zapadł wyrok lub którym nie zostały oficjalnie postawione zarzuty, jak również osób trzecich, których pozyskanie danych dotyczyło bezpośrednio. Jakiekolwiek wyjątki od tej zasady powinny być wskazane wprost w ustawie.

Abonent lub użytkownik, których dane telekomunikacyjne są zatrzymywane i wykorzystywane przez właściwe organy, powinien być o tym poinformowany, gdy tylko dane takie przestaną mieć znaczenie dla opisanych celów[28]. Brak podstaw do uznania, że abonent lub użytkownik powinien być uprawniony do uzyskania informacji w tym przedmiocie wcześniej. Gdyby informacja na ten temat miała być przekazana abonentowi i użytkownikowi na wcześniejszym etapie, wówczas istniałoby realne ryzyko nieosiągnięcia celów, dla których te dane miałyby być zatrzymywane. Kontrola prowadzona przez sąd, uruchamiana będzie więc dopiero po zakończeniu gromadzenia danych. Kontrola taka ma znaczenie dla oceny wartości dowodu uzyskanego za pomocą zgromadzonych danych telekomunikacyjnych, a także dla ewentualnych roszczeń odszkodowawczych. Nie będzie więc możliwe, poprzez wniesienie środka zaskarżenia, spowodowanie zaprzestania gromadzenia danych.

Ze względu na bezpieczeństwo narodowe uzasadnione wydaje się także stanowisko, że właściwe organy, które mają dostęp do zatrzymanych danych, nie powinny być zobowiązane do udzielania informacji na wniosek zainteresowanego, tj. wniosek o udzielenie informacji, czy dana agencja (organ) uzyskała dostęp do danych telekomunikacyjnych wnioskodawcy.

13. Ustawa musi określać postępowanie ze zgromadzonymi danymi telekomunikacyjnymi, zwłaszcza zasady ich wykorzystania oraz niszczenia danych zbędnych i niedopuszczalnych[29]. Ustawa musi precyzyjnie wskazywać zakres wykorzystania pozyskanych danych, a zwłaszcza wykorzystanie ich w procesie karnym jako materiałów dowodowych. W przypadku, gdy dane są zbędne lub niedopuszczalne powinny podlegać niezwłocznemu, protokolarnemu i komisyjnemu zniszczeniu. Przepisy powinny zagwarantować nieodwracalne niszczenie danych po upływie ich okresu zatrzymania. Powinny nie tylko określić sam obowiązek niszczenia danych, ale również precyzować tryb i sposób jego realizacji[30].

---

[28] Por. A. Rzepliński, *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu. Sprawa Klass przeciwko Niemcom: wyrok z dnia 22 września 1993 r. (27/1992/372/446)*, Prokuratura i Prawo 1996, nr 1, s. 133–142; A. Rzepliński, *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 22 września 1993 r. (27/1992/372/446), Sprawa Klass przeciwko Niemcom*, Prokuratura i Prawo 1996, nr 2–3, s. 135–142; A. Rzepliński, *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 22 września 1993 r., sygn. 27/1992/372/446, Sprawa Klass przeciwko Niemcom*, Prokuratura i Prawo 1996, nr 4, s. 119–129; A. Rzepliński, *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z 22 września 1993 r., sygn. 27/1992/372/446, Sprawa Klass przeciwko Niemcom (cz. IV)*, Prokuratura i Prawo 1996, nr 5, s. 117–123; F. Boehm, *Information Sharing and Data Protection*..., s. 34 i n.

[29] Zob. wniosek RPO do TK z dnia 18 lutego 2016, II.519.109.2015.KŁS/VV/AG, https://www.rpo.gov.pl/sites/default/files/Wniosek_do_TK_kontrola_operacyjna.pdf.

[30] Wyrok TK z 30 lipca 2014 r., sygn. K 23/11, Dz.U. z 2014 r., poz. 1055, cz. III, pkt 5; http://trybunal.gov.pl; Legalis nr 994752.

Niszczenie zbędnych danych zapobiega nieuprawnionemu wykorzystaniu przez organy państwa zebranych legalnie informacji i ich przechowywaniu na wszelki wypadek, gdyby w przyszłości okazały się przydatne do innych celów. Ingerencją w sferę prywatności jednostek będzie nie tylko jednorazowe pozyskanie danych o jednostce, ale również każde kolejne operacje na tych danych, w tym przechowywanie czy wtórne wykorzystywanie w toku innych postępowań[31].

Z Konstytucji RP (art. 51 ust. 2) wynika zakaz gromadzenia, w demokratycznym państwie prawnym, danych innych, niż niezbędne. Dane, które stały się zbędne dla toczącego się postępowania, powinny być więc obligatoryjnie niszczone. W ten sposób zostanie wyeliminowane ryzyko nadużyć, szczególnie poważne, gdy nie funkcjonują prawidłowo mechanizmy zewnętrznej kontroli niezbędności dalszego przetwarzania danych do realizacji ustawowych zadań.

14. Przepisy powinny ustanawiać gwarancje wystarczające do zapewnienia skutecznej ochrony danych przed ryzykiem nadużyć oraz przed jakimkolwiek nieuprawnionym dostępem do nich ze strony innych podmiotów i wykorzystywaniem w sposób niedozwolony. Przepisy powinny zapewniać ochronę i bezpieczeństwo tych danych w taki sposób, aby zapewnić ich integralność i poufność[32].

Przepisy prawa telekomunikacyjnego powinny gwarantować, że przedsiębiorcy telekomunikacyjni będą zachowywać odpowiednio wysoki poziom ochrony i bezpieczeństwa danych dzięki zastosowaniu odpowiednich środków technicznych i organizacyjnych. Przepisy prawa nie powinny pozwalać im przy określaniu stosowanych przez nich poziomów bezpieczeństwa kierować się względami gospodarczymi, jeśli chodzi o koszty wprowadzenia tych środków bezpieczeństwa.

Szczególne wymagania prawne powinny być przewidziane w przypadku transferu danych poza obszar UE ze względu na brak zapewnienia nadzoru przez niezależny organ nad transferowanymi danymi[33].

15. W aktach prawnych wykonawczych należy określić precyzyjne wymagania w zakresie wniosków lub postanowień o udostępnienie danych telekomunikacyjnych. Pozwoli to na ograniczenie lub nawet wyeliminowanie uchybień formalnoprawnych związanych z żądaniami ich udostępnienia. Błędy i nieprawidłowości powodują wydłużenie procesu udostępniania danych, a w niektórych przypadkach nawet uniemożliwiają wykonanie żądania udostępnienia przekazów i danych telekomunikacyjnych.

16. Z uwagi na rozwój technologii informatycznych, postulować należy takie zmiany w przepisach działania organów wymiaru sprawiedliwości, które pozwalałyby

---

[31] M. Birnhack, N. Elkin-Koren, *Does Law Matter Online?. Empirical Evidence on Privacy Law Compliance*, Michigan Telecomunications & Technology Law Review 2011, nr 17, s. 337, 344; S. Corbett, *The retention of personal information online: A call for international regulation of privacy law*, Computer Law & Security Review 2013, nr 29, s. 247.

[32] Wyrok TK z 30 lipca 2014 r., sygn. K 23/11, Dz.U. z 2014 r., poz. 1055, cz. III, pkt 5; http://trybunal.gov.pl; Legalis nr 994752.

[33] Zob. J. Kühling, S. Heitzer, *Returning through the national back door? The future of data retention after the ECJ judgment on Directive 2006/24/ in the UK and elsewhere*, European Law Review 2015, nr 40(2), s. 263; A. Savelyev, *Russia's new personal data localization regulations: A step forward or a self – imposed sanction?*, Computer Law & Security Review 2016, nr 32, s. 138; M. Taylor, *Electronic Communication – EU. The EU Data Retention Directive*, Computer Law & Security Report 2006, nr 22, s. 311.

na doręczanie postanowień o udostępnienie danych telekomunikacyjnych nie tylko w uwierzytelnionych odpisach, ale także za pomocą poczty elektronicznej. Wymagałoby to stworzenia odpowiednich rozwiązań technologicznych, zapewniających z jednej strony ochronę tych informacji przed dostępem do nich osób niepowołanych, a z drugiej strony, wiarygodność i prawdziwość dostarczanych w ten sposób pism[34].

17. Należy z dużą ostrożnością wykorzystywać systemy teleinformatyczne do bezpośredniego, tj. z pominięciem uprawnionych pracowników przedsiębiorcy telekomunikacyjnego, przekazywania danych telekomunikacyjnych podmiotom ich żądających, po wprowadzeniu konkretnego zapytania przez pracownika podmiotu żądającego. Powinna być zapewniona możliwość kontroli co do zakresu i ilości udostępnianych danych. W praktyce może powstać stała infrastruktura, tzw. stałych łącz, dzięki którym funkcjonariusze służb, bez udziału pracowników usługodawcy lub przy niezbędnym ich udziale, będą mogli w dowolnym zakresie pozyskiwać dane. W przypadku możliwości zawierania porozumień pomiędzy uprawnionymi podmiotami a przedsiębiorcami telekomunikacyjnymi, których przedmiotem będzie bezpośrednie, za pomocą łączy informatycznych, przekazywanie danych telekomunikacyjnych, powinny być określone w ustawie przesłanki zawierania takich porozumień. Powinna być także zagwarantowana realizacja zasady swobody działalności gospodarczej po stronie przedsiębiorcy telekomunikacyjnego w zakresie zawierania takiego porozumienia.

18. Należy z bardzo dużą ostrożnością stosować zautomatyzowane systemy dostępu do danych, czyli takie, gdzie wprowadzane się tylko podstawowe informacje przez pracownika uprawnionego podmiotu, a następnie uzyskuje on bezpośredni dostęp do tych danych w formie elektronicznej. Z praktycznego punktu widzenia rozwiązania te są korzystne, gdyż pozwalają przyśpieszyć uzyskanie tych danych nawet o kilka tygodni. Stosowanie tych rozwiązań prowadzić jednak może do przekazywania przez przedsiębiorców danych telekomunikacyjnych w szerszym zakresie niż wynikałoby to z przepisów i przygotowanego w normalnym trybie wniosku lub postanowienia. Praktyka pokazała, że systemy teleinformatyczne generują często dane telekomunikacyjne w zakresie szerszym, niż to jest określone w treści postanowień, zawierających żądanie udostępnienia danych telekomunikacyjnych oraz zwolnienie z tajemnicy telekomunikacyjnej. Stanowi to naruszenie przepisów Prawa telekomunikacyjnego dotyczących ochrony tajemnicy telekomunikacyjnej.

19. Gromadzenie i udostępnianie danych telekomunikacyjnych powinno być subsydiarnym środkiem pozyskiwania informacji lub dowodów o jednostkach, gdy nie można ich uzyskać w inny, mniej dolegliwy dla nich sposób – gdy inne stosowane środki okazały się bezskuteczne[35]. W przeciwny razie, podmiot prowadzący działalność

---

[34] Zob. A. Baworowski, *Doręczenia elektroniczne w toku postępowania przygotowawczego*, Prokuratura i Prawo 2007, nr 11, s. 40; K. Woźniewski, *Prawidłowość czynności procesowych w polskim procesie karnym*, Gdańsk 2010, s. 121; J. Skorupka (red.), *Kodeks postępowania karnego. Komentarz*, Legalis 2013, t. 10 do art. 132; L.K. Paprzycki [w:] J. Grajewski (red.), L.K. Paprzycki, S. Steinborn, *Kodeks postępowania karnego. Komentarz*, Zakamycze 2006, s. 399.

[35] S. Nouwt, *Toward a Common European Approach to Data Protection: A Critical Analysis of Data Protection Perspectives of the Council of Europe and the European Union*, [w:] *Reinventing Data Protection*, S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwange, S. Nouwt (red.), Spronger 2009, s. 282; F. Boehm, *Information Sharing and Data Protection*..., s. 37 i 39; W. Kozielewicz, *Postępowanie w przedmiocie zarządzenia kontroli operacyjnej*, [w:] L. Paprzycki, Z. Rau, *Praktyczne elementy*

telekomunikacyjną będzie zobowiązany w każdym przypadku do realizacji obowiązku udostępnienia danych, gdy tylko zwrócą się o to uprawnione podmioty, a nie tylko wówczas, gdy jest to niezbędne. Konieczne jest więc wprowadzenie przepisów, które wykorzystanie danych telekomunikacyjnych będą uzależniać od niemożności zastosowania innych, mniej ingerujących w prawa obywatelskie środków.

20. Powinna być zagwarantowana transparentność stosowania czynności operacyjno-rozpoznawczych przez poszczególne organy, przejawiająca się w publicznej jawności i dostępności zagregowanych danych statystycznych, nadających się do porównania, o ilości i rodzaju stosowanych pozyskiwanych danych.

Powinien istnieć prawny obowiązek podawania do publicznej wiadomości zagregowanych danych statystycznych o liczbie gromadzonych i udostępnianych danych telekomunikacyjnych. Prawodawca powinien, w celu efektywnego i rzetelnego wykonywania obowiązku sprawozdawczego, ustalić w miarę możliwości jedną, stosowaną przez wszystkie zobowiązane podmioty metodologię sporządzania statystyk, gwarantującą rzetelność oraz jednoznaczność i porównywalność upublicznianych danych, nawet w odniesieniu do lat ubiegłych. Powinny być precyzyjnie określone wskaźniki pomiarowe. Procedury powinny być tak skonstruowane, aby zapobiegały występowaniu rażących błędów. Zakres gromadzonych danych sprawozdawczych powinien pozwalać na ocenę, dla jakich celów, jak często i z jakim skutkiem retencja danych jest stosowana. Prawidłowa ocena funkcjonowania systemu retencji danych będzie możliwa, gdy będą gromadzone co najmniej dane w zakresie: liczby przypadków, w których uprawnione organy uzyskiwały od przedsiębiorców telekomunikacyjnych dane retencyjne (z wyodrębnieniem sytuacji, gdy były to wyłącznie dane osobowe użytkownika); liczby osób, których dane telekomunikacyjne były pozyskiwane i wykorzystywane przez uprawnione organy; łącznej liczby odmów udostępnienia danych (ze wskazaniem zasadniczych przyczyn); informacji na temat rodzaju spraw, w których środek ten wykorzystywano oraz jego skuteczności.

Pozwoliłoby to na dokonywanie porównań z liczbą analogicznych danych w innych krajach UE oraz oceniać tendencje, tj. wzrost lub spadek liczby pozyskiwanych danych i dokonywać analizy wpływu uregulowań prawnych na ilość pozyskiwanych danych.

21. Nie jest wykluczone zróżnicowanie intensywności ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się z uwagi na to, czy dane o osobach pozyskują służby wywiadowcze i zajmujące się ochroną bezpieczeństwa państwa, czy też czynią to służby policyjne. Zróżnicowanie poziomu ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się może także nastąpić z uwagi na to, czy niejawne pozyskiwanie informacji dotyczy obywateli, czy osób niemających polskiego obywatelstwa[36].

---

zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna, Warszawa 2009, s. 511; wyrok TK z 30 lipca 2014 r., sygn. K 23/11, Dz.U. z 2014 r., poz. 1055, cz. III, pkt 6; http://trybunal.gov.pl; Legalis nr 994752.

[36] Wyrok TK z 30 lipca 2014 r., sygn. K 23/11, Dz.U. z 2014 r., poz. 1055, cz. III, pkt 5; http://trybunal.gov.pl; Legalis nr 994752.

22. Wreszcie należy rozważyć wprowadzenie przynajmniej częściowej odpłatności za gromadzenie i udostępnienia danych telekomunikacyjnych[37]. Istnienie nawet symbolicznej odpłatności prowadziłoby do większej staranności w zakresie ilości i zakresu żądanych danych, co z pewnością prowadziłoby do zmniejszenia ich liczby.

23. Przedstawione założenia powinny być podstawą do skonstruowania nowego modelu zbierania danych telekomunikacyjnych. Przyjęcie zaproponowanych założeń i rozwiązań powinno doprowadzić do zmniejszenia liczby zapytań o dane telekomunikacyjne[38]. Obecne bowiem rozwiązania pozwalają na żądanie danych telekomunikacyjnych, często w szerszym zakresie niż wynikałoby to z celów prowadzonego postępowania. Funkcjonujące obecnie mechanizmy kontroli pozyskiwania danych retencyjnych nie sprzyjają także ograniczaniu liczby zapytań, choćby z powodu braku obowiązywania zasady subsydiarności. Wreszcie aktywny udział samego zainteresowanego, którego dane są zbierane, jest bardzo ograniczony, gdyż staje się możliwy dopiero po zakończeniu procesu zbierania danych.

BIBLIOGRAFIA

Adamski D., *Retencja danych telekomunikacyjnych – uwagi de lege ferenda wynikające z przepisów wspólnotowych*, Monitor Prawniczy 2007, nr 4 – dodatek Prawo Mediów Elektronicznych 2007.

Anderson D., *References to the European Court*, London 1995.

Baworowski A., *Doręczenia elektroniczne w toku postępowania przygotowawczego*, Prokuratura i Prawo 2007, nr 11.

Bernatt M., Turno B., *Zasada Legal Professional privilege w projekcie zmiany ustawy o ochronie konkurencji i konsumentów*, Internetowy Kwartalnik Antymonopolowy i Regulacyjny 2013, nr 1(2).

Birnhack M., Elkin-Koren N., *Does Law Matter Online?. Empirical Evidence on Privacy Law Compliance*, Michigan Telecomunications & Technology Law Review 2011, nr 17.

Boehm F., *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Springer 2012.

Bruno T., *Ciąg dalszy sporu o zakres zasady legal professional privilege – glosa do wyroku SPI z dnia 17.09.2007 w połączonych sprawach: T-125/03 i T-253/03 Akzo Nobel Chemicals Ltd i Agros Chemicals Ltd przeciwko Komisji WE*, EPS 2008, nr 6.

Corbett S., *The retention of personal information online: A call for international regulation of privacy law*, Computer Law & Security Review 2013, nr 29.

Craig P., *The Jurisdiction of the Community Courts*, [w:] *The European Court of Justice*, G. de Búrca, J.H.H. Weiler (red.), Oxford New York 2001.

Dąbrowska P., *Skutki orzeczenia wstępnego Europejskiego Trybunału Sprawiedliwości*, Warszawa 2004.

---

[37] Por. M.-H. Maras, *The economic costs and consequences of mass communications data retention: is the data retention directive a proportionate measure?*, European Journal of Law Economics 2012, nr 33, s. 455.

[38] Zob. statystyki Urzędu Komunikacji Elektronicznej w sprawie ilości żądań o udostępnienie danych telekomunikacyjnych: https://www.uke.gov.pl/informacja-o-rocznym-sprawozdaniu-dotyczacym-udostepniania-danych-telekomunikacyjnych-13495.

Di Federico G., *Case C-550/07 P, Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v. European Commission, Judgment of the European Court of Justice (Grand Chamber) of 14 September 2010*, Common Market Law Review 2011, nr 2.

Długosz J., *Obowiązki prawników wykonujących wolne zawody w zakresie przeciwdziałania praniu pieniędzy. Komentarz do wyroku ETS z 26 czerwca 2007 r. (sygn. C-305/05) i do wyroku TK z 2 lipca 2007 r. (sygn. K 41/05)*, Radca Prawny 2008, nr 4.

Garlicki L., *Uwaga nr 21, 22, 23, 24, 25, 26, 27 do art. 33 Konstytucji RP*, [w:] Garlicki L. (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. II, Warszawa 2002.

Górski M., *Skutki wyroku Digital Rights Ireland w płaszczyźnie krajowej*, Radca Prawny 2014, nr 154.

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),

Kolasiński M.K., *Dopuszczalność ograniczenia tajemnicy adwokacko-radcowskiej w imię zapewnienia skuteczności prawa konkurencji Unii Europejskiej*, Glosa 2012, nr 2.

Kosta E., Valcke P., *Telecommunications – the EU data retention directive Retaining the data retention directive*, Computer Law & Security Report 2006, nr 22.

Kowalik-Bańczyk K., *Konsekwencje przyjęcia protokołu polsko-brytyjskiego dotyczącego stosowania Karty Praw Podstawowych*, [w:] A. Wróbel (red.), *Karta Praw Podstawowych w europejskim i krajowym porządku prawnym*, Warszawa 2009.

Kozielewicz W., *Postępowanie w przedmiocie zarządzenia kontroli operacyjnej*, [w:] L. Paprzycki, Z. Rau, *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, Warszawa 2009.

Kühling J., Heitzer S., *Returning through the national back door? The future of data retention after the ECJ judgment on Directive 2006/24/ in the UK and elsewhere*, European Law Review 2015, nr 40(2).

Lach A., *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, Prokuratura i Prawo 2003, nr 10.

Maras M.-H., *The economic costs and consequences of mass communications data retention: is the data retention directive a proportionate measure?*, European Journal of Law Economics 2012, nr 33.

Milaj J., *Invalidation of the data retention directive – Extending the proportionality test*, Computer Law & Security Review 2015, nr 31.

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

Nouwt S., *Toward a Common European Approach to Data Protection: A Critical Analysis of Data Protection Perspectives of the Council of Europe and the European Union*, [w:] S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwange, S. Nouwt (red.), *Reinventing Data Protection*, Spronger 2009.

Ojanen T., *Privacy is more than just a seven-letter word: the Court of Justice of the European Union sets constitutional limits on mass surveillance*, European Constitutional Law Review 2014, nr 10(3).

Paprzycki L.K. [w:] Grajewski J. (red.), Paprzycki L.K, Steinborn S., *Kodeks postępowania karnego. Komentarz*, Zakamycze 2006.

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

Rzepliński A., *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu. Sprawa Klass przeciwko Niemcom: wyrok z dnia 22 września 1993 r. (27/1992/372/446)*, Prokuratura i Prawo 1996, nr 1.

Rzepliński A., *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 22 września 1993 r. (27/1992/372/446)*, Sprawa Klass przeciwko Niemcom, Prokuratura i Prawo 1996, nr 2–3.

Rzepliński A., *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 22 września 1993 r., sygn. 27/1992/372/446, Sprawa Klass przeciwko Niemcom*, Prokuratura i Prawo 1996, nr 4.

Rzepliński A., *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z 22 września 1993 r., sygn. 27/1992/372/446, Sprawa Klass przeciwko Niemcom (cz. IV)*, Prokuratura i Prawo 1996, nr 5.

Rzepliński A., *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 26 marca 1987 r., Seria A nr 116. Sprawa Leander przeciwko Szwecji (cz. I)*, Prokuratura i Prawo 1998, nr 1.

Rzepliński A., *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 26 marca 1987 r., Seria A nr 116. Sprawa Leander przeciwko Szwecji (cz. II)*, Prokuratura i Prawo 1998, nr 2.

Savelyev A., *Russia's new personal data localization regulations: A step forward or a self – imposed sanction?*, Computer Law & Security Review 2016, nr 32.

Skorupka J. (red.), *Kodeks postępowania karnego. Komentarz*, Legalis 2013.

Stoeva E., *The Data Retention Directive and the right to privacy*, ERA Forum 2014, nr 15.

Taylor M., *Electronic Communication – EU. The EU Data Retention Directive*, Computer Law & Security Report 2006, nr 22.

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

Tracol X., *Legislative Genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national law which enacted it*, Computer Law & Security Review 2014, nr 30.

Wach M., *Zatrzymywanie danych telekomunikacyjnych przez dwa lata w celach bliżej nieokreślonych a prawo do prywatności*, Radca Prawny. Dodatek naukowy 2011, nr 115–116.

Wąsek-Wiaderek M., *Telegraaf Media Nederland Landelijke Media B.V. i inni przeciwko Niderlandom – wyrok z dnia 22 listopada 2012 r., skarga nr 39315/06 (kluczowe zagadnienia: ochrona tajemnicy dziennikarskiej (źródła informacji dziennikarskiej), stosowanie podsłuchu wobec dziennikarzy, ochrona tajemnicy państwowej, prawo do prywatności),* Przegląd Orzecznictwa Europejskiego dotyczącego Spraw Karnych 2012, nr 4.

Wilk A., Skutki orzeczenia wstępnego, Przegląd Prawa Europejskiego 2006, nr 1–2.

Wiśniewski L., *Prawo a wolność człowieka – pojęcie i konstrukcja prawna*, [w:] L. Wiśniewski (red.), *Podstawowe prawa jednostki i ich sądowa ochrona*, Warszawa 1997.

Wojtyczek K., *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP*, Kraków 1999.

K. Woźniewski, *Prawidłowość czynności procesowych w polskim procesie karnym*, Gdańsk 2010.

Wright D., de Hert P., *Privacy Impact Assessment*, Springer 2012.

Wróbel A., *Czy Karta Praw Podstawowych może być bezpośrednio stosowana przez sądy polskie*, Europejski Przegląd Sądowy 2008, nr 7.

Wróbel A., *O niektórych problemach sądowego stosowania Karty Praw Podstawowych*, [w:] Wróbel A. (red.), *Karta Praw Podstawowych w europejskim i krajowym porządku prawnym*, Warszawa 2009.

ZAŁOŻENIA MODELU ZBIERANIA I UDOSTĘPNIANIA DANYCH TELEKOMUNIKACYJNYCH

Streszczenie

W artykule przedstawiono wyniki prac zespołu realizującego projekt badawczy nr 2015/17/B/HS5/00472 pt. Gromadzenie i udostępnianie danych telekomunikacyjnych finansowany przez Narodowe Centrum Nauki. Celem prowadzonych badań w ramach tego projektu badawczego było dokonanie analizy istniejących rozwiązań prawnych w zakresie gromadzenia i udostępniania danych telekomunikacyjnych wynikających z przepisów kodeksu postępowania karnego, ustaw regulujących działalność tzw. uprawnionych podmiotów i przepisów prawa telekomunikacyjnego. W szczególności przeprowadzane analizy miały udzielić odpowiedzi na pytanie, czy obowiązujące uregulowania prawne w zakresie gromadzenia i udostępniania danych telekomunikacyjnych są właściwe, czy też pozwalają na pozyskiwanie tych danych nieadekwatnie do celów, jakim służą, zarówno pod względem ilościowym, jak i zakresu. Efektem tych prac było stworzenie modelu zbierania i udostępniania danych telekomunikacyjnych.

Słowa kluczowe: *dane telekomunikacyjne*, *retencja danych*, *billingi*, *dostęp do danych telekomunikacyjnych*

ASSUMPTIONS OF THE MODEL OF COMMUNICATIONS DATA RETENTION AND DISCLOSURE

Summary

The article presents the findings of the research project no. 2015/17/B/HS5/00472 entitled "Telecommunications data retention and disclosure" financed by the National Science Centre. The research aim was to analyse the existing legal solutions in the field of telecommunications data retention and disclosure under the regulations of the Criminal Procedure Code, Acts regulating the activities of the so-called authorized entities and the regulations of the communications law. The conducted analyses were to answer the question whether the legal regulations in force in the field of data retention and disclosure are appropriate or if they allow for obtaining data inadequately to the aims they serve, with respect to both the quantity and the scope. The research resulted in the development of a model of telecommunications data retention and disclosure.

Key words: *telecommunications data*, *data retention*, *billing*, *access to telecommunications data*