Ius Novum
3/2016

DALSZE LOSY RETENCJI DANYCH PO WYROKU TRYBUNAŁU SPRAWIEDLIWOŚCI UE

MARLENA WACH[1]

I. WPROWADZENIE

Od kilku lat temat zatrzymania danych wywołuje wiele dyskusji i jest oceniany w zakresie celowości i zasadności wprowadzenia do porządku prawnego takiego rozwiązania. Gromadzenie i przechowywanie danych o ruchu w sieciach telekomunikacyjnych dla potrzeb organów ściągania i służb specjalnych jest kontrowersyjne. Wiele osób wskazywało, że stanowi to głęboką ingerencję w sferę praw i wolności obywatelskich, która narusza utrwalone w Europe standardy ochrony praw człowieka. Są też poglądy inne, wskazujące, że ingerencja ta jest niezbędnym warunkiem zmierzającym do zapewnienia bezpieczeństwa publicznego, zwłaszcza w sytuacji narastających zagrożeń związanych z terroryzmem i postępującej informatyzacji. Zdaniem jeszcze kolejnych, wdrożone rozwiązanie było nieefektywne a kosztowne i ingerujące głęboko w prawa i wolności obywatelskie, a wprowadzenie takich rozwiązań nie doprowadzi do podniesienia poziomu bezpieczeństwa obywateli.

Możliwość zatrzymania i przechowywania danych miała zapewnić organom ścigania identyfikację różnego rodzaju groźnych zamierzeń, ataków i umożliwić szybszą reakcję w celu zapobieżenia im. Suma bowiem wielu informacji, także tych związanych z ruchem w sieci, pozwala na ustalenie szczegółów przestępstwa lub przygotowań do niego. Obowiązek zatrzymania danych powoduje natomiast po stronie dostawców Internetu oraz dostawców usług konieczność automatycznej rejestracji i archiwizacji tych danych przechodzących przez ich serwery, ze względu na potencjalną przydatność tych informacji dla organów zajmujących się ściganiem przestępstw. Było i jest to rozwiązanie, które niesie z sobą obawy i ze strony dostawców, gdyż związane jest z kosztami i ewentualnym naruszeniem wizerunku oraz ze strony instytucji i organizacji odpowiedzialnych za ochronę danych osobowych z uwagi na zagrożenie naruszenia

[1] Adres e-mail: marlena.wach@oirpwarszawa.pl

poufności i zasad przetwarzania danych[2]. Nic też dziwnego, że zasadność istnienia i stosowania tego instrumentu została oceniona przez Trybunał Sprawiedliwości UE w wyroku z dnia 8 kwietnia 2014 r., sygn. C-293/12 i C-594/12 (sprawy połączone). Oceniana była także przez sądy różnych państw oraz w Polsce, w dość wąskim zakresie, przez Trybunał Konstytucyjny.

Z tych powyższych powodów zagadnieniu temu warto ponownie bliżej się przyjrzeć czy ewoluowały poglądy czy też może sama regulacja uległa zmianie i z jaką sytuacją mamy do czynienia obecnie zarówno w Polsce, jak i Europie. Ponadto analizowana będzie również kwestia tego, czy dane zatrzymane i przechowywane objęte są tajemnicą telekomunikacyjną.

II. ZBIERANE INFORMACJE I ICH OCHRONA

W celu świadczenia usług telekomunikacyjnych przedsiębiorcy telekomunikacyjni gromadzą wiele informacji, które mogą być wykorzystane nie tylko dla realizacji podstawowej usługi zapewnienia komunikacji. Dane generowane w ramach lub w związku z procesem komunikowania się stanowią informacje poufne, a co za tym idzie, podlegają ochronie. Określona jest ona w wielu dokumentach z obszaru prawa unijnego i krajowego. Monitorowanie połączeń i pozyskiwanie związanych z tym danych osobowych komunikujących się podmiotów stanowi ingerencję w życie prywatne i korespondencję. Kwestia ta była rozpatrywana w sprawie Weber i Saravia przeciwko Niemcom w której zakwestionowano niemieckie przepisy regulujące strategiczny monitoring połączeń telekomunikacyjnych, polegający na utrwalaniu rozmów telefonicznych nieoznaczonego kręgu rozmówców, a następnie identyfikowaniu, za pomocą słów kluczy, informacji zawartych w tych rozmowach, które mogą potencjalnie identyfikować sprawców przestępstw lub plany ich popełnienia. W ocenie Europejskiego Trybunału Praw Człowieka (ETPC) doszło do ingerencji w tajemnicę telekomunikacyjną chronioną przez art. 8 Konwencji[3] o ochronie praw człowieka i podstawowych wolności (Konwencji)[4]. W prawie krajowym ochronie danych z obszaru komunikacji w sektorze telekomunikacyjnym służy instytucja tajemnicy telekomunikacyjnej. Dane towarzyszące telekomunikacji są chronione również przepisami o ochronie danych osobowych w takim zakresie, w jakim są uznawane za dane osobowe[5].

---

[2] Zob. stanowisko Komitetu Doradczego Unii Europejskiej ds. Ochrony Danych Osobowych i Prywatności wyrażone w dwóch dokumentach: Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes, 5085/99EN/Final WP 25, oraz Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime, adopted on 22 March 2001, 5001/01/EN/Final WP41.

[3] Zob. § 76 uzasadnienia ww. orzeczenia Weber and Saravia v. Germany, wniosek nr 54934/00.

[4] Sporządzonej w Rzymie dnia 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej Protokołem nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284, z 1995 r. Nr 36, poz. 175, 176 i 177, z 1998 r. Nr 147, poz. 962, z 2001 r. Nr 23, poz. 266, z 2003 r. Nr 42, poz. 364 oraz z 2010 r. Nr 90, poz. 587).

[5] Tak: S. Piątek, P. Piątek, *Anonimizacja danych objętych tajemnicą telekomunikacyjną*, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2014, nr 8(3), s. 46–47.

Tajemnica telekomunikacyjna jest instytucją chroniącą dane przetwarzane przez przedsiębiorców telekomunikacyjnych. Zasadne jest omówienie tej instytucji w relacji do obowiązku zatrzymania i przechowywania danych. Stosownie do art. 159 ust. 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne[6] (Pr. tel.) tajemnica telekomunikacyjna obejmuje dane dotyczące użytkownika, treść indywidualnych komunikatów, dane transmisyjne, w tym dane lokalizacyjne, dane o lokalizacji oraz dane o próbach uzyskania połączenia między zakończeniami sieci.

Artykuł 159 ust. 1 pkt 1 Pr. tel. obejmuje ochroną wynikającą z tajemnicy telekomunikacyjnej wszystkie dane o użytkowniku przetwarzane przez przedsiębiorcę telekomunikacyjnego. Skutkuje to tym, ze można te dane przetwarzać jedynie w sytuacjach uregulowanych w art. 159 ust. 2 Pr. tel. Oznacza to, że jest to możliwe, gdy przetwarzanie jest przedmiotem usługi lub jest niezbędne do jej wykonania, gdy następuje za zgodą nadawcy lub odbiorcy, których te dane dotyczą, służy zapewnieniu dowodów transakcji handlowej lub celów łączności w działalności handlowej lub gdy jest konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi. Tak skonstruowana ochrona w ramach tajemnicy telekomunikacyjnej w stosunku do danych o użytkowniku, uniemożliwia lub w sposób istotny utrudnia wykorzystanie przykładowo przesłanki przetwarzania na podstawie wypełnienia prawnie usprawiedliwionego celu administratora danych, gdy przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Przesłanka ta określona jest w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (uodo)[7].

Artykuł 180a Pr. tel. określający obowiązek przechowywania i udostępniania danych stanowi, że operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt chronić dane podlegające zatrzymaniu i przechowywaniu przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, zgodnie z przepisami dotyczącymi tajemnicy telekomunikacyjnej. Ochrona ma zapobiec zdarzeniom uniemożliwiającym zachowanie danych w stanie niezmienionym przez cały okres objęty obowiązkiem przechowywania danych. Obejmuje zarówno zdarzenia przypadkowe, jak i celowe działania bezprawne zmierzające do naruszenia obowiązku zachowania danych. Obowiązek ochrony obejmuje także zakaz przetwarzania danych zatrzymanych przez okres dłuższy niż wymagany lub przetwarzania w tym okresie w sposób sprzeczny z celami retencji, udostępnianie podmiotom nieuprawnionym lub ujawnianie. Do ochrony danych objętych retencją stosuje się przepisy o ochronie tajemnicy telekomunikacyjnej z uwagi na to, że praktycznie całość danych podlegających retencji jest objęta tajemnicą telekomunikacyjną. Szczególne środki techniczne i organizacyjne ochrony danych objętych retencją przewiduje art. 180e Pr. tel.

---

6 Dz.U. z 2014 r., poz. 243.

7 Dz.U. z 2014 r., poz. 1182.

III. DANE PODLEGAJĄCE ZATRZYMANIU I PRZECHOWYWANIU

Dyrektywa 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 zmieniającej dyrektywę 2002/58/WE[8] (Dyrektywa 2006/24/WE) nałożyła na dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności obowiązek zatrzymywania niektórych danych generowanych lub przetwarzanych przez tych dostawców. Obowiązek ten dotyczył połączeń zarówno telefonicznych, jak i internetowych oraz obejmował szeroki zakres danych niezbędnych do: a) ustalenia źródła połączenia, w tym nazwisko i adres użytkownika (abonenta), b) określenia odbiorcy połączenia, w tym numeru lub identyfikatora użytkownika (abonenta), jego nazwiska i adresu, c) określenia daty, godziny i czasu trwania połączenia, d) określenia rodzaju połączenia, e) narzędzia komunikacji, f) identyfikacji lokalizacji urządzenia komunikacji ruchomej. Obowiązek zatrzymania danych trwa od 6–24 miesięcy. Określone zostały także w Dyrektywie 2006/24/WE wymogi dotyczące zapewnienia ochrony i bezpieczeństwa danych, sposobu ich przechowywania, nadzoru państwa nad egzekwowaniem tych obowiązków i kar za ich nieprzestrzeganie.

Obowiązkowi retencji podlegają dane dotyczące połączeń zrealizowanych i nieudanych prób połączeń, o których mowa w art. 159 ust. 1 pkt 5 Pt. tel. Oznacza to, że wszelkie przekazy pomiędzy przyłączonymi bezpośrednio lub pośrednio do zakończeń sieci urządzeniami końcowymi aktualizują obowiązek zatrzymania danych. Nieudana próba połączenia została określona w art. 159 ust. 1 pkt 5 Pr. tel. jako połączenie między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostało zestawione i nie zostało odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianego połączenia. Tajemnicą telekomunikacyjną objęte są również dane o próbie uzyskania połączenia między określonymi zakończeniami sieci, w tym dane o nieudanych próbach połączeń. Zarejestrowane dane tego rodzaju są chronione tajemnicą telekomunikacyjną na takich samych zasadach, jak dane o zrealizowanych połączeniach.

Przepisy Dyrektywy 2006/24/WE zostały implementowane do prawa polskiego w art. 179 oraz 180a–180g Pr. tel. oraz w rozporządzeniu Ministra Infrastruktury z 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania[9]. Regulacje te określają obowiązki przedsiębiorców telekomunikacyjnych oraz prawa podmiotów uprawnionych, które uprawnione są do żądania przekazania informacji objętych obowiązkiem retencji. Określają one także procedury przekazywania informacji oraz wymagania techniczne.

[8] Dz.U.UE.L.06.105.54.
[9] Dz.U. Nr 226, poz. 1828.

IV. WYROK TRYBUNAŁU KONSTYTUCYJNEGO

Dnia 30 lipca 2014 r. Trybunał Konstytucyjny rozpoznał połączone wnioski Rzecznika Praw Obywatelskich oraz Prokuratora Generalnego dotyczące określenia katalogu zbieranych informacji o jednostce za pomocą środków technicznych w działaniach operacyjnych oraz zasad niszczenia pozyskanych danych. W wyroku (sprawa K 23/11), Trybunał uznał, że konstytucyjną ochroną objęte są wszelkie sposoby przekazywania wiadomości, w każdej formie komunikowania się, bez względu na fizyczny ich nośnik. Ochrona konstytucyjna obejmuje nie tylko treść wiadomości, ale także wszystkie okoliczności procesu porozumiewania się, do których zaliczają się dane osobowe uczestników tego procesu, informacje o wybieranych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze IMEI. Trybunał Konstytucyjny zwracał uwagę, że wnioskodawcy nie zakwestionowali przepisów prawa telekomunikacyjnego nakładających na przedsiębiorców telekomunikacyjnych obowiązek zatrzymywania danych telekomunikacyjnych. Poza zakresem zaskarżenia znajdował się w rezultacie problem dopuszczalności i proporcjonalności tego obowiązku, zakresu danych podlegających retencji i obowiązkowego okresu ich zatrzymywania. Zarzuty wnioskodawców związane z wykorzystywaniem danych telekomunikacyjnych koncentrowały się na problemie udostępniania służbom policyjnym i ochrony państwa – w ramach czynności operacyjno-rozpoznawczych – zatrzymanych danych telekomunikacyjnych. Pomimo tego, że zakwestionowane przepisy ustawowe regulujące przesłanki udostępniania właściwym służbom zatrzymanych danych telekomunikacyjnych, nie stanowiły bezpośredniej implementacji Dyrektywy 2006/24/WE, to jednak pozostawały z nią w funkcjonalnym związku.

Zdaniem Trybunału warunki gromadzenia i przetwarzania tych danych przez władze publiczne muszą być unormowane w ustawie w sposób jak najbardziej przejrzysty, wykluczający arbitralność i dowolność ich stosowania. Konieczne jest precyzyjne ustawowe uregulowanie przesłanek dopuszczalności kontroli operacyjnej i pozyskiwania danych telekomunikacyjnych. Istotne jest sprecyzowanie sposobu niejawnego wkroczenia w sferę prywatności jednostki, określenie w przepisach prawa zamkniętego rodzajowo katalogu środków i metod działania, za pomocą których władze publiczne mogą w sposób niejawny gromadzić informacje o jednostkach. Ustawa ma precyzować maksymalny czas prowadzenia niejawnych czynności, po upływie którego dalsze ich prowadzenie jest już niedopuszczalne. Zdaniem Trybunału w ustawie ma być uregulowana procedura zarządzenia czynności operacyjno-rozpoznawczych, włączywszy w to powierzenie kompetencji do zainicjowania tych czynności, a także badanie ich legalności przez zewnętrzny i niezależny od organów władzy wykonawczej podmiot, najlepiej przez sąd. Ustawa ma wskazywać podstawowe elementy proceduralne, zasady wykorzystywania zgromadzonych materiałów oraz przesłanki czy tryb ich niszczenia. Konieczne jest także uregulowanie procedury raportowania z przeprowadzonych w sposób niejawny czynności i środków gwarantujących przekazanie zapisów w stanie nienaruszonym, umożliwiającym ich późniejszą weryfikację. Ustawa musi precyzyjnie wskazywać zakres wykorzystania

danych pozyskanych w toku czynności operacyjno-rozpoznawczych, a zwłaszcza wykorzystanie ich w procesie karnym jako materiałów dowodowych. Ustawa ma także określać postępowanie z materiałami, które podlegają niezwłocznemu, protokolarnemu i komisyjnemu zniszczeniu, z uwagi na ich zbędność lub nieprzydatność. Zarządzenie kontroli operacyjnej lub pozyskanie danych telekomunikacyjnych może nastąpić jednak w takich wypadkach, w których prawdopodobieństwo popełnienia przestępstwa jest realne, a nie tylko hipotetyczne. Konieczne jest zagwarantowanie bezpieczeństwa zgromadzonych danych przed nieuprawnionym dostępem ze strony innych podmiotów. Niezbędne jest również unormowanie procedury informowania jednostek o niejawnym pozyskaniu informacji na ich temat, w rozsądnym czasie po zakończeniu działań operacyjnych i zapewnienie na wniosek zainteresowanego poddania sądowej ocenie legalności zastosowania tych czynności.

W rezultacie Trybunał Konstytucyjny uznał za niezgodne z Konstytucją RP część przepisów ustawy o Policji, ustawy o Straży Granicznej, ustawy o kontroli skarbowej, ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu itd. przez to, że nie przewidują one niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d Pr. tel.

V. WYROK TRYBUNAŁU SPRAWIEDLIWOŚCI UE

W wyroku z dnia 8 kwietnia 2014 r. w sprawach połączonych o sygnaturach sygn. C-293/12 i C-594/12, Trybunał Sprawiedliwości (TSUE) stwierdził nieważność Dyrektywy 2006/24/WE. Jak wynika z orzeczenia, zgodnie z zasadą proporcjonalności akty prawne Unii Europejskiej powinny zawierać postanowienia odpowiednie do realizacji uzasadnionych celów, którym mają one służyć i nie powinny one wykraczać poza to, co jest niezbędne do osiągnięcia tych celów.

Postępowanie zostało wszczęte na podstawie wniosku o wydanie orzeczenia w trybie prejudycjalnym na podstawie art. 267 Traktatu o Funkcjonowaniu Unii Europejskiej (TFUE), złożonym przez High Court z Irlandii oraz Verfassungsgerichtshof z Austrii. Zapytanie o wydanie orzeczenia w trybie prejudycjalnym powstało w związku ze skargą Digital Rights Ireland Ltd, w której została zakwestionowana zgodność z prawem przepisów krajowych dotyczących zatrzymywania danych związanych z łącznością elektroniczną. Źródłem dla postępowania przed TSUE była też druga skarga rządu krajowego Karyntii oraz kilkunastu tysięcy osób dotycząca również zgodności Dyrektywy 2006/24/WE z Kartą Praw Podstawowych UE. Sprzeczność ta była ograniczana do zakresu, w jakim Dyrektywa 2006/24/WE pozwala na masowe gromadzenie przez długi okres czas różnego rodzaju danych dotyczących nieograniczonej ilości osób.

W skargach podniesione zostało, że zakres nałożonych obowiązków i związanych z tym ograniczeń praw jest nieproporcjonalny, a także nie jest konieczny lub jest nieodpowiedni do uzasadnionych celów, tj. do zapewnienia dostępności danych w celu wykrywania, prowadzenia czynności i ścigania poważnych przestępstw lub zapewnienia prawidłowego funkcjonowania rynku wewnętrznego UE. Postawione zostały pytania w szczególności o zgodność Dyrektywy 2006/24/WE z prawem obywateli

do swobodnego przemieszczania się i przebywania na terytorium państw członkowskich (art. 21 TFUE) oraz prawem do poszanowania życia prywatnego (art. 7 Karty praw podstawowych Unii Europejskiej[10] (Karta) i art. 8 Europejskiej Konwencji Praw Człowieka (EKPC) oraz prawem do ochrony danych osobowych i wolności wypowiedzi (art. 8 i art. 11 Karty). We wniosku austriackim wskazane zostało, że Dyrektywa 2006/24/WE zezwala na masowe gromadzenie przez okres co najmniej 6 miesięcy różnego rodzaju danych dotyczących nieograniczonej liczby osób, będących prawie wyłącznie osobami, których zachowanie nie uzasadnia zatrzymywania ich danych. Osoby te są narażone na zwiększone ryzyko zainteresowania władz, które będą miały nieuzasadnioną niczym możliwość dostępu do informacji o ich życiu prywatnym[11].

Pod rozwagę Trybunału zostało przedstawione to, czy Dyrektywa 2006/24/WE pozwala na osiągnięcie założonych celów oraz, czy ingerencja w prawa podstawowe jest proporcjonalna. Podstawową kwestią, jaką badał Trybunał było ustalenie czy ustanowiony w dyrektywie obowiązek zatrzymywania danych w celu ich ewentualnego udostępniania właściwym organom krajowym, realizuje w istocie cel interesu ogólnego – a z tej perspektywy, czy ingerencja prawodawcy unijnego jest proporcjonalna. Zgodnie z ustalonym orzecznictwem Trybunału, zasada proporcjonalności wymaga, aby unijne akty prawne były odpowiednie do realizacji uzasadnionych celów, którym mają one służyć, a także by nie wykraczały poza to, co jest konieczne do osiągnięcia tych celów. W rezultacie TSUE stwierdził nieważność dyrektywy i wskazał, że przekroczone zostały granice, które wyznacza poszanowanie zasady proporcjonalności na gruncie art. 7, 8 i art. 52 ust. 1 Karty, a Dyrektywa 2006/24/WE nie zawiera jasnych i precyzyjnych reguł określających zakres ingerencji w prawa podstawowe ustanowione w art. 7 i art. 8 Karty.

VI. CO DALEJ Z RETENCJĄ DANYCH

Orzeczenie Trybunału zostało wydane w trybie prejudycjalnym na podstawie art. 267 TFUE i zasadniczo wiąże sąd w danej sprawie. Orzeczenie to jest jednak istotne nie tylko dla określonych spraw, w związku z którymi do Trybunału skierowane zostały wnioski prejudycjalne. Ma ono wpływ na dalszą praktykę krajową w zakresie stosowania Dyrektywy 2006/24/WE. Zgodnie z tym orzeczeniem Trybunału, Dyrektywa 2006/24/WE utraciła ze skutkiem *ex tunc* domniemanie zgodności z prawem pierwotnym. Dyrektywa 2006/24/WE nie powinna być zatem dalej stosowana. Trybunał w sprawie International Chemical Corporation[12] stwierdził, że wyrok prejudycjalny stwierdzający nieważność aktu prawa wtórnego UE jest „wystarczającym uzasadnieniem dla każdego innego sądu krajowego, aby uznać akt za nieważny dla celów orzeczenia, które ma wydać". Zatem polskie sądy, które nie mają kompetencji do

[10] Dz.U. UE C 303 z 14.12.2007, s. 1.

[11] Zob. T. Piątek, *Ochrona danych w telekomunikacji*, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2014, nr 8(3), s. 13–15.

[12] Por. wyrok Trybunału Sprawiedliwości w sprawie International Chemical Corporation, 66/80, pkt 13.

samodzielnego stwierdzenia nieważności dyrektywy, nie powinny jej brać pod uwagę w procesie rozstrzygania spraw. Dotyczyłoby to także organów krajowych stosujących prawo. Utrata przez Dyrektywę 2006/24/WE stosowalności nie skutkuje nieważnością przepisów implementujących tę Dyrektywę 2006/24/WE w prawie krajowym. Nie stają się one automatycznie nieważne.

Bezpośrednim zatem skutkiem wyroku TSUE jest nieważność Dyrektywy 2006/24/WE. W rezultacie nie ma już aktu prawnego na poziomie EU, który zobowiązywałby państwa członkowskie do wprowadzenia lub utrzymania regulacji dotyczących przechowywania danych, jednakże dane państwo samo może zadecydować o wprowadzeniu regulacji w tym zakresie. TSUE uznał Dyrektywę 2006/24/WE za sprzeczną w całości z prawami podstawowymi człowieka. Ponadto Trybunał nie uznał za zasadne tymczasowe dalsze stosowanie tego aktu, lecz orzekł jego nieważność ze skutkiem natychmiastowym. W związku z tym Komisja Europejska ogłosiła, że kończy postępowania przeciwko państwom członkowskim, które naruszały prawo UE przez brak implementacji Dyrektywy 2006/24/WE w wyznaczonym terminie. Dotyczy to przede wszystkim Niemiec, gdzie Federalny Sąd Konstytucyjny dnia 2 marca 2010 r. (sygn. 1 BvR 256/08) orzekł, że przepisy § 113a i § 113b niemieckiego prawa telekomunikacyjnego (dodane na mocy ustawy implementującej Dyrektywę 2006/24/WE) są niezgodne z art. 10 ust. 1 Ustawy zasadniczej, wyrażającym wolność i gwarantującym poszanowanie tajemnicy komunikowania się. Spowodowało to brak implementacji w Niemczech Dyrektywy 2006/24/WE od 2010 r. Rząd niemiecki wskazuje, że trwają jednak prace nad nowym projektem tej regulacji. Jednoznaczne sformułowania wyroku spowodowały, że większość państw członkowskich podjęła działania zmierzające do analizy regulacji w zakresie zatrzymywania danych.

W postanowieniu z dnia 23 kwietnia 2014 r. (sygn. PL. ÚS 10/2014) słowacki Trybunał Konstytucyjny przyjął do rozpoznania wniosek o stwierdzenie niekonstytucyjności przepisów ustawy o łączności implementujących dyrektywę w sprawie zatrzymywania danych. Wydał ponadto postanowienie tymczasowe, w którym zawiesił stosowanie zaskarżonych przepisów. Z uwagi na to, że Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności (Konwencja lub ECHR) chroni prawa podstawowe i akt ten jako prawo pierwotne ma ten sam walor ważności, jak Traktaty, oznacza to, że prawo wtórne, pochodne i działania organów EU powinny być zgodne z tymi prawami. Wyrok TSUE ma niewątpliwie pośredni wpływ na regulacje krajowe. Jednakże, po wyczerpaniu procedur krajowych zmierzających do uzyskania odszkodowania, osoby fizyczne mogą wystąpić z żądaniem do Europejskiego Trybunału Praw Człowieka w Strasburgu (ETPC) twierdząc, że państwo które ratyfikowało Konwencję, narusza prawa w niej określone (art. 8 ECHR). Ponadto ETPC analizuje prawa krajowe także w zakresie praw podlegających transpozycji. Dlatego też regulacje krajowe dotyczące retencji danych mogą być przedmiotem badania przez ETPC.

W kontekście wyroku TSUE stwierdzającego nieważność Dyrektywy 2006/24/WE innego znaczenia nabiera art. 5 oraz 15 ust. 1 Dyrektywy 2002/58/WE[13]. Zgodnie

[13] Dyrektywa Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. 2002/58/WE w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (Dyrektywa o ochronie prywatności i komunikacji elektronicznej) (Dz. Urz. UE L 201 z 31.7.2002).

z art. 15 ust. 1 tej dyrektywy państwa członkowskie mogą przyjąć środki prawne w celu ograniczenia zakresu praw i obowiązków we wskazanych w tym przepisie artykułach, gdy takie ograniczenia stanowią niezbędne, odpowiednie i proporcjonalne w demokratycznym społeczeństwie środki dla zabezpieczenia bezpieczeństwa narodowego (np. bezpieczeństwa państwa), obrony, bezpieczeństwa publicznego oraz zapobiegania, prowadzenia dochodzeń, wykrywania i ścigania przestępstw lub wykorzystywania bez zezwolenia systemów komunikacji elektronicznej. W tym celu państwa członkowskie mogą, między innymi, przyjąć środki prawne przewidujące możliwość przechowywania danych, przez określony, odpowiednio uzasadniony czas. Wszystkie środki prawne powinny być zgodne z ogólnymi zasadami prawa Unii Europejskiej (Traktatem o Unii Europejskiej, ECHR, w tym art. 8 ECHR). O konieczności zapewnienia zgodności z ECHR stanowi także motyw 11) tej Dyrektywy 2002/58/WE. Po stwierdzeniu nieważności Dyrektywy 2006/24/WE wraz ze zmianą Dyrektywy 2002/58/WE dodającą do niej art. 15 ust. 1a, obecnie retencja danych regulowana jest przez art. 15 ust. 1 Dyrektywy 2002/58/WE. Wprowadzony przez Dyrektywę 2006/24/WE ust. 1a do art. 15 Dyrektywy 2002/58/WE stanowił, że ust. 1 [art. 15] nie odnosi się do obowiązków związanych z zatrzymywaniem danych w celu zapobiegania, dochodzenia, wykrywania i karania poważnych przestępstw, takich jak terroryzm i przestępczość zorganizowana, które to obowiązki wynikają z dyrektywy 2006/24/WE. Obecnie, po stwierdzeniu nieważności Dyrektywy 2006/24/WE, także zmiana w zakresie dodania ust. 1a do art. 15 Dyrektywy 2002/58/WE nie ma zastosowania.

Stwierdzenie przez TSUE nieważności Dyrektywy 2006/24/WE nie ma bezpośredniego wpływu na prawo krajowe, które pozostaje nadal wiążące, aż do czasu jego zmiany lub uchylenia. Wskazuje się zatem na konieczność analizy, weryfikacji i zmiany regulacji krajowych odnoszących się do przechowywania danych. W Polsce, w związku także z omówionym już wyrokiem Trybunału Konstytucyjnego, konieczna jest rewizja Prawa telekomunikacyjnego oraz innych zakwestionowanych przez Trybunał przepisów odnoszących się do retencji danych, w celu zapewnienia zgodności prawa krajowego z wyrokiem Trybunału Konstytucyjnego, orzeczeniem TSUE i ochroną praw podstawowych zapewnioną przez ECHR. Brak takiej zmiany może doprowadzić do roszczeń odszkodowawczych zarówno obywateli, jak i organizacji chroniących ich prawa czy też podmiotów, które w związku z retencją danych ponoszą tego koszty. W przypadku długotrwałego braku reakcji ze strony danego państwa członkowskiego również Komisja Europejska (KE) jako strażnik traktatów ma obowiązek monitorowania zgodności praw krajowych z prawem EU. W sytuacji wątpliwości KE może wszcząć procedurę zmierzającą do weryfikacji naruszenia w oparciu o art. 258 Traktatu o Funkcjonowaniu Unii Europejskiej (TFEU). Zapewne w zaistniałej sytuacji KE nie będzie śpieszyła się z wszczęciem takiej procedury, jednakże należy wskazać, że istnieje taka możliwość.

W wyroku z dnia 27 lipca 2014 r.[14] austriacki Trybunał Konstytucyjny stwierdził niezgodność z austriacką konstytucją i Konwencją przepisów upoważniających do

[14] Sygn. G 47/2012, G 59/2012, G 62/2012, G 70/2012, G 71/2012.

przekazywania właściwym służbom danych telekomunikacyjnych, zatrzymywanych na podstawie unormowań implementujących dyrektywę 2006/24/WE. Wyrok ten został wydany po stwierdzeniu przez TSUE w wyroku z dnia 8 kwietnia 2014 r. – m.in. w związku z pytaniem prejudycjalnym austriackiego sądu konstytucyjnego – nieważności tej dyrektywy. Trybunał Konstytucyjny Słowenii również unieważnił krajowe przepisy dotyczące zatrzymywania danych w wyroku z dnia 3 lipca 2014 r. i zobligował również przedsiębiorców zatrzymujących dotąd dane telekomunikacyjne do zniszczenia danych, niezwłocznie po opublikowaniu orzeczenia. Sąd Konstytucyjny w Rumunii już 8 grudnia 2009 r. orzekł o niezgodności całej ustawy nr 298/2008 dotyczącej retencji danych z konstytucją. W związku z tym została wprowadzona w 2012 r. nowa ustawa. Akt ten został ponownie uznany za niekonstytucyjny w jednomyślnej decyzji rumuńskiego Trybunału Konstytucyjnego w dniu 8 lipca 2014 r. Dnia 11 marca 2015 holenderski sąd uchylił stosowanie regulacji dotyczących retencji danych osobowych na skutek postępowania wszczętego przez grupę organizacji chroniących prawa obywatelskie. Trybunał Konstytucyjny w Bułgarii dnia 12 marca 2015 r. orzekł, że przepisy dotyczące zatrzymania danych są niekonstytucyjne. Formalny wniosek w tej sprawie wpłynął od Rzecznika Praw Obywatelskich w kwietniu 2014 r.

Przykładem innego podejścia jest rząd Wielkiej Brytanii, który uchwalił w trybie ekspresowym w lipcu 2014 r. akt regulujący retencję danych (*The Data Retention and Investigatory Powers Act* – DRIPA). Zastąpił on przepisy dotyczące przechowywania danych implementowane na podstawie unieważnionej przez TSUE Dyrektywy 2006/24/WE. Zdaniem rządu takie działanie było niezbędne aby wypełnić potencjalne luki w prawie. DRIPA zobowiązuje dostawców telekomunikacyjnych do retencji informacji o komunikacji klientów i ujawniania ich na żądanie uprawnionych do tego agencji i organów wykonawczych. Sąd (*High Court*) w Wielkiej Brytanii dnia 17 lipca 2015 r. stwierdził niezgodność regulacji dotyczących zatrzymywania danych z art. 7 and 8 Europejskiej Karty Praw podstawowych oraz art. 8 ECHR i odroczył skutek tego orzeczenia do 1 kwietnia 2016 r. Zatem rząd Wielkiej Brytanii ma 9 miesięcy na zmianę tych przepisów. Analogicznie we Francji trwają prace nad uchwaleniem nowych przepisów dotyczących zatrzymania danych[15].

W Polsce trwały prace nad nowelizacją poszczególnych ustaw w zakresie, w którym Trybunał Konstytucyjny wyrokiem z dnia 30 lipca 2014 r. (sprawa K 23/11) stwierdził ich niezgodność z Konstytucją RP. Przepisy określone w wyroku Trybunału Konstytucyjnego straciły moc obowiązującą z upływem 18 miesięcy od dnia ogłoszenia wyroku w Dzienniku Ustaw Rzeczypospolitej Polskiej. Sentencja rozstrzygnięcia została ogłoszona dnia 6 sierpnia 2014 r. w Dz.U. 2014, poz. 1055. Dnia 5 sierpnia 2015 r. odbyło się pierwsze czytanie projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw[16]. Projekt został w większości opinii negatywie oceniony, jako niespełniający wytycznych określonych zarówno w wyroku Trybunału Konstytucyjnego, jak i orzeczeniu TSUE. Dnia 4 lutego 2016 r. weszła w życie ustawa o zmianie

[15] Odnośnie podejścia innych krajów zob. http://observatory.mappingtheinternet.eu/page/data-retention-legislation-europe.

[16] Druk nr 3765 Senacki projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw.

ustawy o Policji oraz niektórych innych ustaw[17]. Biuro Trybunału Konstytucyjnego wyjaśniało na swojej stronie internetowej[18], że ustawa ta jedynie częściowo realizuje wyrok z 30 lipca 2014 r., a dodatkowo wprowadza inne rozwiązania prawne, których wyrok TK w sprawie o sygn. K 23/11 nie wymagał bądź do których w ogóle się nie odnosił. Jest to niewątpliwie bardzo kontrowersyjna nowelizacja, jak i cała regulacja, dotyczący również zbierania danych objętych tajemnicą zawodową.

VII. PODSUMOWANIE

Dane zatrzymywane i przechowywane właściwe w całości objęte są tajemnicą telekomunikacyjną. Dlatego też operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt chronić dane podlegające zatrzymaniu i przechowywaniu przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, zgodnie z przepisami dotyczącymi tajemnicy telekomunikacyjnej. Obowiązek ochrony obejmuje także zakaz przetwarzania danych zatrzymanych przez okres dłuższy niż wymagany lub przetwarzania w tym okresie w sposób sprzeczny z celami retencji, udostępnianie podmiotom nieuprawnionym lub ujawnianie. Do ochrony danych objętych retencją stosuje się przepisy o ochronie tajemnicy telekomunikacyjnej z uwagi na to, że praktycznie całość danych podlegających retencji jest objęta tajemnicą telekomunikacyjną. W przypadku uznaniu przez dany sąd, że Dyrektywa 2006/24/WE nie obowiązuje, a sam obowiązek zatrzymania określonych danych ma charakter nieproporcjonalnej ingerencji w prawo do prywatności oraz ochrony danych osobowych, nie oznacza to równocześnie, że dane te przestają być chronione jako tajemnica telekomunikacyjna, gdyż art. 159 Pr. tel. wprost wskazuje, że np. dane dotyczące użytkownika, dane transmisyjne, dane o lokalizacji oraz próbach uzyskania połączenia stanowią tajemnicę telekomunikacyjną.

W zakresie samej retencji danych dnia 30 lipca 2014 roku Trybunał Konstytucyjny w wyroku określił, jakie wymogi powinny zostać określone w ustawie, aby stanowiła ona podstawę dla zatrzymania i udostępniania informacji. Trybunał, choć zakwestionował brak mechanizmów kontrolnych nad retencją danych telekomunikacyjnych, nie przesądził ani, czy w każdym przypadku pozyskiwania danych konieczna jest kontrola uprzednia czy następcza, ani jak ma wyglądać sama procedura dostępu do tych danych, pozostawiając w tym zakresie swobodę ustawodawcy, który będzie musiał zadbać o wprowadzenie odpowiednich przepisów. Warunkiem pozyskiwania informacji o osobach, jak stwierdził Trybunał, jest ustalenie procedury niezwłocznej selekcji, a także niszczenia materiałów zbędnych czy niedopuszczalnych. Zapobiegać bowiem należy przechowywaniu informacji na wypadek, gdyby miały okazać się przydatne w przyszłości i gdyby miały zostać wykorzystane w innych celach. Istotne

---

[17] Dz.U. poz. 147.

[18] Zob. http://trybunal.gov.pl/fileadmin/content/nie-tylko-dla-mediow/Komunikat_BTK_w_zwiazku_z_nowela_ustawy_o_Policji.pdf

jest także zapobieżenie przekazywaniu w sposób niekontrolowany zatrzymywanych informacji lub ich niekontrolowanemu udostępnieniu.

Trybunał Konstytucyjny postanowił o odroczeniu utraty mocy obowiązującej niekonstytucyjnych przepisów o 18 miesięcy od dnia ogłoszenia wyroku w Dzienniku Ustaw. W okresie odroczenia przepisy te mogły być stosowane przez organy władzy publicznej. Dnia 4 lutego 2016 r. weszła w życie ustawa o zmianie ustawy o Policji oraz niektórych innych ustaw, która jedynie częściowo realizuje wyrok z 30 lipca 2014 r. Wyrok ETSU jak i Trybunału Konstytucyjnego to kolejne bardzo istotne głosy w dyskusji o ochronie prawa do prywatności, proporcjonalności i zakresie ingerencji państwa w konstytucyjnie chronione prawa i wolności jednostki. Ingerencja taka musi być uzasadniona i znajdująca oparcie w przepisach prawa, które z kolei muszą gwarantować kontrolę nad taką ingerencją.

BIBLIOGRAFIA

Piątek S., Piątek P., *Anonimizacja danych objętych tajemnicą telekomunikacyjną*, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2014, nr 8(3).

Piątek T., *Ochrona danych w telekomunikacji*, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2014, nr 8(3).

DALSZE LOSY RETENCJI DANYCH PO WYROKU TRYBUNAŁU SPRAWIEDLIWOŚCI UE

Streszczenie

Celem artykułu jest zwrócenie uwagi czytelnika na kwestię regulacji w zakresie zatrzymania danych, ich ewolucji i często krytycznej jej oceny przez sądy oraz trybunały. Jest to zagadnienie z jednej strony ochrony państwa i bezpieczeństwa publicznego, a z drugiej zakresu i proporcjonalności ingerencji państwa w podstawowe prawa i wolności obywatela. Ukazane są, zwłaszcza na przykładzie orzeczenia Trybunału Konstytucyjnego, warunki tej ingerencji w prawa podstawowe jednostki. Niewątpliwie, w uzasadnionych przypadkach, konieczność takiego pozyskiwania informacji jednak zachodzi. Wskazuje się ponadto, że właściwie wszystkie informacje podlegające zatrzymaniu objęte są tajemnicą telekomunikacyjną.

Słowa kluczowe: *zatrzymanie*, *przechowywanie danych*, *tajemnica telekomunikacyjna*, *prawo telekomunikacyjne*, *dane osobowe*, *Dyrektywa 2006/24/WE*, *prawa i wolności obywateli*

FUTURE TREATMENT OF DATA AFTER THE RULING OF THE COURT OF JUSTICE OF THE EU

Summary

The aim of the article is to draw readers' attention to the issue of regulations on the retention of data, their evolution and frequently critical evaluation by courts and tribunals. It is an issue of the protection of the state and public safety on the one hand and of the scope and proportionality of the state interference into citizens' basic rights and liberties on the other hand. The article presents, especially based on the Constitutional Tribunal judgement, the conditions of that intrusion into an individual's basic rights. Undoubtedly, in justified cases, it is necessary to obtain such information. It is also pointed out that in fact all the retained information is subject to telecommunications data secrecy.

Key words: *retention*, *data storage*, *telecommunications privacy*, *telecommunications law*, *personal data*, *Directive 2006/24/EC*, *citizens' rights and liberties*