Druk nr 1470

Warszawa, 16 lutego 2007 r.

SEJM
RZECZYPOSPOLITEJ POLSKIEJ
V kadencja
Komisja Infrastruktury
INF-00-37/07

Pan
Marek Jurek
Marszałek Sejmu
Rzeczypospolitej Polskiej

Na podstawie art. 32 ust. 2 regulaminu Sejmu, Komisja Infrastruktury wnosi projekt ustawy:

- o zmianie ustawy - Prawo telekomunikacyjne.

Do reprezentowania Komisji w pracach nad projektem ustawy został upoważniony poseł Antoni Mężydło.

Z poważaniem

Przewodniczący Komisji

(-) Janusz Kołodziej

Projekt

Ustawa

z dnia.....2007 r

o zmianie ustawy — Prawo telekomunikacyjne

Art. 1

W ustawie z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm [1].)"

art. 165 ust. 1 otrzymuje brzmienie:

„1. Operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych przetwarzający dane transmisyjne dotyczące abonentów i użytkowników końcowych jest obowiązany, z uwagi na realizację przez uprawnione organy zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego dane te przechowywać przez okres 5 lat. Obowiązek uważa się za wykonany w przypadku gdy zaprzestający działalności operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych przekaże do przechowywania dane transmisyjne innemu operatorowi publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych. Po upływie tego okresu, dane transmisyjne są usuwane lub anonimizowane przez operatora publicznej sieci telekomunikacyjnej lub dostawcę publicznie dostępnych usług telekomunikacyjnych, którzy je przechowują. Operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych przechowujący dane transmisyjne jest obowiązany dołożyć szczególnej staranności w celu ochrony bezpieczeństwa i poufności tych danych oraz interesów osób, których dane dotyczą."

Art. 2

Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

---

[1] Dz.U z 2004 Nr 273 poz. 2703, Dz.U z 2005 Nr 163, poz 1362, Nr 267, poz 2258, Dz.U 2006 Nr 12, poz. 66,

Uzasadnienie

Obecny zapis art. 165 ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, obowiązujący od dnia 9 lutego 2006 r., wprowadzony ustawą z dnia 29 grudnia 2005 r. (Dz. U. z 2006 r., Nr 12, poz. 66), wyznacza 2 letni okres przechowywania danych transmisyjnych dotyczących abonentów i użytkowników końcowych, które udostępniane są uprawnionym organom realizującym zadania i obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Do tego czasu, okres przechowywania takich danych wynosił jedynie 12 miesięcy. Natomiast jeszcze wcześniej obowiązujący art. 40 ustawy z dnia 21 lipca 2000 r. Prawo telekomunikacyjne (Dz. U. nr 73 poz. 852 z późn. zm.) stanowił, iż operator powinien przekazywać żądane informacje od chwili rozpoczęcia eksploatacji sieci.

Ważne znaczenie dowodowe bilingów i innych danych telekomunikacyjnych w postępowaniach karnych, zarówno o najpoważniejsze sprawy, w tym o zabójstwa, działalność zorganizowanych grup lub związków przestępczych o charakterze zbrojnym, terroryzm, wytwarzanie i obrót środkami odurzającymi lub substancjami psychotropowymi, korupcję, lecz także inne drobniejsze przestępstwa, choć bardzo dolegliwe dla pokrzywdzonych, jak np. groźby karalne, jest bezsporne dla organów ścigania i wymiaru sprawiedliwości. Są to bowiem niejednokrotnie jedyne dowody, które umożliwiają wykrycie sprawców przestępstwa, osób z nimi współdziałających, a także ustalenie nieznanych wcześniej pokrzywdzonych, czy nawet miejsc ukrywania się podejrzanych.

Jedną z fundamentalnych zasad polskiego procesu karnego jest legalizm, który na prokuraturę i organy ścigania obowiązek prowadzenia postępowania przygotowawczego w każdej sprawie ściganej z oskarżenia publicznego. Aby był on należycie realizowany, należy prowadzących takie postępowania wyposażyć w odpowiednie instrumenty prawne, które umożliwią zebranie i zabezpieczenie dla potrzeb śledztwa lub dochodzenia obiektywnych dowodów. Ważnym wśród tych dowodów są bilingi i inne dane telekomunikacyjne, gdyż jednoznacznie wskazują na nawiązanie kontaktu telefonicznego między sprawcami lub między sprawcą i pokrzywdzonym. Ten dowód jest obiektywny, niepodatny na przestępczą ingerencję i trwały, stad też potrzeba szerszego niż dotychczas dostępu do jego wykorzystania.

W tym miejscu trzeba powołać się na wybrane postępowania karne, w których dostęp do danych telekomunikacyjnych doprowadził do wykrycia sprawców różnych przestępstw.

W 2005 r. na wysypisku śmieci koło Solca Kujawskiego znaleziono rozkawałkowane zwłoki kobiety i wyłącznie na podstawie bilingu z telefonu pokrzywdzonej zidentyfikowano sprawcę zabójstwa.

W sprawie tzw. „łowców skór" to właśnie na podstawie bilingów Sąd Okręgowy w Łodzi kilka dni temu w wyroku potwierdził kontakty niektórych pracowników pogotowia ratunkowego z zakładami pogrzebowymi.

Na podstawie numeru IMEI aparatu telefonicznego na tzw. kartę, ujęto w 2005 r. podejrzanego o fałszywe alarmy bombowe na lotnisku w Katowicach i klasztorze na Jasnej Górze.

W 2000 r. Łodzi w sprawie uprowadzenia właściciela miejscowej stacji benzynowej i żądania okupu bilingi telefonu, z którego sprawcy kontaktowali się z rodziną uprowadzonego, pozwoliły na ustalenie tożsamości organizatora przestępstwa.

Informacje uzyskane od operatorów telefonicznych, dotyczące tzw. numeru IMEI telefonu komórkowego, znalezionego na miejscu zdarzenia, a następnie wykazy połączeń z takiego aparatu, często pozwalają na identyfikację sprawcy przestępstwa**.**

W śledztwie Prokuratury Apelacyjnej w Krakowie, powszechnie znanym jako „mafia paliwowa", prowadzonym w sprawie działalności zorganizowanej grupy przestępczej, zajmującej się obrotem paliwami ciekłymi, oszustwami, praniem pieniędzy, korumpowaniem funkcjonariuszy publicznych i innymi przestępstwami na niespotykaną dotychczas w kraju skalę, bilingi i dane abonentów posłużyły do weryfikacji wcześniejszych ustaleń, jak też były podstawą do przeprowadzenia następnych dowodów, w tym przesłuchań nieznanych wcześniej świadków.

Wyraźnie jednak należy wskazać, że obowiązujący aktualnie okres 2 lat przechowywania danych transmisyjnych, nadal jest zbyt krótki dla właściwego ich wykorzystania dowodowego w postępowaniach przygotowawczych prowadzonych przez prokuraturę, policję i inne uprawnione organy. W sprawach o wszystkie przestępstwa, czynności wykrywcze muszą często obejmować zdarzenia mające miejsce kilka lat wstecz, a wiec nie będzie wówczas możliwe sięganie po dowody, jakimi są bilingi i inne dane telekomunikacyjne, gdyż wcześniej, po upływie 2 lat od wytworzenia, zostaną one zniszczone.

Zdarzają się co prawda sytuacje, że operator mimo upływu ustawowego okresu udostępnia prokuratorowi potrzebne dane, jak to ma obecnie miejsce w śledztwie prowadzonym we Wrocławiu w sprawie korupcji wśród sędziów piłkarskich, działaczy i zawodników, lecz nie można oczekiwać, że będzie to praktyka powszechna.

Należy więc zapewnić prokuraturze i innym organom prowadzącym śledztwa lub dochodzenia możliwości skutecznego działania, a jedną z nich jest szersze niż dotychczas wykorzystywanie tak istotnych dowodów, jak bilingi i inne dane rejestrowane przez operatorów telekomunikacyjnych. Aby tak się stało, konieczne jest wydłużenie z 2 do 5 lat okresu przechowywania danych przez operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych.

Z tych właśnie powodów, wszystkie propozycje zmian obowiązującego prawa, zmierzające do wyznaczenia dłuższego niż dotychczas okresu udostępniania uprawnionym organom danych przez operatorów telekomunikacyjnych, są popierane przez Ministerstwo Sprawiedliwości.

Oczywiście, uwzględniając prawne potrzeby organów ścigania i prokuratury, najlepiej by się stało, gdyby dane telekomunikacyjne były dostępne aż do przedawnienia karalności za przestępstwa. Zdając sobie jednak sprawę z trudności w zyskaniu dla takiej koncepcji aprobaty ustawodawcy i opinii publicznej, postulować należy wydłużenie obecnie obowiązującego okresu do 5 lat.

Wyraźnie trzeba wskazać, że koncepcja będąca przedmiotem projektowanej regulacji, jest zgodna z prawem Unii Europejskiej, gdyż dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 roku w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianych publicznych sieci łączności, przewiduje możliwość wydłużenia ustalonego ogólnie na 2 lata okresu przechowywania takich informacji, przez każde z państw członkowskich pod warunkiem przedstawienia stosownego uzasadnienia. Dwa kraje Unii Europejskiej przyjęły dłuższy okres retencji takich danych, a mianowicie Włochy – 29 miesięcy i Irlandia – 36 miesięcy.

W przypadku Polski, uzasadnieniem wydłużenia czasu przechowywania danych telekomunikacyjnych może być specyfika procedury karnej, sformalizowanej i legalistycznej, a także efektywność tego dowodu w zwalczaniu przestępczości, w tym tej najpoważniejszej.

Warszawa, 23 lutego 2007 r.

BAS-WAEM-471/07

Pan
Marek Jurek
Marszałek Sejmu
Rzeczypospolitej Polskiej

Opinia prawna
w sprawie zgodności z prawem Unii Europejskiej komisyjnego projektu ustawy o zmianie ustawy – Prawo telekomunikacyjne (przedstawiciel wnioskodawców: poseł Antoni Mężydło)

Na podstawie art. 34 ust. 9 uchwały Sejmu Rzeczypospolitej Polskiej z dnia 30 lipca 1992 r. - Regulamin Sejmu Rzeczypospolitej Polskiej (M.P. z 2002 r. Nr 23, poz. 398, ze zmianami) sporządza się następującą opinię:

1. Przedmiot projektu ustawy

Przedstawiony projekt ustawy przewiduje zmianę brzmienia art. 165 ust. 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, ze zmianami). Proponowana zmiana polega na wydłużeniu okresu, w którym operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych, przetwarzający dane transmisyjne dotyczące abonentów i użytkowników końcowych, jest obowiązany, z uwagi na realizację przez uprawnione organy zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, dane te przechowywać. Okres ten wynosi obecnie 2 lata, natomiast według projektu ma wynosić 5 lat. W ocenie wyrażonej przez projektodawców w uzasadnieniu, dotychczas „obowiązujący aktualnie okres dwóch lat przechowywania danych transmisyjnych […] jest zbyt krótki dla właściwego ich wykorzystania dowodowego w postępowaniach przygotowawczych prowadzonych przez prokuraturę, policję i inne uprawnione organy”.

Proponowana ustawa ma wejść w życie po upływie 14 dni od dnia ogłoszenia.

2. Stan prawa wspólnotowego w materii objętej projektem ustawy

Zmiana proponowana w przedłożonym projekcie wymaga oceny z punktu widzenia zgodności z przepisami prawa Unii Europejskiej dotyczącymi ochrony danych osobowych oraz przetwarzania danych osobowych w sektorze łączności elektronicznej.

1. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995 r., s. 31, ze zmianami; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, s. 355) przewiduje, że państwa członkowskie są zobowiązane chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych. Art. 13 dyrektywy stanowi jednak, że państwo członkowskie może przyjąć środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków, przewidzianego na podstawie niektórych przepisów dyrektywy, kiedy ograniczenie takie stanowi środek konieczny dla zabezpieczenia: a) bezpieczeństwa narodowego, b) obronności, c) bezpieczeństwa publicznego, d) działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych lub w sprawach o naruszenie zasad etyki w zawodach podlegających regulacji, e) ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub Unii Europejskiej, łącznie z kwestiami pieniężnymi, budżetowymi i podatkowymi, f) funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych, nawet sporadycznie, z wykonywaniem władzy publicznej w przypadkach wymienionych w lit. c–e, g) ochrony osoby, której dane dotyczą oraz praw i wolności innych osób.

2. W odniesieniu do przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej obowiązują przepisy szczególne zawarte w dyrektywie 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. WE L 201 z 31.7.2002 r., s. 37, ze zmianami; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 29, s. 514). W motywie 11 dyrektywy stwierdza się, że dyrektywa nie zmienia istniejącej równowagi między prawem do prywatności osoby fizycznej a możliwością państw członkowskich do podejmowania środków, określonych w art. 15 ust. 1 dyrektywy, niezbędnych do ochrony bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając gospodarczy dobrobyt państwa, gdy działania dotyczą zagadnień bezpieczeństwa państwa) i wykonywania prawa karnego. Wskutek tego, dyrektywa nie wpływa na możliwości państw członkowskich zgodnego z prawem przejmowania danych w łączności

elektronicznej lub podejmowania innych środków, jeżeli jest to konieczne dla któregokolwiek z tych celów i zgodne z europejską Konwencją o ochronie praw człowieka i podstawowych wolności, podpisaną w Rzymie 4 listopada 1950 roku[1], której wykładnię stanowi orzecznictwo Europejskiego Trybunału Praw Człowieka. Środki tego rodzaju muszą być właściwe, współmierne do zamierzonego celu i niezbędne w ramach społeczeństwa demokratycznego oraz powinny podlegać stosownym zabezpieczeniom zgodnie z europejską Konwencją o ochronie praw człowieka i podstawowych wolności.

Art. 15 ust. 1 dyrektywy 2002/58/WE stanowi, że państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4, i art. 9 dyrektywy (poufność komunikacji, dane o ruchu, wyświetlanie i ograniczenie identyfikacji rozmów przychodzących i wychodzących oraz dane dotyczące lokalizacji inne niż dane o ruchu), gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (tj. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy 95/46/WE. W tym celu państwa członkowskie mogą m.in. uchwalić środki ustawodawcze, przewidujące przechowywanie danych przez określony czas, uzasadnione na podstawie zasad określonych w tym przepisie[2]. Art. 15 ust. 1 dyrektywy 2002/58/WE zastrzega, że wszystkie środki określone w tym przepisie muszą być zgodne z zasadami ogólnymi prawa wspólnotowego, w tym z zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej (TUE).

3. Zgodnie z art. 6 ust. 1 TUE, Unia opiera się na zasadach wolności, demokracji, poszanowania praw człowieka i podstawowych wolności oraz państwa prawnego, które są wspólne dla państw członkowskich. Unia szanuje prawa podstawowe zagwarantowane w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności oraz wynikające z tradycji konstytucyjnych wspólnych dla państw członkowskich, jako zasady ogólne prawa wspólnotowego (art. 6 ust. 2 TUE). Prawa człowieka i podstawowe wolności zostały określone także w Karcie praw podstawowych Unii Europejskiej, proklamowanej w Nicei w dniu 7 grudnia 2000 r. (Dz. Urz. WE C 364 z 18 grudnia 2000 r., s. 1). Dokument ten nie stanowi samodzielnego, wiążącego źródła prawa w Unii Europejskiej.

---

[1] Polska ratyfikowała Europejską Konwencję o ochronie praw człowieka i podstawowych wolności w dniu 19 stycznia 1993 r. Tekst konwencji został opublikowany w Dz. U. z 1993 r. Nr 61, poz. 284, ze zmianami.

[2] Przepis art. 15 ust. 1 dyrektywy ma zastosowanie z zastrzeżeniem przypadku, o którym mowa w art. 15 ust. 1a dyrektywy w brzmieniu przyjętym przez dyrektywę 2006/24/WE (szczegółowo omówionym w pkt. 2.4 niniejszej opinii).

Jednocześnie należy stwierdzić, że zgodnie z postanowieniami wprowadzonymi do TUE na mocy Traktatu z Amsterdamu i Traktatu z Nicei, działania państw członkowskich mogą być przedmiotem oceny politycznej, w kontekście zasad wolności, demokracji, poszanowania praw człowieka i podstawowych wolności oraz państwa prawnego, dokonywanej przez Radę Unii Europejskiej i Parlament Europejski w trybie art. 7 TUE. W przypadku stwierdzenia w ramach tej procedury wyraźnego ryzyka poważnego naruszenia wskazanych zasad w jednym z państw członkowskich, Rada może skierować do tego państwa stosowne zalecenia. W przypadku zaś stwierdzenia poważnego i stałego naruszenia zasad, Rada może zadecydować o zawieszeniu niektórych praw tego państwa wynikających ze stosowania Traktatu, łącznie z prawem do głosowania przedstawiciela rządu tego państwa w Radzie. Analogiczny przepis zawiera Traktat ustanawiający Wspólnotę Europejską (TWE) w art. 309.

4. Ponadto należy wskazać postanowienia 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 zmieniającej dyrektywę 2002/58/WE (Dz. Urz. UE L 105 z 13.4.2006 r., s. 54). Zgodnie z art. 1 ust. 1 dyrektywy, jej celem jest zbliżenie przepisów państw członkowskich w zakresie obowiązków dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności w zakresie zatrzymywania pewnych danych przez nie generowanych lub przetwarzanych, aby zapewnić dostępność przedmiotowych danych do celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego. Dyrektywę stosuje się do danych o ruchu i lokalizacji, dotyczących zarówno osób fizycznych, jak i prawnych, oraz do powiązanych z nimi danych niezbędnych do identyfikacji abonenta lub zarejestrowanego użytkownika; nie odnosi się ona natomiast do treści komunikatów elektronicznych, w tym informacji uzyskiwanych przy użyciu sieci łączności elektronicznej (art. 1 ust. 2 dyrektywy).

Dyrektywa wprowadza zastrzeżenie, że przepisu art. 15 ust. 1 dyrektywy 2002/58/WE (powoływanego wyżej w punkcie 2.2 niniejszej opinii) nie stosuje się do danych, których zatrzymywanie jest wyraźnie wymagane na mocy dyrektywy 2006/24/WE dla celów określonych w art. 1 ust. 1 tej dyrektywy (nowy art. 15 ust. 1a dyrektywy 2002/58/WE). Oznacza to, że w przypadku tego rodzaju danych przepisy krajowe muszą odpowiadać zasadom określonym w dyrektywie 2006/24/WE. Zobowiązuje ona państwa członkowskie do zagwarantowania, że wymienione w art. 5 dyrektywy kategorie danych są zatrzymywane na okresy nie krótsze niż 6 miesięcy oraz nie dłuższe niż dwa lata od daty połączenia (art. 6).

Wyjątek od stosowania przepisów dyrektywy 2006/24/WE stanowi jej art. 12. Państwo członkowskie, znajdujące się w szczególnych okolicznościach – uzasadniających przedłużenie maksymalnego okresu zatrzymywania (2 lata) o ograniczony okres – może podjąć niezbędne środki. Państwo członkowskie musi niezwłocznie powiadomić Komisję Europejską, poinformować pozostałe państwa członkowskie o podjętych środkach oraz wskazać przyczyny ich podjęcia. W ciągu sześciu miesięcy od powiadomienia, Komisja przyjmuje lub odrzuca odnośne środki krajowe, po uprzednim zbadaniu, czy nie stanowią one środka arbitralnej dyskryminacji lub ukrytego ograniczenia w handlu pomiędzy państwami członkowskimi oraz czy nie będą stanowiły przeszkody dla funkcjonowania rynku wewnętrznego. W przypadku braku decyzji Komisji w ciągu tego okresu, środki krajowe zostają uznane za przyjęte.

Dyrektywa 2006/24/WE weszła w życie w dniu 3 maja 2006 r.[3] Termin transpozycji przepisów dyrektywy 2006/24/WE upływa z dniem 15 września 2007 r. Jednocześnie art. 15 ust. 3 dyrektywy upoważnia każde państwo członkowskie do odroczenia do dnia 15 marca 2009 r. stosowania dyrektywy do zatrzymywania danych z zakresu łączności w odniesieniu do dostępu do Internetu, telefonii internetowej i internetowej poczty elektronicznej. W tym celu zainteresowane państwo członkowskie musiało powiadomić Komisję, składając oświadczenie w momencie przyjmowania dyrektywy. Szesnaście państw członkowskich, w tym Polska, złożyło stosowne oświadczenia, które zostały opublikowane wraz z dyrektywą w Dzienniku Urzędowym UE. W „Deklaracji Rzeczypospolitej Polskiej zgodnie z art. 15 ust. 3 dyrektywy 2006/24/WE" (Dz. Urz. UE L 105 z 13.4.2006 r., s. 62) Polska oświadczyła, że skorzysta z możliwości przewidzianej w art. 15 ust. 3 tej dyrektywy, polegającej na odroczeniu stosowania dyrektywy do zatrzymywania danych z zakresu łączności w odniesieniu dostępu do Internetu, telefonii internetowej i internetowej poczty elektronicznej na okres do 18 miesięcy ponad termin przewidziany w art. 15 ust. 1 dyrektywy. Oznacza to, że Polska podjęła decyzję o odroczeniu stosowania dyrektywy w odniesieniu do zatrzymywania wskazanych danych do dnia 15 marca 2009 r. (maksymalny okres odroczenia przewidziany w dyrektywie).

3. Analiza przepisów projektu pod kątem ustalonego stanu prawa wspólnotowego

1. Ocena zgodności projektu z dyrektywą 2006/24/WE jest uzasadniona i konieczna, pomimo że termin jej transpozycji upływa w dniu 15 września 2007 r. (a w odniesieniu do zatrzymywania niektórych danych – w dniu 15 marca 2009 r.). Zgodnie z orzecznictwem Trybunału Sprawiedliwości Wspólnot

[3] Art. 16 dyrektywy stanowi, że wchodzi ona w życie dwudziestego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej; datą publikacji dyrektywy jest dzień 13 kwietnia 2006 r.

Europejskich z art. 10 akapit drugi w związku z art. 249 akapit trzeci TWE wynika, że w okresie transpozycji dyrektywy państwa członkowskie muszą powstrzymać się od podejmowania jakichkolwiek środków, które mogłyby poważnie zaszkodzić realizacji dyrektywy.[4] Art. 10 akapit drugi TWE zakazuje państwom członkowskim podejmowania wszelkich środków, które mogłyby zagrozić urzeczywistnieniu celów Traktatu, natomiast art. 249 akapit trzeci TWE zobowiązuje państwa członkowskie do osiągnięcia rezultatu określonego w dyrektywie, pozostawiając organom krajowym swobodę wyboru formy i środków. Polska w okresie transpozycji dyrektywy 2006/24/WE (3 maja 2006 r. – 15 września 2007 r.) nie może więc przyjąć przepisów, które – w dniu upływu terminu transpozycji – będą niezgodne z dyrektywą.

2. Analiza treści zaproponowanego brzmienia art. 165 ust. 1 zmienianej ustawy jest niezbędna, aby – dokonując oceny zgodności projektu z prawem Unii Europejskiej – określić, czy i w jakim zakresie przepis należy przyporządkować kategoriom zdefiniowanym w dyrektywie 2002/58/WE lub dyrektywie 2006/24/WE.

Projekt zakłada wydłużenie – do 5 lat – okresu obowiązku przechowywania danych transmisyjnych. Podstawą nałożenia tego obowiązku na operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych jest realizacja przez uprawnione organy zadań i obowiązków na rzecz „obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego”.

3. Zgodnie z art. 6 dyrektywy 2002/58/WE dane o ruchu abonentów i użytkowników przetwarzane i przechowywane przez dostawcę publicznej sieci łączności lub publicznie dostępnych usług łączności elektronicznej muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji. Projekt przewiduje usuwanie lub anonimizowanie danych transmisyjnych dopiero po upływie 5 lat. Oznacza to ograniczenie poziomu ochrony danych przewidzianego w dyrektywie. Art. 15 ust. 1 dyrektywy określa podstawy odstąpienia od reżimu ochrony danych osobowych, m.in. możliwość uchwalenia przez państwa członkowskie środków ustawodawczych przewidujących przechowywanie danych przez określony czas. Podstawami odstąpienia od reżimu są: zapewnienie bezpieczeństwa narodowego (tj. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej. Podstawy ograniczenia obowiązku ochrony danych osobowych określone w projekcie odpowiadają podstawom wskazanym w dyrektywie. Jednakże oprócz wskazania

[4] Wyrok Trybunału z dnia 18 grudnia 1997 r. w sprawie *Inter-Environnement Wallonie ASBL* przeciwko *Région Wallonne*, C-129/96, ECR z 1997 r., §45–50, s. I-7411. Por. C. Mik, *Europejskie prawo wspólnotowe. Zagadnienia teorii i praktyki*, t. 1, Warszawa 2000 r., s. 667.

tych podstaw dyrektywa nakazuje zachowanie określonych wymogów. Ograniczenia musza stanowić „środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego" oraz muszą być zgodne z zasadami ogólnymi prawa wspólnotowego, w tym z zasadami określonymi w art. 6 ust. 1 i 2 TUE.

Proponowane wydłużenie okresu przechowywania danych musi spełniać wyżej wymienione kryteria. Dyrektywa jednak, poza wskazaniem kryteriów, nie określa, jaki środek będzie „niezbędny, właściwy i proporcjonalny". Ocena będzie zależeć m.in. od stosowania przyjętych środków. Zgodność z zasadami ogólnymi prawa wspólnotowego może być natomiast przedmiotem oceny politycznej, dokonywanej przez Radę Unii Europejskiej i Parlament Europejski w trybie art. 7 TUE (opisanym w pkt. 2.3 niniejszej opinii).

4. Inny charakter niż wyjątek przewidziany w art. 15 ust. 1 dyrektywy 2002/58/WE ma odstępstwo od reżimu ochrony danych osobowych przewidziane w dyrektywie 2006/24/WE (nowy art. 15 ust. 1a dyrektywy 2002/58/WE). Art. 15 ust. 1a dyrektywy 2002/58/WE wyraźnie wyłącza stosowanie odstępstwa przewidzianego w art. 15 ust. 1 dyrektywy 2002/58/WE. Oznacza to wzajemne wykluczanie się stosowania art. 15 ust. 1 i art. 15 ust. 1a dyrektywy. Jeśli dane nie podlegają obowiązkowemu zatrzymywaniu, to art. 15 ust. 1 dyrektywy „powinien być stosowany w dalszym ciągu" (motyw 12 dyrektywy 2006/24/WE).

Celem i treścią dyrektywy 2006/24/WE jest zagwarantowanie, że zatrzymywane dane o ruchu i lokalizacji przez pewien okres mogłyby być udostępniane do celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego (art. 1 i motyw 9 dyrektywy). Dyrektywa ściśle wyznacza okres, na jaki dane są zatrzymywane: nie krócej niż 6 miesięcy i nie dłużej niż dwa lata od daty połączenia (art. 6 dyrektywy). Okres ten może być przedłużony o określony czas przez państwo członkowskie znajdujące się w szczególnych okolicznościach. Wyjątkowy charakter możliwości przedłużenia czasu zatrzymywania danych jest podkreślony przez szczególną procedurę, która znajduje zastosowanie w przypadku podjęcia przez państwo członkowskie decyzji o przedłużeniu (art. 12 dyrektywy).

W treści przepisu projektu w wymienionych podstawach przechowywania danych mieści się kryterium szczegółowo zdefiniowane w dyrektywie 2006/24/WE, tj. „dochodzenie, wykrywanie i ściganie poważnych przestępstw". Tylko dane zatrzymywane w celu dochodzenia, wykrywania i ścigania poważnych przestępstw podlegają reżimowi tej dyrektywy. W oparciu o podstawy wskazane w przepisie zmienianej ustawy jedynie niektóre sytuacje (i w odniesieniu do **poważnych** przestępstw) będą więc mogły być kwalifikowane jako zatrzymywanie w rozumieniu dyrektywy i jedynie w takim przypadku

można by polską regulację dotyczącą terminu przechowywania danych odnosić do okresu zatrzymywania określonego w dyrektywie. Należy więc rozstrzygnąć, czy przyjęty w projekcie termin (oczywiście tylko w odniesieniu do ściśle wskazanych wyżej podstaw zatrzymywania) jest zgodny z art. 12 dyrektywy. Przedłużenie terminu zatrzymywania zgodnie z dyrektywą jest możliwe wyłącznie w szczególnych okolicznościach. Z projektu nie wynika szczególny charakter okoliczności, w jakich Polska miałaby się znajdować. Uzasadnienie okoliczności szczególnych musi być przedstawione Komisji Europejskiej oraz pozostałym państwom członkowskim UE. Do Komisji Europejskiej należy decyzja o przyjęciu albo odrzuceniu środków krajowych (pkt 2.4 akapit trzeci niniejszej opinii). W ocenie dopuszczalności przyjętych środków znaczenie będzie miał m.in. czas, o jaki przedłużony został okres zatrzymywania danych. W tym kontekście należy zwrócić uwagę, że okres wskazany w projekcie (5 lat) stanowi znaczące – ponad dwukrotne – przedłużenie maksymalnego okresu zatrzymywania.

5. Przy wprowadzaniu regulacji dotyczącej okresu przechowywania danych transmisyjnych należy uwzględnić różnicę, jaka istnieje między instytucją „przechowywania danych przez określony czas" (art. 15 ust. 1 dyrektywy 2002/58/WE) a instytucją „zatrzymywania danych" (dyrektywa 2006/24/WE). Pierwsza jest jedynie wyjątkiem od stosowania reżimu ochrony danych osobowych w sektorze łączności elektronicznej. Druga jest natomiast odrębną instytucją, której uzasadnieniem jest zagwarantowanie, że udostępnianie danych organom odpowiedzialnym za egzekwowanie prawa karnego (w odniesieniu do poważnych przestępstw) nie będzie stanowiło przeszkody dla wewnętrznego rynku łączności elektronicznej oraz będzie odbywało się z poszanowaniem prawa do prywatności, tajemnicy korespondencji i ochrony danych osobowych (motywy 6, 9 i 22 dyrektywy 2006/24/WE, art. 7 i 8 Karty praw podstawowych UE). Treść uzasadnienia sugeruje, że projektodawca, powołując się na dyrektywę 2006/24/WE, odnosi się do instytucji „zatrzymywania danych". Natomiast z proponowanego brzmienia art. 165 ust. 1 ustawy wynika, że chodzi o instytucję z art. 15 ust. 1 dyrektywy 2002/58/WE. Rozróżnienie dwóch reżimów należy mieć na uwadze w przypadku dokonywania transpozycji dyrektywy 2006/24/WE.

4. Konkluzja

Przedmiot projektu ustawy o zmianie ustawy – Prawo telekomunikacyjne jest objęty prawem Unii Europejskiej.

Projekt nie jest sprzeczny z prawem UE, jednakże:

1. Przedłużenie okresu przechowywania danych transmisyjnych stanowi ograniczenie stopnia ochrony danych. Ocena zgodności proponowanego ograniczenia z **dyrektywą 2002/58/WE** będzie uzależniona od stosowania

ustawy. Wprowadzony przepis może też podlegać ocenie politycznej, dokonywanej przez Radę Unii Europejskiej i Parlament Europejski (pkt. 3.3 akapit drugi niniejszej opinii).

2. Do Komisji Europejskiej należeć będzie ocena ewentualnej zgodności proponowanej regulacji z **dyrektywą 2006/24/WE**. Komisja Europejska mogłaby zakwestionować pięcioletni okres przechowywania danych transmisyjnych, uznając że nie istnieją „szczególne okoliczności" jego wprowadzenia, o których mowa w art. 12 dyrektywy. Ponadto wątpliwości budzi przeszło dwukrotne przedłużenie okresu przechowywania danych, w stosunku do wskazanego w dyrektywie maksymalnego okresu zatrzymywania.

Sporządził: Zespół Prawa Europejskiego

Akceptował: Dyrektor Biura Analiz Sejmowych

Michał Królikowski

Deskryptory Bazy REX: bezpieczeństwo, obronność, ochrona danych osobowych, postępowanie karne, prawa człowieka, projekt ustawy, telekomunikacja, Unia Europejska

Warszawa, 23 lutego 2007 r.

BAS-WAEM-472/07

Pan
Marek Jurek
Marszałek Sejmu
Rzeczypospolitej Polskiej

Opinia prawna
w sprawie stwierdzenia – w trybie art. 95a ust. 3 Regulaminu Sejmu – czy komisyjny projekt ustawy o zmianie ustawy – Prawo telekomunikacyjne (przedstawiciel wnioskodawców: poseł Antoni Mężydło) jest projektem ustawy wykonującej prawo Unii Europejskiej

Przedstawiony projekt ustawy przewiduje zmianę brzmienia art. 165 ust. 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, ze zmianami). Proponowana zmiana polega na wydłużeniu okresu, w którym operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych, przetwarzający dane transmisyjne dotyczące abonentów i użytkowników końcowych, jest obowiązany, z uwagi na realizację przez uprawnione organy zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, dane te przechowywać. Okres ten wynosi obecnie 2 lata, natomiast według projektu ma wynosić 5 lat. . W ocenie wyrażonej przez projektodawców w uzasadnieniu, dotychczas „obowiązujący aktualnie okres dwóch lat przechowywania danych transmisyjnych […] jest zbyt krótki dla właściwego ich wykorzystania dowodowego w postępowaniach przygotowawczych prowadzonych przez prokuraturę, policję i inne uprawnione organy".

Przedmiot projektu ustawy o zmianie ustawy – Prawo telekomunikacyjne jest objęty prawem Unii Europejskiej.

Projekt nie jest sprzeczny z prawem UE, jednakże:

– Przedłużenie okresu przechowywania danych transmisyjnych stanowi ograniczenie stopnia ochrony danych. Ocena zgodności proponowanego ograniczenia z dyrektywą 2002/58/WE będzie uzależniona od stosowania

ustawy. Wprowadzony przepis może też podlegać ocenie politycznej, dokonywanej przez Radę Unii Europejskiej i Parlament Europejski w trybie art. 7 Traktatu o Unii Europejskiej i art. 309 Traktatu ustanawiającego Wspólnotę Europejską.

– Do Komisji Europejskiej należeć będzie ocena ewentualnej zgodności proponowanej regulacji z dyrektywą 2006/24/WE. Komisja Europejska mogłaby zakwestionować pięcioletni okres przechowywania danych transmisyjnych, uznając że nie istnieją „szczególne okoliczności" jego wprowadzenia, o których mowa w art. 12 dyrektywy. Ponadto wątpliwości budzi przeszło dwukrotne przedłużenie okresu przechowywania danych, w stosunku do wskazanego w dyrektywie maksymalnego okresu zatrzymywania.

Dyrektywa 2006/24/WE weszła w życie w dniu 3 maja 2006 r. Termin transpozycji przepisów dyrektywy 2006/24/WE upływa z dniem 15 września 2007 r. W okresie transpozycji dyrektywy, który rozpoczął się w dniu 3 maja 2006 r., państwa członkowskie muszą powstrzymać się od podejmowania jakichkolwiek środków, które mogłyby poważnie zaszkodzić realizacji dyrektywy (wyrok Trybunału Sprawiedliwości Wspólnot Europejskich z dnia 18 grudnia 1997 r. w sprawie *Inter-Environnement Wallonie ASBL* przeciwko *Région Wallonne*, C-129/96, ECR z 1997 r., §45–50, s. I-7411.). W szczególności chodzi o zakaz przyjmowania przepisów, które – w dniu upływu terminu transpozycji – będą niezgodne z dyrektywą.

Treść uzasadnienia sugeruje, że projektodawca, określając okres przechowywania danych transmisyjnych, zmierza do implementacji przepisów dyrektywy 2006/24/WE, tj. do wprowadzenia instytucji „zatrzymywania danych". Jednak przy wprowadzeniu tej regulacji należy uwzględnić różnicę, jaka istnieje między instytucją „przechowywania danych przez określony czas" (art. 15 ust. 1 dyrektywy 2002/58/WE) a instytucją „zatrzymywania danych" (dyrektywa 2006/24/WE). Pierwsza jest jedynie wyjątkiem od stosowania reżimu ochrony danych osobowych w sektorze łączności elektronicznej. Druga jest natomiast odrębną instytucją, której uzasadnieniem jest zagwarantowanie, że udostępnianie danych organom odpowiedzialnym za egzekwowanie prawa karnego (w odniesieniu do poważnych przestępstw) nie będzie stanowiło przeszkody dla wewnętrznego rynku łączności elektronicznej oraz będzie odbywało się z poszanowaniem prawa do prywatności, tajemnicy korespondencji i ochrony danych osobowych (motywy 6, 9 i 22 dyrektywy 2006/24/WE, art. 7 i 8 Karty praw podstawowych Unii Europejskiej).

Analiza proponowanego brzmienia art. 165 ust. 1 ustawy prowadzi jednak do wniosku, że regulacja dotyczy „przechowywania danych przez określony czas" (tj. instytucji z art. 15 ust. 1 dyrektywy 2002/58/WE), a nie „zatrzymywania danych" (z dyrektywy 2006/24/WE). Nie można więc uznać, że zmieniana ustawa będzie wykonywać przepisy dyrektywy 2006/24/WE. W

przypadku dokonywania transpozycji tej ostatniej dyrektywy należy mieć na uwadze rozróżnienie, które wprowadza prawo UE w zakresie znaczenia i stosowania instytucji „przechowywania danych” i instytucji „zatrzymywania danych”.

Projekt ustawy o zmianie ustawy – Prawo telekomunikacyjne **nie jest projektem ustawy wykonującej prawo Unii Europejskiej**.

Sporządził: Zespół Prawa Europejskiego

Akceptował: Dyrektor Biura Analiz Sejmowych

Michał Królikowski

Deskryptory Bazy REX: bezpieczeństwo, obronność, ochrona danych osobowych, postępowanie karne, prawa człowieka, projekt ustawy, telekomunikacja, Unia Europejska