Ius Novum
1/2017

STANOWISKO WYBRANYCH SĄDÓW KONSTYTUCYJNYCH PAŃSTW CZŁONKOWSKICH UE/WE W SPRAWIE ZGODNOŚCI REGULACJI IMPLEMENTUJĄCYCH DYREKTYWĘ 2006/24/WE Z PRAWAMI PODSTAWOWYMI*

PIOTR BRZEZIŃSKI**

1. WPROWADZENIE

Przedmiotem niniejszego artykułu jest analiza orzecznictwa wybranych sądów konstytucyjnych państw członkowskich w przedmiocie zgodności przepisów implementujących dyrektywę 2006/24/WE do ich systemów prawnych z prawami podstawowymi jeszcze przed wydaniem przez Trybunał Sprawiedliwości orzeczenia w sprawie *Digital Rights Ireland*. W wyroku z dnia 8 kwietnia 2014 roku w sprawie *Digital Rights Ireland* Trybunał stwierdził nieważność 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 zmieniająca dyrektywę 2002/58/WE[1]. Zdaniem Trybunału, dyrektywa 2006/24/WE nie przewidywała wystarczających środków gwarantujących bezpieczeństwom obywatelom UE przed nadużyciami w sytuacji przejęcia danych o ruchu i lokalizacji w celu dochodzenia, wykrywania i ścigania poważnych przestępstw a przez to w sposób nieproporcjonalny ingerowała w gwarantowane w Karcie Praw Podstawowych UE prawo do prywatności i ochrony danych osobowych. Orzeczenie Trybunału Sprawiedliwości miało ogromy wpływ na orzecznictwo sądów konstytucyjnych w przedmiocie zgodności regulacji krajowych implementujących dyrektywę

* Artykuł jest współfinansowany i stanowi efekt realizacji projektu badawczego nr 2015/17/B/HS5/00472 pt. *Gromadzenie i udostępnianie danych telekomunikacyjnych* finansowanego przez Narodowe Centrum Nauki.

** dr, adiunkt na Wydziale Prawa i Administracji Uczelni Łazarskiego w Warszawie

[1] Dz.U. L 105 z 13.4.2006, s. 54–63.

2006/24/WE do wewnętrznych systemów prawnych państw członkowskich. Warto jednak zauważyć, że orzecznictwo sądów konstytucyjnych dotyczące regulacji implementujących dyrektywę 2006/24/WE do systemów prawnych państw członkowskich UE stwarzało podstawy do postawienia tezy, że stwierdzenie przez Trybunał Sprawiedliwości nieważności dyrektywy 2006/24/WE było nieuchronne. Z orzecznictwa sądów konstytucyjnych jednoznacznie wynikało, że przepisy krajowe implementujące dyrektywę 2006/24/WE naruszają prawa podstawowe, o czym szerzej poniżej.

Artykuł związany jest z realizacją projektu badawczego nr 2015/17/B/HS5/00472 pt. *Gromadzenie i udostępnianie danych telekomunikacyjnych* w ramach grantu przyznanego przez Narodowe Centrum Nauki.

2. ORZECZNICTWO SĄDÓW KONSTYTUCYJNYCH PRZED WYDANIEM PRZEZ TS WYROKU W SPRAWIE DIGITAL RIGHTS IRELAND

Jeszcze przed wydaniem wyroku *Digital Rights Ireland*, sądy konstytucyjne niektórych państw członkowskich podjęły się oceny zgodności regulacji dotyczących zatrzymywania danych o ruchu i lokalizacji z ich ustawami zasadniczymi. Sądy konstytucyjne Rumunii, Niemiec, Czech oraz Bułgarski Naczelny Sąd Administracyjny i Cypryjski Sąd Najwyższy oceniły zgodność transponowanej do prawa wewnętrznego dyrektywy 2006/24/WE z przepisami konstytucji. Co ciekawe, każdy z sądów odnalazł konflikt przepisów wdrażających dyrektywę 2006/24/WE do systemu prawa wewnętrznego z prawami podstawowymi, jednak każdy uzasadnił ten konflikt w odmienny sposób.

Jako pierwszy podjął się wyzwania Bułgarski Naczelny Sąd Administracyjny w wyroku z dnia 11 grudnia 2008 r.[2], w którym zwrócił uwagę na jedno z postanowień prawa krajowego, gwarantujące dostęp dla organów ścigania do baz danych, bez uprzedniej zgody sądu. Jednak o ile regulacja ta była kontrowersyjna, biorąc pod uwagę przepisy dotyczące ochrony praw człowieka, była jednak ona zgodna z dyrektywą 2006/24/WE, która nie zawierała w tym zakresie żadnych postanowień. Bułgarski Sąd Administracyjny skoncentrował się w swym rozstrzygnięciu na zagadnieniu braku ograniczeń użycia gromadzonych danych oraz braku odpowiednich zabezpieczeń przed niewłaściwym ich użyciem.

W dniu 8 października 2009 r. rumuński sąd konstytucyjny wydał wyrok na skutek skargi Rumuńskiej Organizacji Praw Jednostek[3]. Sąd uznał, że prawo krajowe pozostaje w konflikcie z art. 8 EKPC. Sąd ten zauważył, że uprawnienia organów ścigania są zbyt rozległe. Prawo stanowiło o dostępie do danych w celu zapobiegania zagrożeniu bezpieczeństwa państwa. Brak było jednak definicji zagrożenia bezpieczeństwa i innych,

[2] Decyzja nr 13627, Bułgarskiego Naczelnego Sądu Administracyjnego z dnia 11 grudnia 2008. Tekst orzeczenia jest dostępny na stronie internetowej: http://www.econ.bg/law86421/enactments/article153902.html. Komentarz do orzeczenia w języku angielskim: http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention

[3] Decyzja nr 1258, Rumuńskiego Sądu Konstytucyjnego z dnia 8 października 2009. Tłumaczenie orzeczenia w języku angielskim (nieoficjalne): http://www.legiinternet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf

takich jak *„powiązane dane"*[4] niezbędne do identyfikacji abonenta lub użytkownika. Zdaniem sądu, takie określenie podstawy dostępu do danych nie było wystarczające precyzyjne. Ponadto sąd uznał, że masowe zbieranie danych, także od „niewinnych" jednostek prowadzi do założenia *a priori*, że wszyscy użytkownicy elektronicznych usług telekomunikacyjnych mogą być podejrzani o przestępstwa terrorystyczne i inne poważne przestępstwa. Sąd, idąc tym tropem, stwierdził, że taka regulacja sprawia, że treść prawa do prywatności staje się jedynie teoretyczna i iluzoryczna.

Po wyroku rumuńskiego Sądu Konstytucyjnego, przyszła kolej na Niemiecki Federalny Sąd Konstytucyjny. Na skutek skargi złożonej przez 34 000 skarżących, w dniu 2 marca 2010 r. niemiecki sąd wydał wyrok, w którym stwierdził, że niemiecka ustawa implementująca dyrektywę 2006/24/WE jest niezgodna z konstytucją z uwagi na to, że nie spełnia przesłanki proporcjonalności[5]. Niemiecki Federalny Sąd Konstytucyjny nie skrytykował dyrektywy 2006/24/WE, lecz sposób, w jaki akt ten był interpretowany przez niemiecki parlament. W wyroku z dnia 2 marca 2010 roku niemiecki sąd uznał, że „ochrona komunikacji obejmuje nie tylko treść, lecz również poufność okoliczność dotyczących komunikacji, w tym w szczególności okoliczności wskazujących na to czy, kiedy i jak wiele razy dana osoba kontaktuje się inną osobą lub próbuje nawiązać z nią kontakt"[6]. Niemiecki Federalny Trybunał Konstytucyjny poddał ustawę implementującą dyrektywę 2006/24/WE weryfikacji stosując tzw. *„privacy test"* podobny do tego, który został wypracowany przez Trybunał w Strasburgu. Niemiecki Federalny Trybunał Konstytucyjny uznał, że co do zasady, że sześciomiesięczny okres przechowywania danych może być uzasadniony, ale tylko na zasadzie wyjątku[7]. Trybunał, powołując się na orzeczenie w sprawie traktatu lizbońskiego, uznał, że „zakaz zupełnej rejestracji percepcji wolności obywateli jest częścią konstytucyjnej tożsamości prawnej Republiki Federalnej Niemiec". A. Wróbel trafnie zauważa, że tożsamość narodowa, która zgodnie z art. 4 ust. 2 TUE, jest „szanowana" przez Unię, jest chętnie wykorzystywana przez

---

[4] Poniżej przytaczam przepisy rumuńskiej ustawy nr 298/2008 dotyczącej zatrzymywania danych generowanych i przetwarzanych przez dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności.

„art. 1 (1) The present law established the obligation of the electronic communication providers of services and public networks to retain certain data produced or processed during their activity of providing electronic communication services, in order to make them available to the competent authorities to use them in activities of enquiry, detection and proceedings against serious crimes.

(2) The present law is applied to traffic and localization data of the physical and legal persons, as well as to the related data necessary to identify the subscriber or the registered user.

(3) The present law does not apply to the content of the communication or information accessed while using an electronic communication network.

(4) The enforcement of the present law shall be done by respecting law 677/2001 for people's protection on processing personal data and the free movement of these data, with the subsequent modifications, as well as law 506/2004 r egarding the personal data processing and protection of private life in the field of electronic communication area, with the subsequent changes.".

[5] Zob. szerzej K. de Vries, R. Bellanova, P. De Hert, S. Gutwirth, *The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Desn't It?)*, [w:] *Computers, Privacy and Data Protection: An Element of Choice*, S. Gutwirth, Y. Poullet, P.D. Hert, R. Leenes (red.), Springer 2011, s. 3–23.

[6] Mohini, *On the BVG ruling on Data Retention: "So lange" – here it goes again…* Zob. https://free-group.eu/2010/03/05/so-lange-here-it-goes-again/

[7] *Ibidem*.

trybunały konstytucyjne państw członkowskich UE, najczęściej jako jeden z podstawowych argumentów uzasadniających kompetencje trybunałów do oceny zgodności prawa unijnego, zarówno pierwotnego, jak i wtórnego, z konstytucją[8]. K. Wojtowicz potwierdza, że niektóre krajowe sądy konstytucyjne przekształciły „traktatową" tożsamość narodową w tożsamość konstytucyjną potwierdzając przysługujące im prawo do kontrolowanego zakresu przyznanych UE kompetencji, a nawet sprawdzenia, czy akty unijne respektują tę tożsamość[9].

Zasada tożsamości konstytucyjnej może usprawiedliwiać odstąpienie od zasady przyznania prymatu prawu unijnemu w sytuacji konfliktu przepisów unijnych z prawem krajowym. O. Lynskey zwraca uwagę, że chociaż w orzeczeniu w sprawie *Digital Rights Ireland* słowo „pierwszeństwo", „nadrzędność" prawa unijnego nie zostało przywołane, to jednak orzeczenie rzutuje na tło sporu pomiędzy sądami konstytucyjnymi a Trybunałem Sprawiedliwości w kontekście zasady pierwszeństwa praw unijnego i prawa konstytucyjnego państw członkowskich[10]. Powstaje pytanie, który organ jest uprawniony do ustalenia, co należy rozumieć pod pojęciem „tożsamości konstytucyjnej" w konkretnej sprawie, tj. czy będzie to sąd konstytucyjny danego państwa członkowskiego, czy Trybunał Sprawiedliwości. A. von Bogdandy i S. Schill twierdzą, że treść „*tożsamości konstytucyjnej*" jest określana przez pryzmat prawa konstytucyjnego państw członkowskich[11]. W mojej ocenie, pojęcie tożsamości narodowej, które obejmuje tzw. tożsamość konstytucyjną, stanowi autonomiczne pojęcie prawa unijnego, a tym samym organem uprawnionym do zweryfikowania, czy określone przez sąd konstytucyjny standardy, które miałby usprawiedliwiać ingerencję w prawa jednostki (np. standardy wdrażające wytyczne z orzeczenia *Digital Rights Ireland*), mieszczą się, czy też wykraczają poza formułę tzw. tożsamości konstytucyjnej, jest Trybunał Sprawiedliwości. Taki wniosek wydaje się być uzasadniony w świetle konieczności zachowania zasady jednolitego stosowania prawa unijnego we wszystkich państwach członkowskich UE.

Wracając do wyroku niemieckiego Federalnego Trybunału Konstytucyjnego, należy zauważyć, że w ocenie trybunału krajowe przepisy dotyczące zatrzymywania danych nie spełniały testu proporcjonalności, który jest oparty o cztery kryteria, tj. kryterium ochrony danych (ang. *proportional data security standards*); zakresu stosowania danych (ang. *proportional purpose limitation*), przejrzystości (ang. *transparency*) oraz kryterium sądowej kontroli oraz środków ochrony prawnych (ang. *judicial control and effective legal remedies*)[12]. Niemiecki Federalny Trybunał Konstytucyjny nie określił, jaki poziom bezpieczeństwa danych powinien być gwarantowany w przepisach wewnętrznych

---

[8] A. Wróbel, *Tożsamość narodowa czy różnorodność w jedności*, „Europejski Przegląd Sądowy" 2012, nr 8, s. 1.

[9] K. Wojtowicz, *Zachowanie tożsamość konstytucyjnej państwa polskiego w ramach UE – uwagi na tle wyroku TK z dnia 24 listopada 2010 r., (k 32/09)*, „Europejski Przegląd Sądowy" 2011, nr 11, s. 11.

[10] O. Lynskey, *The Data Retention Directive is incompatibile with the rights to privacy and data retention protection and is invalid in its entirety: Digital Rights Ireland*, "Common Market Law Review" 2014, nr 51, s. 1799. Zob. szerzej P. Brzeziński, *Zasada pierwszeństwa w orzecznictwie sądów konstytucyjnych państw członkowskich UE*, „Ius Novum" 2010, nr 1; s. 77–01.

[11] A. von Bogdandy, S. Schill, *Overcoming absolute primacy: respect for national identity under the Lisbon Treaty*, „Common Market Law Review" 2011, nr 48, s. 1429.

[12] K. de Vries, R. Bellanova, P. De Hert, S. Gutwirth, *op. cit.*, s. 8.

państwa, ale wspomniał, że to musi być „*bardzo wysoki poziom bezpieczeństwa*", i że „*bierze pod uwagę wszystkie nowe odkrycia*" oraz musi obejmować nadzór przez organ zewnętrzny, jak również odpowiedni system sankcji[13]. Warto zauważyć, że Trybunał Sprawiedliwości w sprawie *Digital Rights Ireland* nie wskazał, że nieuprawniony dostęp do zatrzymywanych danych powinien być sankcjonowany. W odniesieniu do kryterium zakresu korzystania z danych, z orzeczenia niemieckiego trybunału wynika, że dostęp do danych jest możliwy co do zasady, jeżeli istnieje uzasadnione podejrzenie popełnienia poważnego przestępstwa opisanego w katalogu przestępstw w ustawodawstwie wewnętrznym. Kryterium przejrzystości zostanie zachowane, jeżeli zostanie stwierdzone, że brak dostępu do zatrzymanych danych zniweczy wysiłek prowadzonego śledztwa oraz jeżeli osoby, który dane zostaną zatrzymane, zostaną o tym poinformowane po zakończeniu właściwego postępowania[14]. Ostatnie kryterium zostanie spełnione, jeżeli bezpośredni dostęp do danych będzie mógł być poddany kontroli sądowej[15].

Warto zauważyć, że rumuński oraz niemiecki sąd konstytucyjny poddały ocenie przepisy implementujące dyrektywę 2006/24/WE stosując podobny test zgodności. W przeciwieństwie do orzeczenia Niemieckiego Federalnego Trybunału Konstytucyjnego, rumuński sąd położył większą uwagę na kwestie blankietowego przechowywania danych[16]. W przeciwieństwie do niemieckiego sądu konstytucyjnego, rumuński naczelny sąd administracyjny uważa, że korzystanie z danych stanowi mniej radykalne zagrożenie dla jednostek niż blankietowe przechowywanie danych, gdyż tylko w tym ostatnim wypadku takie działanie tworzy sytuację, w której naruszenie prawa do życia prywatnego, wolności wypowiedzi, jak również przetwarzanie danych nie stanowi wyjątku, lecz zasadę[17].

Podobnie również, w dniu 1 lutego 2011 roku cypryjski Sąd Najwyższy, stwierdził w rozpoznawanej sprawie karnej, że regulacje krajowe implementujące dyrektywę 2006/24/WE nie są zgodne z konstytucyjnymi prawami takimi jak prawo do życia prywatnego oraz tajemnicy porozumiewania się i z tych względów dane telekomunikacyjne zatrzymane przez policję nie mogą służyć jako dowód w sprawie. Cypryjski Sąd Najwyższy skoncentrował się na kwestii dostępu do danych przez organy krajowe, czyli kwestii, która jest poza zakresem przedmiotowym dyrektywy. Poza zakresem analizy cypryjskiego sądu było zagadnienie zatrzymywania danych na mocy przepisów implementujących dyrektywę 2006/24/WE. W 2006 roku do cypryjskiej konstytucji został wprowadzony art. 1a, z którego wynika, że żaden przepis konstytucji nie może stanowić podstawy do uchylenia lub anulowania jakiegokolwiek przepisu prawa cypryjskiego, aktu lub środków podjętych przez Republikę Cypru, które są konieczne dla zapewnienia zgodności z prawem unijnym[18]. Innymi słowy, na mocy art. 1a cypryjskiej konstytucji istnieje podstawa do formułowania domniemania

---

[13] Mohini, *On the BVG ruling on Data Retention: "So lange" – here it goes again…* Zob. https://free-group.eu/2010/03/05/so-lange-here-it-goes-again/

[14] K. de Vries, R. Bellanova, P. De Hert, S. Gutwirth, *op. cit.*, s. 8.

[15] *Ibidem*, s. 8.

[16] *Ibidem*, s. 14–15.

[17] *Ibidem*, s. 15.

[18] Ch. Markou, *The Cyprus and Rother EU court rulings on data retention: The Directive as a privacy bomb*, „Computer Law & Security Review" 2012, nr 28, s. 472.

zgodności aktu implementującego dyrektywę 2006/24/WE do cypryjskiego systemu prawnego z konstytucją. Można zauważyć, że istniejące na gruncie cypryjskiej konstytucji domniemanie zgodności z konstytucją przepisów implementujących prawo unijne może czynić niemożliwym zastosowanie zasady pierwszeństwa.

Również Czeski Sąd Konstytucyjny w wyroku z dnia 22 marca 2011r. orzekł o niezgodności regulacji krajowych z uwagi na ich nieprecyzyjność oraz brak odpowiednich zabezpieczeń danych. Brak było ponadto dokładnego wskazania, które z organów mają mieć dostęp do danych. Co więcej, czeski ustawodawca wdrożył do krajowego systemu prawnego dyrektywę 2006/24/WE w szerszym zakresie niż było to konieczne przewidując obowiązek zatrzymywania informacji na temat ilości transferowanych danych (ang. *the volume of data transferred*), stosowania szyfrowania danych (ang. *use of encryption*), identyfikowania kart pre-paid SIM (ang. *identification of pre-paid SIM cards*), korzystania z publicznych telefonów (ang. *use of public phone booths*)[19]. Przepisy prawa czeskiego nie przewidywały również ograniczenia korzystania z danych w celu wykrywania poważnych przestępstw, obowiązku poinformowania osoby, której dane zostały zatrzymane oraz procedur regulujące zniszczenie danych[20].

Można zauważyć, że zarówno cypryjski Sąd Najwyższy, jak i czeski Sąd Konstytucyjny nie formułowały zarzutów pod adresem samej dyrektywy 2006/24/WE, lecz aktów implementujących dyrektywę w zakresie, w jakim regulowały one zasady dostępu do danych przez właściwe organy. Niemiecki Federalny Trybunał Konstytucyjny oraz część sądów konstytucyjnych zakwestionowały przepisy krajowe regulujące zasady dostępu do danych, które pozostawały poza zakresem dyrektywy. Wyrok *Digital Rights Ireland* ponownie spowodował falę kolejnych wyroków sądów konstytucyjnych państw członkowskich[21].

3. PODSUMOWANIE

Podsumowując, orzeczenie w sprawie *Digital Rights Ireland* może być zaliczone do orzeczeń stanowiących kominie milowe w zakresie przestrzegania i stosowania praw podstawowych w płaszczyźnie prawa unijnego. Trybunał Sprawiedliwości dokonał oceny zgodności przepisów dyrektywy 2006/24/WE, które w imię zapewnienia bezpieczeństwa publicznego i walki z terroryzmem, wprowadziły daleko idące ograniczenia w korzystaniu z praw podstawowych, w szczególności z prawa do prywatności oraz prawa do ochrony danych osobowych, oraz wolności, gwarantowanych przez KPP oraz EKPC. Orzeczenie to miało ogromny wpływ na linię orzeczniczą sądów konstytucyjnych w przedmiocie przepisów implementujących

---

[19] N. Vainio, S. Miettinen, *Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States*, „International Journal of Law and Information Technology" 2015, nr 23, s. 295. Por. P. Molek, *Czech Constitutional Court Unconstitutionality of the Czech Implementation of the Data Retention Directive; Decision of 22 March 2011, Pl. ÚS 24/10*, „European Constitutional Law Review" 2012, nr 8, s. 348–349.

[20] N. Vainio, S. Miettinen, *op. cit.*, s. 295.

[21] Zob. M. Salgado, *Data retention – what now?*, „Privacy & Data Protection" 2014, nr 14(7), s. 14.

do wewnętrznych systemów prawnych dyrektywę 2006/24/WE. Standardy prawne wyznaczone przez Trybunał Sprawiedliwości w orzeczeniu w sprawie *Digital Rights Ireland* oraz sądy konstytucyjne powinny być respektowane przez ustawodawców krajowych. Obecnie w wielu państwach członkowskich toczą się prace nad nowymi przepisami dotyczącymi zatrzymywania danych telekomunikacyjnych.

Z pewnością bardzo trudno będzie osiągnąć równowagę pomiędzy obowiązkiem zapewnienia ochrony praw podstawowych gwarantowanych w płaszczyźnie prawa unijnego na mocy przepisów KPP, Traktatu o Funkcjonowaniu Unii Europejskiej (prawa podstawowe chronione są jako zasady ogólne), w płaszczyźnie prawa międzynarodowego przede wszystkim na mocy EKPC, a obowiązkiem utrzymania międzynarodowego pokoju i bezpieczeństwa, które stanowią cel interesu ogólnego Unii. Jeżeli uznać, że nadrzędną wartością jest ochrona życia ludzkiego, wówczas można postawić tezę, że ochrona interesu publicznego powinna przeważyć nad ochroną interesu prywatnego, co nie oznacza, że nadrzędność interesu publicznego powinna być niczym nieograniczona. Granice ingerencji w interesy prywatne wyznacza właśnie KPP i EKPC, zaś w płaszczyźnie prawa wewnętrznego państw członkowskich ustawy zasadnicze i ustawodawcy krajowi powinni je respektować.

BIBLIOGRAFIA

von Bogdandy A., Schill S., *Overcoming absolute primacy: respect for national identity under the Lisbon Treaty*, „Common Market Law Review" 2011, nr 48.

Brzeziński P., *Zasada pierwszeństwa w orzecznictwie sądów konstytucyjnych państw członkowskich UE*, „Ius Novum" 2010, nr 1.

Decyzja nr. 13627, Bułgarskiego Naczelnego Sądu Administracyjnego z dnia 11 grudnia 2008. Tekst orzeczenia jest dostępny na stronie internetowej: http://www.econ.bg/law86421/enactments/article153902.html. Komentarz do orzeczenia w języku angielskim: http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention

Decyzja nr.1258, Rumuńskiego Sądu Konstytucyjnego z dnia 8 października 2009. Tłumaczenie orzeczenia w języku angielskim (nieoficjalne):http://www.legiinternet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf

Lynskey O., *The Data Retention Directive is incompatibile with the rights to privacy and data retention protection and is invalid in its entirety: Digital Rights Ireland*, „Common Market Law Review" 2014, nr 51.

Markou Ch., *The Cyprus and Rother EU court rulings on data retention: The Directive as a privacy bomb*, „Computer Law & Security Review" 2012, nr 28.

Mohini, *On the BVG ruling on Data Retention: "So lange" – here it goes again…* Zob. https://free-group.eu/2010/03/05/so-lange-here-it-goes-again/

Molek P., *Czech Constitutional Court Unconstitutionality of the Czech Implementation of the Data Retention Directive*; Decision of 22 March 2011, Pl. ÚS 24/10, „European Constitutional Law Review" 2012, nr 8.

Salgado M., *Data retention – what now?*, „Privacy & Data Protection" 2014, nr 14(7).

Vainio N., Miettinen S., *Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States*, „International Journal of Law and Information Technology" 2015, nr 23.

de Vries K., Bellanova R., Hert P. De, Gutwirth S., *The German Constitutional Court Judgment on Data Retention : Proportionality Overrides Unlimited Surveillance (Desn't It?)*, [w:] *Computers, Privacy and Data Protection: An Element of Choice*, Gutwirth S., Poullet Y., Hert P.D., Leenes R. (red.), Springer 2011.

Wojtowicz K., *Zachowanie tożsamość konstytucyjnej państwa polskiego w ramach UE – uwagi na tle wyroku TK z dnia 24 listopada 2010 r., (k 32/09)*, „Europejski Przegląd Sądowy" 2011, nr 11.

Wróbel A., *Tożsamość narodowa czy różnorodność w jedności*, „Europejski Przegląd Sądowy" 2012, nr 8.

STANOWISKO WYBRANYCH SĄDÓW KONSTYTUCYJNYCH PAŃSTW CZŁONKOWSKICH UE/WE W SPRAWIE ZGODNOŚCI REGULACJI IMPLEMENTUJĄCYCH DYREKTYWĘ 2006/24/WE Z PRAWAMI PODSTAWOWYMI

Streszczenie

Przedmiotem niniejszego artykułu jest wskazanie na orzecznictwo sądów konstytucyjnych dotyczące regulacji implementujących dyrektywę 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 do systemów prawnych wybranych państw członkowskich UE/WE. W artykule przedstawiono zasadnicze argumenty podnoszone przez sądy konstytucyjne wybranych państw członkowskich UE/WE, które uznały akty prawne implementujące dyrektywę 2006/24/WE za niezgodne z prawami podstawowymi chronionymi w regulacjach wewnętrznych w systemach prawnych tych państw członkowskich oraz w Europejskiej Konwencji Praw Człowieka oraz Karcie Praw Podstawowych.

Słowa kluczowe: retencja danych o ruchu i lokalizacji, ochrona praw podstawowych, prawo unijne

SELECTED EU/EC CONSTITUTIONAL COURTS' POSITION ON THE COMPLIANCE OF DIRECTIVE 2006/24/EC IMPLEMENTING REGULATIONS WITH FUNDAMENTAL RIGHTS

Summary

The article aims to present the rulings of constitutional courts on regulations implementing Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networking and amending Directive 2002/58/EC in the legal systems of selected member states of the EU/UC. The article discusses basic arguments raised by the constitutional courts of selected EU/EC member states, which recognised legal regulations implementing Directive 2006/24/EC to be in conflict with fundamental rights protected in domestic regulations of those member states' legal systems as well as the European Convention on Human Rights and the Charter of Fundamental Rights of the EU.

Key words: retention of data on traffic and location, fundamental rights protection, European Union law