Kazimierz Mordaszewski

Retencja danych objętych tajemnicą telekomunikacyjną w świetle prawa europejskiego i polskiego

I

Pojęcie r e t e n c j a wymaga etymologicznej interpretacji i wyjaśnienia jego dokładnego znaczenia. Pochodzi ono od łacińskiego słowa *retentio* i oznacza „zatrzymanie", „powstrzymywanie", „bycie zatrzymanym"[1]. Słowo to weszło do powszechnego użycia, podobnie bowiem brzmi w językach roboczych UE, tj. w języku francuskim (*rétention*) i angielskim (*retention*)[2] i w obu przypadkach ma takie samo znaczenie. R e t e n c j a w geologii oznacza zdolność do magazynowania (*retention)* wody opadowej w gruncie, jeziorach i rzekach lub zbiornikach retencyjnych[3]. Określenie to w terminologii prawnej oznacza (w ujęciu potocznym) prawo do zatrzymania należących do dłużnika przedmiotów w wypadku roszczenia o zwrot nakładów. Mogą to być rzeczy stanowiące przedmiot zastawu, jeśli zostały oznaczone w sposób, który je indywidualizuje[4]. Instytucją prawną, od dawna stosowaną w obrocie prawnym, jest zastaw jako ograniczone prawo rzeczowe stanowiące formę zabezpieczenia wierzytelności na rzeczach ruchomych i niektórych prawach. Może powstać na podstawie czynności prawnej i *ex lege*, czyli jako zastaw ustawowy.

Retencja danych w telekomunikacji oznacza gromadzenie, przechowywanie i archiwizowanie lub usuwanie zapisów dotyczących komunikacji, np. o połączeniach telefonicznych czy danych o ruchu w sieciach telekomunikacyjnych dla potrzeb organów ścigania i służb specjalnych. Pojecie to może także obejmować dane przesyłane poprzez system teleinformatyczny drogą elektroniczną umożliwiającą porozumiewanie się za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej.

Retencja danych ma służyć zapobieganiu przestępczości, a szczególnie terroryzmowi, poprzez docieranie do wszelkich możliwych elektronicznych danych, które mogą okazać się naprowadzeniami na dowody popełnionego przestępstwa. Dowodami tymi mogą być dane o ruchu w sieci, generowane podczas prowadzenia zwykłej działalności przedsiebiorców telekomunikacyjnych lub przez dostawców dostępu do internetu. Przepisy dotyczące retencji danych obligują operatorów telekomunikacyjnych i dostawców usług internetowych do rutynowego zatrzymywania na czas określony danych ruchowych przechodzących w ich serwerach.

---

[1] *Słownik wyrazów obcych*, Warszawa 1980, PWN, s. 646.

[2] Por. *Webster Third New International Dictionary,* Springfield, Mass., 2000, s. 1938; *Słownik prawniczy polsko-angielski*, PAN, Ossolineum 1986, s. 202.

[3] *Słownik języka polskiego*, tom 3, Warszawa 1980, PWN, s. 51.

[4] *Kodeks cywilny z komentarzem*, J. Winiarz (red.), t. 1, Warszawa 1989, Wydawnictwo Prawnicze, s. 249.

II

W społeczeństwach demokratycznych obywatele wykorzystują różne środki oddziaływania, żeby zwrócić uwagę ustawodawcy i wpływać na kształt przepisów. Mogą to być otwarte dyskusje, wysyłanie listów, tworzenie grup obywatelskich, prezentowanie stanowisk poprzez organizacje pozarządowe itd[5].

Od pewnego czasu w środowiskach naukowych, organizacjach pozarządowych i środkach masowego przekazu toczy się dyskusja o wykorzystywaniu bilingów przez służby policyjne. Często jest to dyskusja z tezą przyjętą z góry, że służby te, strzegąc porządku publicznego i bezpieczeństwa państwa, niezasadnie ograniczają prawa i wolności obywatelskie. Można chociażby przywołać interesującą dyskusję, która toczyła się na konferencji zorganizowanej w dniu 17 grudnia 2010 r. przez Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Generalnego Inspektora Ochrony Danych Osobowych oraz Naukowe Centrum Prawno-Informatyczne. Dyskusja ta, zdaniem GIODO, „wbiła kij w mrowisko", czyli była punktem wyjścia do prac nad tzw. dużą nowelizacją ustawy o ochronie danych osobowych. Spotkanie moderowała prof. Irena Lipowicz – Rzecznik Praw Obywatelskich, wypowiadając się na temat stanu prawnego w zakresie retencji danych w świetle zasad konstytucyjnych i wywodząc w konkluzji, że stan ten jest niezgodny z Konstytucją RP. Poza tym głos zabrał m.in.: Wojciech Wiewiórowski (GIODO), który wygłosił referat pt. *Privacy by Design jako paradygmat ochrony prywatności* i podkreślił wagę ochrony danych osobowych, łącznie z tzw. prawem zapomnienia. Z punktu widzenia tematyki niniejszego artykułu istotne było wystąpienie prof. Andrzeja Adamskiego (UMK), które dotyczyło retencji danych telekomunikacyjnych w kontekście zasady proporcjonalności. Z przywołanych przez niego badań wynika, że prokuratorzy w 70% spraw występują o obszerne dane pochodzące z bilingów również w niezbyt istotnych sprawach. Dane te są powszechnie wykorzystywane w postępowaniach w sprawach narkotykowych, nawet dotyczących drobnych dilerów. Wystarczy, że osoba nie związana ze sprawą występuje w bilingu, a wzywana jest do prokuratury w celu złożenia stosownych wyjaśnień. W niewielkich środowiskach tego typu sytuacja komentowana jest w sposób nieprzychylny dla takiego przypadkowego uczestnika postępowania karnego. Dotyczy to na przykład nauczycieli. Zdaniem A. Adamskiego, prawo telekomunikacyjne i ustawa o Policji w zakresie korzystania z danych bilingowych naruszają zasady konstytucyjne.

W niektórych artykułach prasowych tytuły brzmią alarmująco, przestrzegając przed naruszaniem przez służby swobód obywatelskich. Kazimierz Olejnik – były zastępca Prokuratora Generalnego – w wywiadzie dla „Gazety Wyborczej"[6] stwierdził, że sprawdzanie bilingów dziennikarzy to działanie sprzeczne z prawem, za które Polska będzie płacić odszkodowania na skutek zaskarżania tego typu czynności do Trybunału w Strasburgu. Z artykułu red. E. Siedleckiej natomiast wynika, że w Polsce ponad milion zapytań służb o bilingi czyni nas absolutnym liderem w UE[7]. W komentarzu autorka wskazuje, *że rząd zamiast uregulować inwigilację na europejskim poziomie, rozsądnie godząc ochronę bezpieczeństwa z poszanowaniem prywatności, poddaje się temu szantażowi* (w domyśle służb, które szantażują zagrożeniem).

[5] Por. B. D. Fisher, *Law for business*, New York 1991, West Publishing Company, s. 111.
[6] A. Kublik, *Służby wciskają ciemnotę*, „Gazeta Wyborcza" z dnia 22 października 2010 r.
[7] E. Siedlecka, *Służby zaglądają nam w telefon*, „Gazeta Wyborcza" z dnia 9 listopada 2010 r.

W artykule pt. *Bilingi tylko za zgodą sądu*[8] mec. mec. Jacek Kondracki i Krzysztof Stępiński, polemizując z Prokuratorem Dariuszem Barskim, stwierdzają, że dostęp służb do bilingów dziennikarzy jest możliwy tylko za zgodą sądu. Były Prokurator Krajowy D. Barski prezentuje odmienny pogląd. Twierdzi, *iż prawa i wolności obywatelskie ulegają jednak ograniczeniom określonym w przepisach prawa w imię racji uznanych przez ustawodawcę za nadrzędną w stosunku do tych praw i wolności*[9].

Zatem w toczącej się w naszym kraju dyskusji publicznej o wykorzystywaniu bilingów przez służby, w środkach masowego przekazu przeważa stanowisko prezentowane przez organizacje pozarządowe, aczkolwiek inne poglądy dotyczące tego problemu także są dostrzegalne.

III

Wspomiana wyżej dyskusja dotyczy ostatecznie kwestii fundamentalnych, jakimi z jednaej strony są prawna ochrona prywatności oraz prawa i wolności osobiste, a z drugiej – ograniczenia tajemnicy komunikowania się. Debata toczy się na poziomie zarówno krajowym, jak i europejskim.

Akceptowany obecnie w Europie standard gwarancji praw człowieka wyznacza przyjęta w ramach Rady Europy *Konwencja o ochronie praw człowieka i podstawowych wolności*. Państwa członkowie Rady Europy uznały, że jednym z celów Rady jest ochrona oraz rozwój praw człowieka i podstawowych wolności, i odwołując się do *Powszechnej Deklaracji Praw Człowieka* uchwalonej 10 grudnia 1948 r. przez Zgromadzenie Ogólne Narodów Zjednoczonych, przyjęli w listopadzie 1950 r. Konwencję. Konwencja ta, zwana popularnie Europejską Konwencją Praw Człowieka, weszła w życie 3 września 1953 r., a Polska ratyfikowała ją 15 grudnia 1992 r.[10]. Z art. 8 ust. 1 tego dokumentu wynika, że każdy ma prawo do poszanowania swojej korespondencji, co dotyczy także technicznych form przekazywania wiadomości. Zgodnie z art. 8 ust. 2 natomiast niedopuszczalna jest ingerencja władzy publicznej w prawo do poszanowania korespondencji, z wyjątkiem przypadków koniecznych w demokratycznym społeczeństwie, związanych m.in. z zagrożeniem dla bezpieczeństwa państwa, bezpieczeństwa publicznego lub dobrobytu gospodarczego kraju i z zapobieganiem przestępstwom.

Należy podkreślić, że w celu zapewnienia przestrzegania zobowiązań z *Konwencji* i jej protokołów utworzony został Europejski Trybunał Praw Człowieka z siedzibą w Strasburgu. Każdy obywatel państwa członkowskiego, organizacja pozarządowa lub grupa jednostek, która uważa, że stała się ofiarą naruszenia przez państwo członkowskie praw zawartych w Konwencji lub w jej protokołach, może złożyć skargę do tego Trybunału.

Zgodnie z postanowieniami Konwencji[11] Trybunał może zacząć rozpatrywać sprawę dopiero po wyczerpaniu wszystkich środków odwoławczych przewidzianych prawem wewnętrznym, na podstawie powszechnie uznanych zasad prawa międzynarodowego, oraz jeśli sprawa została wniesiona w ciągu sześciu miesięcy od daty podję-

[8] J. Kondracki, K. Stępinski, *Bilingi tylko za zgodą sądu*, „Rzeczpospolita" z dnia 19 października 2010 r.
[9] D. Barski, *Tajemnica dziennikarska nie chroni bilingów*, „Rzeczpospolita" z dnia 15 października 2010 r.
[10] Dz.U. z 1993 r., Nr 61, poz. 284.
[11] Por. art. 35 *Konwencji o ochronie praw człowieka i podstawowych wolności.*

cia ostatecznej decyzji. Jest to istotny element funkcjonowania europejskiego systemu ochrony praw człowieka, którego brak powodował, że mimo ratyfikacji traktatów, takich jak Międzynarodowy Pakt Praw Obywatelskich i Politycznych, nie było radykalnego podwyższenia standardów ochrony praw człowieka w praktyce wielu krajów[12]. Większy wpływ niż zobowiązania traktatowe wywierają często czynniki pozaprawne. Gwałtowny rozwój nowych technologii w ostatnich trzydziestu latach wpływa na poziom życia codziennego, prowadzenie biznesu, a także na kwestie praw człowieka. Po raz pierwszy wszystkie rodzaje informacji – liczby, tekst, dźwięk, video – mogą być zapisywane w formie cyfrowej na komputerach, przetwarzane i przesyłane dalej[13]. Właśnie rozwój telewizji i internetu powoduje, że naruszanie praw człowieka staje się coraz bardziej widoczne. Państwa zawsze były skłonne płacić (choć nie za dużo), żeby usunąć dostrzegalne naruszanie praw człowieka w innych państwach, niezależnie od wymogów międzynarodowych[14]. Przykładem może być sytuacja w wielu krajach Afryki i Ameryki Południowej, gdzie naruszanie praw człowieka bywało drastyczne. Państwa demokratyczne i organizacje międzynarodowe podejmowały interwencje humanitarne dopiero wtedy, gdy dochodziło do zbrodni ludobójstwa. Dopiero ex post została powołana Międzynarodowa Komisja Śledcza do spraw sytuacji w Darfurze oraz Międzynarodowy Trybunał Karny dla Rwandy. W Europie mieliśmy do czynienia z taką sytuacją w latach 90. XX wieku na Bałkanach, gdy interwencja NATO w byłej Jugosławii powstrzymała dalsze zbrodnie przeciwko ludzkości w Bośni i Hercegowinie. Ostatecznie został powołany Międzynarodowy Trybunał Karny dla byłej Jugosławii[15]. Obecne ruchy wolnościowe i zmiany systemów w państwach arabskich zmierzajace ku demokratyzacji rozpoczęły się w dużym stopniu również pod wpływem informacji przekazywanych za pośrednictwem telewizji informacyjnych oraz domen społecznościowych w internecie.

Zdaniem dr. Wolfganga Zellnera, zastępcy dyrektora Instytutu Badań nad Pokojem i Polityką Bezpieczeństwa na Uniwersytecie w Hamburgu i szefa centrum badań OBWE[16], zagrożenia, które mogą się pojawić na terenie OBWE, nie będą miały charakteru międzypaństwowego, tylko transgraniczny. Ich źródłem może być niewydolność państw w zapewnieniu prawidłowego funkcjonowania demokratycznych instytucji[17].

Polska jest krajem, w którym podstawowe prawa człowieka są przestrzegane. Prawa te w Rzeczypospolitej – demokratycznym państwie prawa – są chronione dzięki zapisom w Konstytucji (m.in. w art. art. 47 i 49). Wolności i tajemnicy komunikowania się dotyczy w szczególności prawo telekomunikacyjne oraz prawo prasowe.

Zgodnie z Konstytucją RP ograniczenia w zakresie korzystania z wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne dla porządku

[12] J. Goldsmith, *The limits of international law*, New York 2005, Oxford University Press, s. 120 - 121.

[13] B. Gates, *Business and the speed of thought, using a digital nervous system*, A time Warner Company, New York 1999, s. 15.

[14] J. Goldsmith, *The limits of* ..., s. 123.

[15] Por. *The UN Genocide Convention, a Commentary*, P. Gaeta (red.), Oxford 2009, Oxford University Press.

[16] OSCE, *Ministerial Council*, Maastricht 2003, 2 December 2003, OSCE *Strategy to Address Threats to Security and Stability in the Twenty-First Century*, http://www.osce.org/documents/mcs/2003/12/4175_en.pdf.

[17] Po. W. Zellner, „Security and Human Rights" 2008, nr 4.

publicznego lub zapewnienia bezpieczeństwa demokratycznego państwa (art. 31 ust. 3 *Konstytucji RP*). Ograniczenia prywatności w zakresie komunikowania się poprzez udostępnianie danych bilingowych dla celów ścigania przestępstw organom odpowiedzialnym za egzekwowanie prawa regulowane są w tzw. ustawach pragmatycznych, tj. w ustawie o Policji, Straży Granicznej, Żandarmerii Wojskowej, wywiadzie skarbowym oraz w ustawach dotyczących poszczególnych służb specjalnych: ABW, AW, CBA oraz SKW i SWW.

IV

W prawie unijnym powyższe zagadnienie reguluje *Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15.03.2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności*. Dyrektywa ta określa cel, jakim jest ułatwienie wykrywania, zapobiegania i ścigania poważnych przestępstw podkreślając, że istotne jest, aby państwa członkowskie przyjęły środki legislacyjne zapewniające udostępnianie danych zatrzymywanych na jej mocy jedynie właściwym organom krajowym, zgodnie z ustawodawstwem krajowym, przy pełnym poszanowaniu podstawowych praw osób zainteresowanych. *Dyrektywa* nie definiuje jednak pojęcia p o w a ż n e p r z e s t ę p s t w a[18], zostawiając tę kwestię do uregulowania państwom członkowskim.

Proponowane regulacje budziły żywe dyskusje oraz sprzeciw organizacji pozarządowych. Podczas uchwalania wyżej wymienionej dyrektywy nie doszło jednak do poważnej różnicy zdań w UE. Propozycje Komisji przeszły w Parlamencie przy poparciu chrześcijańskich demokratów (EPP) oraz socjalistów (PSE). Z kolei w Radzie nową dyrektywę popierała Wielka Brytania sprawująca wówczas prezydencję. *Głosowanie w parlamencie Europejskim stanowi wyraźny sygnał, że Europa jest zjednoczona przeciw terroryzmowi i zorganizowanej przestępczości* – komentował w grudniu 2005 r. Charles Clarke, minister spraw wewnętrznych Wielkiej Brytanii.

V

W krajach członkowskich UE dyrektywa nie obowiązuje wprost; winna być implementowana do krajowego porządku prawnego. Taką implementację wyżej wymienionej dyrektywy do prawa polskiego stanowią art. art. 180a i 180c *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne*. Na podstawie art. 180a operator publicznej sieci telekomunikacyjnej oraz dostawca usług telekomunikacyjnych są obowiązani zatrzymywać, chronić i udostępniać dane wskazane w art. 180c (potocznie nazywane „bilingowymi”[19]) uprawnionym podmiotom (służbom) oraz sądowi i prokuratorowi, w trybie określonym w odrębnych przepisach. Dane muszą być chronione zgodnie z przestrze-

[18] Por. w wersji angielskiej – *for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.*

[19] Dane niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie lub do którego kierowane jest połączenie, a także do określenia: daty i godziny połączenia, czasu jego trwania oraz rodzaju połączenia i lokalizacji telekomunikacyjnego urządzenia końcowego.

ganiem zasady tajemnicy telekomunikacyjnej. Tajemnicę telekomunikacyjną, która w szczególności obejmuje dane dotyczące użytkownika oraz dane transmisyjne, definiuje art. 159 prawa telekomunikacyjnego. Przepis art. 159 ust. 2 przewiduje silniejszą ochronę danych niż przepis art. 23 ust. 1 *Ustawy o ochronie danych osobowych* i dlatego to on znajduje zastosowanie jako podstawa legalizująca przetwarzanie danych objętych tajemnicą telekomunikacyjną[20].

Podczas prac prowadzonych od 2006 r. nad nowelizacją prawa telekomunikacyjnego w Polsce dochodziło do poważnej różnicy zdań. Niektórzy posłowie proponowali nawet 15-letni okres obowiązkowego przechowywania danych bilingowych. Rządy natomiast stały na stanowisku, że nie powinien on być krótszy niż 5 lat. Uchwalony ostatecznie przez sejm w 2009 r. przepis art. 180a *Prawa telekomunikacyjnego* nałożył na operatora publicznej sieci telekomunikacyjnej oraz dostawcę publicznie dostępnych usług telekomunikacyjnych obowiązek przechowywania danych przez maksymalny okres 2 lat. Wprowadzenie maksymalnego okresu dopuszczalnego przez dyrektywę argumentowano tym, że nasz kraj może być wykorzystywany jako zaplecze dla ugrupowań terrorystycznych. *Ratio legis* przepisu stanowi ułatwienie wykrywania przestępstw skierowanych przeciwko obronności i bezpieczeństwu państwa oraz jego porządkowi publicznemu.

Porównując przepisy prawa polskiego do zapisów zawartych w dyrektywie retencyjnej, można mieć wątpliwości co do ich pełnej zgodności. Nawet tak istotne normy, jak zawarte w art. 218 § 1 kpk, nie są tożsame z analogicznymi zapismi wyżej wymienionej dyrektywy, gdyż nie wprowadza ona wymogu zaistnienia poważnych przestępstw, analogicznie do tych, które zostały wprowadzone w artykule 237 § 2 kpk. Artykuł 237 kpk bowiem, regulujący kwestię kontroli procesowej, zawiera ograniczenie do enumeratywnie wyliczonych przestępstw. Brak takiego ograniczenia w art. 218 § 1 kpk może powodować wątpliwości co do jego zgodności z dyrektywą. Nie budzi natomiast wątpliwości przepis art. 218a kpk, stanowiący o „zabezpieczeniu danych", który jest uznawany za wyraz kompromisu pomiędzy interesem wymiaru sprawiedliwości a prawami obywatelskimi.

W konfrontacji ustawy o Policji z postanowieniami dyrektywy retencyjnej wątpliwości mogą dotyczyć braku wykazu poważnych przestępstw, analogicznego do tego, który zawarty jest w art. 19 ust. 1 tej ustawy. Zgodnie bowiem z art. 20c ust. 1 dane bilingowe mogą być ujawnione Policji wyłącznie w celu zapobieżenia przestępstwom lub wykrycia ich[21]. Podobna uwaga nasuwać się może przy analizie norm ustawy o Straży Granicznej oraz o Żandarmerii Wojskowej. Wątpliwości pojawiają się także w zakresie rozwiązań przyjętych w ustawie o Centralnym Biurze Antykorupcyjnym. Artykuł 18 tej ustawy, który upoważnia CBA do pozyskiwania danych bilingowych, odsyła do art. 2, zawierającego katalog poważnych przestępstw. W zakresie postępowań kontrolnych przepisy te mogą jednak budzić wątpliwości jeśli chodzi o zasadę proporcjonalności w świetle dyrektywy retencyjnej w sytuacji, gdy postępowanie kontrolne nie przechodzi do etapu postępowania przygotowawczego.

Z kolei analizując normę art. 28 ustawy o ABW oraz AW upoważniającą ABW do uzyskiwania danych bilingowych, należy stwierdzić, iż przepis wprowadza warunek,

[20] Por. wyrok NSA z dnia 26.01.2009 r., I OSK 174/08, LEX nr 478301.

[21] Dotyczy zatem także czynów nieumyślnych lub podejrzenia kradzieży na kwotę 251 zł; przy wykroczeniu na kwotę 249 zł zaś żądanie bilingów byłoby niezasadne.

że dane te muszą być niezbędne do rozpoznawania, zapobiegania i wykrywania poważnych przestępstw. Gdy skonfrontujemy przepis art. 5 tej ustawy z postanowieniami dyrektywy retencyjnej, to wątpliwości dotyczące zasady proporcjonalności nie wydają się uzasadnione. Podnoszony z kolei zarzut, że przepis art. 28 odsyła także do art. 5 ust. 1 pkt 1 odnoszącego się do rozpoznawania zagrożeń godzących w porządek konstytucyjny jest nieuprawniony w związku z tym, że rozpoznawanie tych zagrożeń polega na ustaleniu, czy nie są wypełnione znamiona przestępstw z rozdziału XVII kk (przestępstwa przeciwko RP). Podnoszony w mediach zarzut braku uprzedniej zgody sądu na udostępnienie danych bilingowych także nie wydaje się zasadny. Dyrektywa stanowi bowiem, że proces oraz warunki uzyskiwania dostępu do zatrzymanych danych, w przypadkach, gdy został spełniony wymóg konieczności oraz proporcjonalności, określone są w prawie krajowym każdego państwa członkowskiego. Należy podkreślić, iż dyrektywa nie wprowadza warunku uzyskania uprzedniej zgody sądu. W praktyce stosowania przepisu istnieją zabezpieczenia uniemożliwiające osobie nieuprawnionej dostęp do tych danych. W sytuacji zdobycia informacji spoza zakresu określonego w katalogu zawartym w art. 5 ustawy o ABW oraz AW mogłoby dojść do wypełnienia znamion czynu zabronionego z art. 231 kk. Przestępstwo to jest ścigane z oskarżenia publicznego. W przypadku postanowienia prokuratora o odmowie wszczęcia śledztwa, osobie pokrzywdzonej przysługuje zażalenie do sądu. Otwiera się zatem droga kontroli sądowej nie uprzedniej, ale następczej, co wydaje się być regulacją prawidłową.

Dyskusyjne byłoby w świetle dyrektywy korzystanie z bilingów dla celów postępowań sprawdzających przeprowadzanych na podstawie ustawy o ochronie informacji niejawnych. Tutaj jednak służby nie działają „z urzędu", a prowadzą postępowanie na wniosek zainteresowanego. W razie skargi osoby ubiegającej się o certyfikat bezpieczeństwa skierowanej do sądu, całość zebranych akt podlega kontroli sądowej, konkretnie wojewódzkiego sądu administracyjnego. Dlatego niesłuszny jest zarzut, że służby działają tu poza kontrolą zewnętrzną.

Nie ma w zakresie wykorzystania retencji danych orzeczeń Trybunału Konstytucyjnego ani Sądu Najwyższego. SN zajmował się kwestią bilingów jedynie w sprawie I KZP 45/02 w 2003 r., dotyczącej rozliczania kosztów połączeń.

Jak już wspomniano, w porządku prawnym UE, którego Polska jako jej członek zobowiązana jest przestrzegać, wszystkie państwa członkowskie winny implementować przyjęte dyrektywy do porządku krajowego, pod rygorem ewentualnego zaskarżenia do Europejskiego Trybunału Sprawiedliwości.

W związku z implementacją dyrektyw odnośnie do sieci i usług łączności elektronicznej, m.in. *Dyrektywy 2002/21/WE*, Polska była już zaskarżona przez Komisję Europejską do Europejskiego Trybunału Sprawiedliwości o uchybienie zobowiązaniom państwa członkowskiego co do określenia pojęcia a b o n e n t .

Wyrok Trybunału (piąta izba) z dnia 22 stycznia 2009 r. w sprawie C 492/07 brzmiał:

1) *Nie dokonując prawidłowo transpozycji dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywy ramowej, a w szczególności jej art. 2 lit. k) dotyczącej pojęcia „abonent", Rzeczpospolita Polska uchybiła zobowiązaniom, które na niej ciążą na mocy tej dyrektywy.*
2) *Rzeczpospolita Polska zostaje obciążona kosztami postępowania.*

Zatem Europejski Trybunał Sprawiedliwości orzekł, że Polska nie dokonała właściwie transpozycji do polskich przepisów definicji pojęcia a b o n e n t usług te-

lekomunikacyjnych. Polskie pojęcie abonent ograniczało się do osoby, która zawarła umowę pisemną. To pozbawiało abonentów, takich jak użytkownicy telefonów na kartę, wielu praw, w tym prawa do umieszczenia swoich danych w ogólnie dostępnej książce telefonicznej, prawa do otrzymywania rachunków zbiorczych oraz niektórych praw dotyczących wyświetlania identyfikacji rozmów przychodzących lub możliwości zablokowania automatycznego przekazywania połączeń. Komisja Europejska jako „strażnik traktatów" posiada uprawnienia do zapewniania przestrzegania prawa wspólnotowego przez państwa członkowskie[22].

Za brak implementacji dyrektywy retencyjnej do Europejskiego Trybunału Sprawiedliwości została zaskarżona również Szwecja. Należy przypomnieć, że Polska dotychczas nie dokonała na przykład pełnej transpozycji dyrektywy retencyjnej w zakresie danych internetowych.

VI

Zakończył się pierwszy etap prac nad ewaluacją stosowania dyrektywy retencyjnej na poziomie europejskim. Komisja Europejska nie stwierdziła niezgodności polskich regulacji z jej postanowieniami. Ustaliła natomiast, że zatrzymywane dane dotyczące połączeń odgrywają ważną rolę w ochronie społeczeństwa przed szkodami wynikającymi z poważnych przestępstw. Takie dane stanowią materiał dowodowy nie tylko do skazywania osób winnych popełnienia poważnych przestępstw i aktów terroryzmu, lecz także do oczyszczania z zarzutów osób niewinnych[23].

Dyskusja prowadzona w kraju, ale także i w Brukseli, może zaowocować rozwiązaniami bardziej harmonizującymi ze szczegółowymi rozwiązaniami dotyczącymi zasady bezpieczeństwa oraz ochrony praw obywatelskich. Komisarz ds. wewnętrznych UE podkreśliła, iż zatrzymywane dane odnośnie do połączeń dostarczają głównych dowodów niezbędnych do wykrywania sprawców przestępstw oraz wymierzania sprawiedliwości. Transpozycja dyrektywy nie przebiega jednak równomiernie, a różnice w implementacji będą pomocne w ocenie, na ile potrzebna będzie modyfikacja dyrektywy 2006/24/WE. Ewaluacji podlegają także dane statystyczne dotyczące wykorzystywania danych bilingowych. Podawana w mediach liczba ponad miliona bilingów rocznie, które w Polsce były wykorzystywane przez prokuraturę, sądy oraz służby policyjne w związku z przepisami o retencji danych, może być niemiarodajna, ponieważ obejmuje zapytania o abonentów, którzy nie zastrzegli numeru telefonicznego (czyli w zasadzie jest to przeglądanie książki telefonicznej oraz kilkakrotne zliczanie tych samych zapytań, kierowanych do różnych operatorów).

Zdaniem Komisji dyrektywa sama w sobie nie gwarantuje, że dane będą przechowywane, pozyskiwane i wykorzystywane w pełnej zgodności z prawem do ochrony danych osobowych. Doprowadza to do unieważnienia przepisów dotyczących jej transpozycji przez sądy w niektórych państwach członkowskich. Aby udoskonalić istniejące przepisy prawne, Komisja ma dokonać przeglądu obowiązujących zasad dotyczących zatrzymywania danych po skonsultowaniu się ze służbami policyjnymi i sądowniczy-

[22] Por. także: *Prawo Wspólnot Europejskich. Orzecznictwo*, W. Czapliński i in. (wyb. i red.), Warszawa 2005, Scholar, s. 40.

[23] Por. *Report From The Commission To The Council And The European Parlament, Evaluation report on the Data Retention Directive* (Directive 2006/24/EC), www.europa.ue.

mi, z przedstawicielami branży telekomunikacyjnej, organów ds. ochrony danych oraz społeczeństwa obywatelskiego[24].

Z kolei na szczeblu krajowym trwają prace tzw. roboczego zespołu bilingowego, powołanego przez premiera w ramach Kolegium do Spraw Służb Specjalnych, którego zadaniem jest wypracowanie stanowiska w sprawie zakresu zmian legislacyjnych odnośnie do pozyskiwania przez uprawnione organy informacji objętych tajemnicą telekomunikacyjną oraz przygotowanie propozycji tych zmian.

VII

W podsumowaniu należy stwierdzić, że niektóre przepisy implementujące przedmiotową dyrektywę wymagają doprecyzowania. Niewątpliwie niezgodne z nią jest uzyskiwanie od operatorów danych bilingowych dla celów spraw rozwodowych w trybie art. 248 § 1 kpc. Jednocześnie korzystanie z regulowanych dyrektywą retencyjną danych przez służby państwowe i wymiar sprawiedliwości stanowi ważny i skuteczny instrument ułatwiający zwalczanie poważnej przestępczości, w tym terroryzmu. Instrumentu tego nie należy jednak nadużywać.

Przykład Wielkiej Brytanii pokazuje, że na kilkaset tysięcy bilingów wykorzystanych przez policję i służby specjalne, skarg do specjalnego Trybunału (*Investigatory Powers Tribunal*) jest kilkanaście rocznie, a za słuszne uznawanych jest kilka. Retencję danych uzyskiwanych w wyniku komunikacji implementowano w Wielkiej Brytanii, traktując dyrektywę retencyjną jako istotną inicjatywę instytucji unijnych.

Artykuł 8 ust. 2 Europejskiej Konwencji Praw Człowieka umożliwia ingerencję w prawa jednostki do prywatności, jeśli jest to konieczne z punktu widzenia bezpieczeństwa narodowego oraz zapobiegania i wykrywania niektórych rodzajów przestępstw.

W Polsce natomiast na ponad milion spraw, w których wykorzystywano dane bilingowe, tylko kilka przypadków zostało nagłośnionych jako dopuszczenie się nadużyć.

Na zakończenie niniejszego artykułu nasuwa się wniosek, że nie należy eliminować tak skutecznego i niezbędnego narzędzia zwalczania przestępczości, jakim jest możliwość wykorzystywania bilingów, powołując się na pojawiające się jedynie sporadycznie nadużycia.

[24] Por. Oświadczenie Cecilii Malmström, Komisarza do spraw wewnętrznych UE z dnia 18 kwietnia 2011 r. www.europa.ue.

Streszczenie

Artykuł przedstawia analizę prawną oraz stanowisko autora w toczącej się aktualnie debacie dotyczącej wykorzystywania przez uprawnione podmioty (m.in. służby specjalne) tzw. danych retencyjnych, czyli gromadzonych przez operatorów lub dostawców usług telekomunikacyjnych, związanych z sieciowym ruchem ich usługobiorców. Stanowiąc próbę całościowego ujęcia tematu, artykuł przybliża znaczenie, tak potoczne, jak i normatywne, pojęcia r e t e n c j i d a n y c h, opisuje zagadnienia retencji na tle rozwiazań normatywnych Unii Europejskiej oraz krajowych, a także dokonuje zwięzłej oceny implementacji przepisów *Dyrektywy 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych* (...) do polskiego porządku prawnego. Dla poszerzenia perspektywy ocena ta podejmowana jest przez autora przy uwzględnieniu tak wymagń zapewnienia należytej ochrony praw obywateli, jak i ciążącego na państwach obowiązku skutecznego zwalczania przestępczości. W niniejszej publikacji wskazano na głosy krytyczne wobec rozwiązań prawnych przyjętych w zakresie retencji danych oraz przywołano pozytywne oceny, w tym także wyrażane na arenie międzynarodowej.

Abstract

The paper introduces legal analysis and author's opinion relating to the currently ongoing debate concerning the use of the so called data retention by competent national authorities (i.a. law enforcement agencies), that is data gathered by operators or providers of telecommunication services, concerning network traffic of their services users. Being an attempt to address the topic integrally, the paper brings closer the meaning, both colloquial and legal, of the term 'data retention', analyzes retention based on legal regulations stipulated in the European Union and national laws, and also presents a brief evaluation of implementation of Directive 2006/24/EC on the retention of data [...] into Polish law. To extend the perspective, this evaluation is done with having in mind both the requirements of ensuring the protection of civil rights as well as duty of national authorities to effectively fight crimes. In this thesis, is author points both to criticism on regulations concerning retention of data and to positive opinions, including those presented on international level.