



KOMISJA WSPÓLNOT EUROPEJSKICH

Bruksela, dnia 21.9.2005
COM(2005) 438 końcowy

2005/0182 (COD)

Wniosek dotyczący

DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie zatrzymywania przetwarzanych danych w związku ze świadczeniem publicznych usług łączności elektronicznej (2002 r.), zmieniająca dyrektywę 2002/58/WE

(przedstawiona przez Komisję)

{SEC(2005) 1131}

UZASADNIENIE

1. KONTEKST WNIOSKU

- **Podstawa i cele wniosku**

Obywatele coraz częściej dokonują codziennych operacji i transakcji, korzystając z sieci i usług łączności elektronicznej. W wyniku wykonywanych przy tej okazji połączeń generowane są „dane o ruchu” lub „dane o lokalizacji” zawierające na przykład szczegóły dotyczące lokalizacji dzwoniącego, wybranego numeru oraz czasu i długości połączenia. Dostępność wspomnianych danych o ruchu w połączeniu z danymi umożliwiającymi identyfikację abonenta lub osoby korzystającej z usługi jest ważna do celów związanych z egzekwowaniem prawa i bezpieczeństwem, takich jak zapobieganie, dochodzenie, wykrywanie i karanie poważnych przestępstw, takich jak działalność terrorystyczna i przestępczość zorganizowana.

Jednakże ze względu na zmiany, jakie nastąpiły w modelach działalności gospodarczej i ofertach usługowych, takie jak taryfy zryczałtowane, usługi na zasadzie przedpłaty (*pre-paid*) oraz nieodpłatne usługi łączności elektronicznej, dane o ruchu mogą nie zawsze być zatrzymywane przez wszystkich operatorów w takim samym stopniu, jak to miało miejsce w ostatnich latach, w zależności od świadczonej usługi. Tendencja ta uwydatniła się jeszcze bardziej przy okazji najnowszych ofert usług telefonii internetowej (*Voice over IP*) czy usług telefonii stacjonarnej opartych na stawkach zryczałtowanych. W takich przypadkach operatorzy nie musieliby już przechowywać danych o ruchu w celu naliczania opłat. Jeżeli dane o ruchu nie są zatrzymywane w celu naliczania opłat ani w innych celach związanych z działalnością gospodarczą, to nie będą one dostępne dla organów publicznych w razie uzasadnionej prawnie potrzeby dostępu do takich danych. Innymi słowy taka zmiana sytuacji utrudnia znacznie organom publicznym wypełnianie obowiązków polegających na zapobieganiu i zwalczaniu zorganizowanej przestępczości i terroryzmu, a przestępcom ułatwia komunikowanie się ze sobą bez obawy, że dane na temat połączenia umożliwią organom ścigania trafienie na ich ślad.

Przyjęcie ujednoczonych przepisów w tej dziedzinie na poziomie UE stało się obecnie pilną sprawą. Kilka Państw Członkowskich przyjęło – lub planuje przyjąć – krajowe środki zobowiązujące niektórych lub wszystkich operatorów do zatrzymywania określonych rodzajów danych do ich ewentualnego wykorzystania w celach wyszczególnionych powyżej. Różnice między Państwami Członkowskimi w zakresie prawnych, regulacyjnych i technicznych przepisów w dziedzinie zatrzymywania danych o ruchu stanowią przeszkodę dla rynku wewnętrznego łączności elektronicznej, gdyż usługodawcy natykają się na różne wymagania odnośnie do rodzaju danych przeznaczonych do zatrzymywania oraz warunków zatrzymywania. Stąd też omawiane przepisy powinny zostać ujednoczone zgodnie z art. 14 Traktatu WE.

- **Kontekst ogólny**

W swojej Deklaracji w sprawie zwalczania terroryzmu wydanej dnia 25 marca 2004 r. Rada Europejska potwierdziła konieczność posiadania przepisów na poziomie UE,

które gwarantowałyby dostępność danych o ruchu dla celów zwalczania terroryzmu na obszarze 25 Państw Członkowskich. W wyniku terrorystycznych ataków bombowych w Madrycie Rada Europejska zaleciła Radzie zbadanie „wniosków dotyczących ustalenia przepisów w sprawie zatrzymywania przez usługodawców danych o ruchu połączeń” z możliwością przyjęcia ich w 2005 r. Zarówno Rada Europejska w swoich konkluzjach z dnia 16 i 17 czerwca br., jak i Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych na specjalnym posiedzeniu w dniu 13 lipca 2005 r., które zwołano po bombowych atakach terrorystycznych w Londynie, potwierdziły znaczenie przyjęcia właściwego instrumentu prawnego w tej kwestii.

- **Obowiązujące przepisy w dziedzinie, której dotyczy wniosek**

Artykuły 6 i 9 dyrektywy 2002/58/WE o prywatności i łączności elektronicznej ujednolicają przepisy dotyczące ochrony danych osobowych odnoszące się do przetwarzania danych o ruchu i lokalizacji powstałych w wyniku korzystania z usług łączności elektronicznej. Dane tego typu muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu, z wyjątkiem danych niezbędnych w celu naliczania opłat i rozliczeń międzyoperatorskich; niektóre dane - za zgodą abonenta - mogą być też przetwarzane w celach marketingowych i świadczenia usług stanowiących wartość dodaną. Artykuł 15 ust. 1 stanowi, że Państwa Członkowskie mogą przyjąć ograniczenia przewidziane (między innymi) w art. 5, 6 i 9, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia zachowanie bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw.

- **Spójność z innymi politykami i celami Unii**

Niniejszy wniosek jest zgodny z prawem wspólnotowym oraz Kartą Praw Podstawowych. Pomimo niewątpliwego wpływu, jaki proponowana dyrektywa będzie miała na prawo obywateli do prywatności gwarantowane na mocy art. 7 Karty czy też na prawo do ochrony danych osobowych gwarantowane na mocy art. 8 Karty, sprzeczność z wymienionymi prawami jest uzasadniona w myśl art. 52 tejże Karty. Ograniczenia wspomnianych praw wprowadzane przez niniejszy wniosek są proporcjonalne i niezbędne do osiągnięcia ogólnie uznanych celów, jakimi są zapobieganie i zwalczanie przestępczości i terroryzmu.

Wniosek ogranicza ponadto wpływ proponowanych przepisów na życie prywatne obywateli: po pierwsze poprzez jasne określenie celu, dla którego zatrzymywane dane mogą być wykorzystane, po drugie poprzez ograniczenie kategorii danych, które mają być zatrzymywane, i po trzecie poprzez ograniczenie czasu ich zatrzymywania. Dodatkowym środkiem zabezpieczającym jest to, że dyrektywa nie odnosi się do treści komunikató, co równałoby się to przejmowaniu treści komunikató, a to nie mieści się w granicach omawianego instrumentu prawnego.

Zgodnie z przepisami dyrektywy przetwarzanie danych osobowych zatrzymywanych przez dostawców usług i sieci podlegać będzie ogólnym i szczegółowym przepisom dotyczącym ochrony danych, ustalonym na mocy dyrektyw 95/46/WE oraz 2002/58/WE, co w praktyce oznacza, że nie ma potrzeby opracowywania szczególnych przepisów dodatkowych w sprawie ogólnych zasad ochrony i

bezpieczeństwa danych. Oznacza to także, że przetwarzanie tego rodzaju danych będzie w całości podlegało władzy nadzorczej organów ochrony danych powołanych we wszystkich Państwach Członkowskich.

2. KONSULTACJE Z ZAINTERESOWANYMI STRONAMI ORAZ OCENA WPŁYWU

• Konsultacje z zainteresowanymi stronami

Metody konsultacji, główne sektory objęte konsultacjami i ogólny profil respondentów

Począwszy od spotkań w 2001 r. w ramach Forum na temat Przestępczości Internetowej (*Cybercrime Forum*) zagadnienie zatrzymywania danych o ruchu było przedmiotem konsultacji z przedstawicielami organów ścigania, branży łączności elektronicznej oraz ekspertów do spraw ochrony danych.

W dniu 14 czerwca 2004 r. pod auspicjami Forum na rzecz Zapobiegania Przestępczości Zorganizowanej zorganizowane zostało spotkanie *ad hoc* okrągłego stołu, w którym wzięli udział przedstawiciele organów ścigania, branży łączności elektronicznej i organizacji ochrony danych. Po DG INSFO i DG JLS wydały w dniu 30 lipca 2004 r. wspólny dokument konsultacyjny na temat zatrzymywania danych o ruchu w ramach przygotowań do otwartych warsztatów poświęconych temu zagadnieniu, które odbyły się w dniu 21 września 2004 r. W odpowiedzi na wspólny dokument konsultacyjny nadeszły uwagi i wnioski od różnych stron, zwłaszcza od branży i stowarzyszeń do spraw swobód obywatelskich. Wspomniane otwarte warsztaty z dnia 21 września dostarczyły Komisji dalszych materiałów.

Przygotowując swój wniosek Komisja zainicjowała zakrojoną na szeroką skalę otwartą debatę w tej kwestii, która obejmowała dyskusje na plenum Parlamentu Europejskiego.

Streszczenie odpowiedzi oraz sposób, w jaki zostały one uwzględniane

Konsultacje potwierdziły, że zatrzymywanie danych o ruchu na temat połączenia stanowi dla organów ścigania istotne narzędzie przeciwdziałania i zwalczania przestępczości i terroryzmu. Przedstawiciele organów ścigania oświadczyli, że dla ich celów okresy zatrzymywania danych powinny być tak długie, jak to będzie niezbędne i zawierać tak wiele danych, jak to będzie niezbędne. Szczególnie w przypadkach złożonych śledztw dotyczących poważnych przestępstw, których zakończenie może trwać wiele lat, nadal regularnie wykorzystuje się stare dane o ruchu. Istnieją liczne przykłady na to, jak istotne są tego typu dane dla dochodzeń w sprawach karnych, zwłaszcza w przestępstwach związanych z atakami bombowymi i morderstwami.

Przedstawiciele europejskich stowarzyszeń branży telekomunikacyjnej i internetowej oraz pojedyncze przedsiębiorstwa działające w dziedzinie łączności elektronicznej deklarowały wolę dalszej współpracy z organami ścigania wysuwając jednocześnie kwestię znacznych kosztów związanych z długotrwałym zatrzymywaniem danych oraz sugerując, że zachowywanie danych byłoby wystarczające. Postulowały w każdym razie wprowadzenie okresów zatrzymywania danych nie dłuższych niż sześć

miesiący, jako że i tak większość danych potrzebnych organom ścigania nie wykracza poza okres sześciu miesięcy, oraz mechanizmów rekompensujących powstałe w związku z tym dodatkowe koszty.

Przedstawiciele organów ochrony danych i stowarzyszeń do spraw swobód obywatelskich wysunęli wniosek, że zatrzymywanie danych ingeruje w prywatne życie obywateli i dlatego okresy zatrzymywania danych powinny być możliwie najkrótsze. Ogólnie rzecz biorąc, kwestionowali oni proporcjonalność wymogu zatrzymywania danych przez okres ponad sześciu miesięcy. Wyraziły także obawy dotyczące celów i powodów zatrzymywania danych, które powinny zostać jasno określone.

Niniejszy wniosek stanowi podejście kompromisowe i opiera się na załączonej ocenie wpływu. Roczne okresy zatrzymywania danych o ruchu połączeń za pośrednictwem telefonii komórkowej i stacjonarnej oraz sześciomiesięczne dla danych o ruchu połączeń internetowych zaspokoją główne potrzeby organów ścigania, ograniczając jednocześnie wynikające stąd koszty dla branży oraz ingerencję w prywatne życie obywateli. Sześciomiesięczny okres zatrzymywania wszystkich danych byłby zbyt krótki, gdyż nawet, jeśli większa część wniosków od organów ścigania dotyczy danych, pochodzących z okresu nie dłuższego niż sześć miesięcy, w przypadku najpoważniejszych przestępstw, takich jak terroryzm, przestępczość zorganizowana czy ludobójstwo niezbędne są dane starsze niż sześć miesięcy.

- **Gromadzenie i wykorzystanie wiedzy fachowej**

Nie zaistniała potrzeba skorzystania z wiedzy specjalistycznej pochodzącej ze źródeł zewnętrznych.

- **Ocena wpływu**

Rozważane były różne możliwości. W 2002 r. Rada wyraźnie wezwała do dialogu na poziomie krajowym i unijnym zmierzającego do rozwiązania kwestii zatrzymywania danych o ruchu, które spełniałyby potrzebę zapewnienia zarówno skutecznych narzędzi zapobiegania, dochodzenia, wykrywania oraz karania przestępstw, jak i ochrony podstawowych praw i wolności osób fizycznych, zwłaszcza ich prawa do prywatności, ochrony danych i tajemnicy korespondencji. Zorganizowanie szeroko zakrojonej publicznej konsultacji i debaty w tej kwestii, w tym dyskusji na plenum Parlamentu Europejskiego, nie doprowadziło to jednak do osiągnięcia żadnych wspólnych rozwiązań.

Wstrzymanie się od podjęcia inicjatywy w kwestii zatrzymywania danych oznaczałoby utrzymanie nieładu panującego obecnie wśród przepisów dotyczących zatrzymywania danych. Instrumenty prawa współregulacji i samoregulacji zostały zniesione, jako że nie zapewniały wysokiego poziomu pewności prawnej. Inicjatywa ze strony trzeciego filaru dotycząca obowiązków w zakresie zatrzymywania danych została odrzucona jako niezgodna z istniejącym prawem wspólnotowym. Do opracowania koncepcji prawnej nawoływała także Rada Europejska w swojej deklaracji o zwalczaniu terroryzmu.

Opcja wniosku dotyczącego dyrektywy zapewnia wymagany dla wspólnego rynku poziom ujednoczenia. W porównaniu do rozporządzenia, pozostawia ona Państwom Członkowskim pewien margines swobody w zakresie wdrażania przepisów w kwestiach drażliwych. Rozporządzenie byłoby środkiem zbyt kategorycznym, zwłaszcza mając na względzie różne rozwiązania techniczne stosowane przez poszczególnych operatorów w różnych krajach. Dyrektywa zostawia Państwom Członkowskim wystarczająco duży margines swobody do tego, by mogły się one przystosować do wewnętrznych ograniczeń. W każdym razie aktualny stan rzeczy nie może trwać dalej z uwagi na przeszkodę, jakie rozbieżne przepisy krajowe w tej dziedzinie stanowią dla swobodnego świadczenia usług. Wybór instrumentu prawnego oraz szczególnej podstawy prawnej w postaci art. 95 WE zostały także dokonane dzięki analizie prawnej przedstawionej w dokumencie roboczym służb Komisji SEC(2005) 420 z dnia 22 marca 2005 r. Komisja przeprowadziła ocenę wpływu, z której sprawozdanie można znaleźć:

http://europa.eu.int/comm/dgs/justice_home/evaluation/dg_coordination_evaluation_annexe_en.htm.

3. PRAWNE ELEMENTY WNIOSKU

• **Streszczenie proponowanych działań**

Proponowana dyrektywa ma ujednoczyć obowiązki dostawców ogólnie dostępnych usług łączności elektronicznej oraz publicznej sieci łączności w zakresie zatrzymywania pewnych danych o ruchu, aby dane te mogły być dostępne dla właściwych organów Państw Członkowskich w celu zapobiegania, dochodzenia, wykrywania i karania poważnych przestępstw takich jak terroryzm i przestępczość zorganizowana.

• **Podstawa prawna**

Artykuł 95 Traktatu WE.

• **Zasada pomocniczości**

Zasada pomocniczości ma zastosowanie, o ile wniosek nie mieści się w ramach wyłącznych kompetencji Wspólnoty.

Istnieją przyczyny, dla których cele wniosku nie mogą być w sposób wystarczający realizowane przez Państwa Członkowskie.

Same Państwa Członkowskie nie mogą doprowadzić do ujednoczenia okresów zatrzymywania danych o ruchu. Działanie UE – podjęte na wezwanie Rady Europejskiej – spowoduje, że dane o ruchu będą zatrzymywane w całej Unii Europejskiej oraz udostępniane organom ścigania.

Z uwagi na to, że skuteczność dochodzeń w sprawach naruszenia prawa zależy w dużym stopniu od współpracy międzynarodowej, a różne podejścia na płaszczyźnie krajowej mają negatywny wpływ na rynek łączności elektronicznej, ogólnoeuropejska harmonizacja reguł zatrzymywania danych o ruchu stanowi

najtrafniejsze rozwiązanie polityczne. Zasada zwrotu kosztów pozwoli na stworzenie równych reguł gry na rynku wewnętrznym dla dostawców łączności elektronicznej.

Istnieją przyczyny, dla których działanie Wspólnoty umożliwi lepszą realizację celów wniosku.

Działanie UE przyczyni się do lepszego osiągnięcia celów wniosku gdyż spowoduje, że dane o ruchu będą zatrzymywane w całej Unii Europejskiej oraz udostępniane organom ścigania. Będzie ono także z korzyścią dla branży łączności elektronicznej, a zwłaszcza przedsiębiorstw świadczących usługi na terenie kilku różnych Państw Członkowskich, gdyż pozwoli im na znormalizowanie technologii.

Do wskaźników jakościowych, z których wynika, że cele mogą zostać lepiej osiągnięte przez Unię, należy skuteczność organów ścigania w dziedzinie zapobiegania i zwalczania przestępczości i terroryzmu, zwłaszcza jeśli chodzi o przestępczość zorganizowaną i terroryzm, które mają często charakter międzynarodowy.

Niniejszy wniosek ogranicza się wyłącznie do tych tego, czego Państwa Członkowskie nie mogą w sposób satysfakcjonujący osiągnąć, a co Unia robi lepiej ograniczenie zakresu do dostawców usług łączności elektronicznej oraz publicznej sieci komunikacyjnej. Wniosek pozostawia w gestii Państw Członkowskich wybór co do tego, które organy miałyby dostęp do zatrzymywanych danych i na jakich warunkach. Dostęp i wymiana informacji pomiędzy właściwymi organami ścigania jest kwestią pozostającą poza zakresem postanowień Traktatu WE.

Dlatego warto wspomnieć w tym miejscu, że Komisja jest aktualnie w trakcie przygotowywania projektów wniosków legislacyjnych w oparciu o postanowienia Traktatu o Unii Europejskiej odnoszących się do zasady dostępności informacji w celach egzekwowania prawa oraz ustalenia zasad ochrony danych na użytek trzeciego filaru. Należy ponadto odnotować, że w myśl wspomnianej dyrektywy dostęp do „zatrzymywanych danych” będzie przysługiwał jedynie organom ścigania, a zatem nie będą go mieć dostawcy usług łączności elektronicznej.

Wniosek jest zatem zgodny z zasadą pomocniczości.

- **Zasada proporcjonalności**

Wniosek jest zgodny z zasadą proporcjonalności, jako że jego wpływ na obywateli i branżę łączności elektronicznej został ograniczony do minimum. Należy jeszcze raz przypomnieć, że omawiany instrument odnosi się wyłącznie do danych o ruchu, które są przetwarzane przez dostawców usług łączności elektronicznej. Treść komunikatów połączeń elektronicznych jest wyłączona z zakresu niniejszej dyrektywy.

Podstawową przesłanką poszukiwania właściwego kompromisu pomiędzy wszystkimi wchodzącymi w grę interesami związanymi ze sprawami społecznymi, gospodarką, bezpieczeństwem i prywatnością było i jest poszanowanie podstawowych praw i wolności, a w szczególności prawa do życia i ścisłego ograniczenia ingerencji w sferę prywatną.

Stąd też we wniosku dotyczącym dyrektywy wzięto pod uwagę kwestie proporcjonalności, zwłaszcza w odniesieniu do długości proponowanych okresów zatrzymywania, rozróżnienie pomiędzy danymi telefonicznymi i internetowymi, ograniczenia kategorii danych, które mają być zatrzymywane oraz programu zwrotu kosztów. Niniejszy wniosek ściśle ogranicza cele, w jakich zatrzymywane dane mogą zostać udostępnione organom ścigania prawa. Zatrzymywane dane są w pełni objęte przepisami prawodawstwa dotyczącego ochrony danych, natomiast wpływ na prawa osób fizycznych i podmiotów gospodarczych jest ograniczony poprzez wybór ograniczonego zestawu danych o ruchu przeznaczonych do zatrzymywania. Ponadto krótsze okresy przetrzymywania danych o ruchu generowanych w wyniku korzystania z Internetu, w przeciwieństwie do danych o ruchu generowanych w wyniku korzystania z „tradycyjnej” telefonii komórkowej lub stacjonarnej, biorą pod uwagę aktualne praktyki gospodarcze, zmniejszając znaczenie objętość danych, które mają być zatrzymywane.

Ciężar finansowy i administracyjny spadający na rządy krajowe, podmioty gospodarcze i obywatele został ograniczony na szereg sposobów. Dyrektywa przewiduje po pierwsze ujednoczenie przepisów, co oznacza zmniejszenie kosztów związanych z zapewnieniem zgodności z przepisami tej dyrektywy dla dostawców usług łączności elektronicznej czy publicznej sieci komunikacyjnej. Po drugie poprzez ściśle ograniczenie długości okresów zatrzymywania danych oraz zakresu danych objętych zatrzymywaniem zapewniona została minimalizacja kosztów. Zważywszy na znaczenie omawianego środka dla zapobiegania i zwalczania przestępczości i terroryzmu, dodatkowe koszty wynikające z tytułu świadczenia zwrotu kosztów dla Państw Członkowskich uznaje się za proporcjonalne (patrz ocena wpływu).

Należy także podkreślić, że niniejsza dyrektywa nie odrzuca możliwości zażądania przez Państwa Członkowskie wprowadzenia szczególnych środków zachowywania danych na przykład w przypadku, gdy organizacja przestępcza lub podejrzana o działalność przestępczą została wcześniej zidentyfikowana lub w przypadku szczególnych zdarzeń, takich jak ataki terrorystyczne.

- **Wybór instrumentów prawnych**

Proponowane instrumenty: dyrektywa.

Istnieją powody, dla których inne środki nie byłyby odpowiednie.

Zagadnienie odpowiedniej podstawy prawnej dla wniosku dotyczącego zatrzymywania danych o ruchu zostało ostatnio rozpatrzone w dokumencie roboczym służb Komisji. W skrócie, według stanowiska przedstawionego we wspomnianym dokumencie, zagadnienia zatrzymywania danych o ruchu zostały już uwzględnione w poprzednich instrumentach prawnych opartych na podstawie prawnej pierwszego filaru, takich jak wspomniane wyżej dyrektywy 2002/58/WE oraz 95/46/WE. W analizie stwierdza się dalej, że jedynie z uwagi na brak osiągnięcia politycznego porozumienia w kwestii rzeczywistej długości okresu zatrzymywania danych, omawiane zagadnienie nie zostało pełniej ujednoczone w dyrektywie 2002/58/WE i w związku z tym każdy następny instrument prawny odnoszący się do zatrzymywania danych o ruchu jako takiego (w przeciwieństwie do przepisu regulującego wymianę i dostęp do tego typu danych przez organy ścigania)

musi także uwzględniać podstawę prawną pierwszego filaru. Zasada ta jest zgodna z przepisami art. 47 Traktatu o Unii Europejskiej, który reguluje kwestię związku pomiędzy Traktatem o Unii Europejskiej i Traktatem WE, stanowiąc, że żaden instrument prawny przyjęty w myśl Traktatu o Unii Europejskiej nie może wpłynąć na rami prawne przyjęte na mocy Traktatu WE.

4. NASTĘPSTWA BUDŻETOWE

Wniosek nie ma żadnych konsekwencji finansowych dla budżetu Wspólnoty.

5. INFORMACJE DODATKOWE

- **Klauzula przeglądu/weryfikacji/wygaśnięcia**

Wniosek zawiera klauzulę przeglądu. W celu wsparcia Komisji w przy wypełnianiu przez nią zadań w zakresie przeglądu przewiduje się stworzenie zespołu do spraw zatrzymywania danych. Grupa ta składałaby się z ekspertów w dziedzinie techniki łączności elektronicznej oraz przedstawicieli organów ścigania i organów do spraw ochrony danych.

- **Tabela korelacji**

Państwa Członkowskie są zobowiązane do przekazania Komisji tekstu przepisów krajowych, na mocy których dokonuje się transpozycji dyrektywę, jak również tabeli korelacji między tymi przepisami a dyrektywą.

Wniosek dotyczący

DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie zatrzymywania przetwarzanych danych w związku ze świadczeniem publicznych usług łączności elektronicznej (2002 r.), zmieniająca dyrektywę 2002/58/WE

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 95,

uwzględniając wniosek Komisji¹,

uwzględniając opinię Europejskiego Komitetu Społeczno-Ekonomicznego²,

uwzględniając opinię Komitetu Regionów³,

stanowiąc zgodnie z procedurą określoną w art. 251 Traktatu,

a także mając na uwadze, co następuje:

- (1) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych⁴ wymaga od Państw Członkowskich zapewnienia osobom fizycznym praw i wolności w zakresie przetwarzania danych osobowych, w szczególności prawa do prywatności, w celu zapewnienia swobodnego przepływu danych osobowych we Wspólnocie;
- (2) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej⁵ przekłada zasady ustanowione w dyrektywie 95/46/WE na zasady szczególne dla sektora łączności elektronicznej;
- (3) Artykuły 5, 6, i 9 dyrektywy 2002/58/WE ustalają zasady odnoszące się do przetwarzania danych o ruchu i lokalizacji generowanych w wyniku korzystania z usług łączności elektronicznej przez dostawców sieci i usług. Wspomniane dane muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu z wyjątkiem danych niezbędnych do naliczania opłat i rozliczeń międzyoperatorskich; niektóre dane - za zgodą abonenta - mogą być też przetwarzane w celach marketingowych i świadczenia usług stanowiących wartość dodaną;

¹ Dz.U. C [...] z [...], str. [...].

² Dz.U. C [...] z [...], str. [...].

³ Dz.U. C [...] z [...], str. [...].

⁴ Dz.U. L 281 z 23.11.1995, str. 31.

⁵ Dz.U. L 201 z 30.7.2002, str. 37.

- (4) Artykuł 15 ust. 1 dyrektywy 2002/58/WE określa warunki, w jakich Państwa Członkowskie mogą ograniczyć zakres praw i obowiązków gwarantowanych przepisami art. 5, art. 6, art. 8 ust. 1, 2, 3 i 4 oraz art. 9 przedmiotowej dyrektywy; wszelkie tego typu odstępstwa muszą być niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego dla celów porządku publicznego, tj., zachowania bezpieczeństwa narodowego (tj. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego czy też zapobiegania, dochodzenia, wykrywania i karania przestępstw lub nielegalnego wykorzystania systemów łączności elektronicznej;
- (5) Kilka Państw Członkowskich przyjęło ustawy przewidujące zatrzymywanie danych przez usługodawców w celu zapobiegania, dochodzenia, wykrywania i karania przestępstw; przepisy poszczególnych ustawodawstw krajowych znacznie od siebie odbiegają;
- (6) Prawne i techniczne różnice pomiędzy przepisami krajowymi w zakresie zatrzymywania danych w celu zapobiegania, dochodzenia, wykrywania i karania przestępstw stanowią przeszkodę dla wewnętrznego rynku łączności elektronicznej; usługodawcy napotykają na różne wymogi odnośnie do rodzajów danych o ruchu, które mają być zatrzymywane, oraz warunków i okresów zatrzymywania;
- (7) W swoich wnioskach z posiedzenia, które odbyło się w dniu 20 września 2001 r., Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych wzywa do zapewnienia organom ścigania możliwości prowadzenia śledztw w sprawach kryminalnych, które obejmują korzystanie z łączności elektronicznej oraz podjęcia środków prawnych przeciwko osobom popełniającym te przestępstwa, zachowując jednocześnie równowagę pomiędzy ochroną danych osobowych, a potrzebą uzyskania dostępu do danych w celach prowadzenia śledztw kryminalnych przez organy ścigania;
- (8) We wnioskach z posiedzenia Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych z dnia 19 grudnia 2002 r. podkreślono, że z uwagi na znaczny wzrost możliwości, jakie daje łączność elektroniczna, dane odnoszące się do korzystania z łączności elektronicznej są szczególnie ważne, a co za tym idzie, stanowią istotne narzędzie służące zapobieganiu, dochodzeniu, wykrywaniu oraz karaniu przestępczości i przestępstw, zwłaszcza z zakresu przestępczości zorganizowanej;
- (9) Przyjęta w dniu 25 marca 2005 r. przez Radę Europejską deklaracja w sprawie zwalczania terroryzmu zaleca Radzie zbadanie środków przyjęcia przepisów w sprawie zatrzymywania przez usługodawców danych o ruchu połączeń;
- (10) Deklaracja przyjęta na specjalnym nieformalnym posiedzeniu Rady w dniu 13 lipca 2005 r. jeszcze raz podkreśla potrzebę możliwie szybkiego przyjęcia środków odnoszących się do zatrzymywania danych o ruchu połączeń;
- (11) Zważywszy na znaczenie, jakie dane o ruchu mają w zapobieganiu, dochodzeniu, wykrywaniu i ściganiu poważnych przestępstw, takich jak działalność terrorystyczna i przestępczość zorganizowana, istnieje - jak to wykazały badania i doświadczenia kilku Państw Członkowskich, - potrzeba zatrzymywania przez pewien czas danych przetwarzanych przez dostawców łączności elektronicznej podczas świadczenia publicznych usług łączności elektronicznej lub udostępniających publicznej sieci łączności;

- (12) Kategorie informacji, które mają być zatrzymywane, odzwierciedlają właściwą równowagę pomiędzy korzyściami z punktu widzenia zapobiegania, dochodzenia, wykrywania i karania poważnych przestępstw, a poziomem ingerencji w sferę prywatną, jaką spowodują. Obowiązujący roczny (lub sześciomiesięczny w przypadku odnoszących się do łączności elektronicznych, które odbywają się wyłącznie za pośrednictwem protokołu internetowego) okres zatrzymywania danych, także stanowi właściwy kompromis pomiędzy interesami wszystkich zainteresowanych stron.
- (13) Z uwagi na fakt, że zatrzymywanie danych powoduje znaczne dodatkowe koszty dla dostawców łączności elektronicznej, podczas gdy korzyści w sensie bezpieczeństwa publicznego mają znaczenie dla ogółu społeczeństwa, należy przewidzieć mechanizm zwrotu kosztów wykazanych przez Państwa Członkowskie, powstałych na skutek spełniania wymogów nałożonych na nie niniejszą dyrektywą;
- (14) Technologie mające znaczenie dla łączności elektronicznej ulegają szybkiemu rozwojowi i dlatego uzasadnione wymogi właściwych organów także mogą ulec zmianie; w celu uzyskania opinii na temat tych zagadnień Komisja pragnie stworzyć zespół składający się z przedstawicieli organów ścigania, przedstawicieli branży łączności elektronicznej oraz organów ochrony danych;
- (15) Należy także przypomnieć, że przepisy dyrektywy 95/46/WE oraz dyrektywy 2002/58/WE w pełni odnoszą się do danych zatrzymywanych zgodnie z niniejszą dyrektywą; art. 30 ust. 1 lit. c) mówi o wymogu przeprowadzania konsultacji z „grupą roboczą art. 29”.
- (16) Bardzo istotne jest, aby Państwa Członkowskie przewidziały środki prawne, które zapewnią udostępnianie danych zatrzymywanych w myśl niniejszej dyrektywy jedynie właściwym organom krajowym zgodnie z krajowym ustawodawstwem przy pełnym poszanowaniu praw podstawowych zainteresowanych osób; takie środki przewidują w szczególności odpowiednie warunki, ograniczenia i zabezpieczenia, tak by przekazywanie zatrzymywanych danych było zgodne z prawami podstawowymi gwarantowanymi zwłaszcza na mocy postanowień Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności;
- (17) Środki niezbędne do wdrożenia niniejszej dyrektywy należy przyjąć zgodnie z decyzją Rady 1999/468/WE z dnia 28 czerwca 1999 r. ustanawiającą warunki wykonywania uprawnień wykonawczych przyznanych Komisji⁶;
- (18) Cele planowanego działania, mianowicie ujednoczenie obowiązków spoczywających na dostawcach odnośnie do zatrzymywania pewnych danych oraz zapewnienia dostępu do tych danych w celu zapobiegania, dochodzenia, wykrywania i karania poważnych przestępstw, takich jak działalność terrorystyczna i przestępczość zorganizowana, nie mogą zostać osiągnięte w wystarczający sposób przez Państwa Członkowskie, mogą natomiast, z uwagi na zasięg i efekty działań zostać lepiej osiągnięte na poziomie wspólnotowym. Stąd też Wspólnota może przyjąć środki w zgodzie z zasadą pomocniczości, zapisaną w art. 5 Traktatu. Stosownie do zasady proporcjonalności, określonej w tym samym artykule, zakres niniejszej dyrektywy nie wykracza poza to, co jest konieczne dla osiągnięcia powyższych celów;

⁶ Dz.U. L 184 z 17.7.1999, str. 23.

- (19) Niniejsza dyrektywa respektuje prawa podstawowe i przestrzega zasad uznanych w szczególności w Karcie Praw Podstawowych Unii Europejskiej; niniejsza dyrektywa wraz z dyrektywą 2002/58/WE mają na celu zwłaszcza zagwarantowanie pełnego przestrzegania praw podstawowych w zakresie poszanowania prywatności życia i komunikacji obywateli oraz ochrony danych osobowych (art. 7 i 8 Karty),

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

Artykuł 1

Przedmiot i zakres

1. Celem niniejszej dyrektywy jest ujednoczenie przepisów Państw Członkowskich w zakresie obowiązków dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznej sieci łączności w zakresie przetwarzania i zatrzymywania pewnych danych o ruchu, aby zapewnić dostępność przedmiotowych danych do celu zapobiegania, dochodzenia, wykrywania i karania poważnych przestępstw, takich jak terroryzm i przestępczość zorganizowana.
2. Niniejsza dyrektywa odnosi 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.

Artykuł 2

Definicje

1. Dla celów niniejszej dyrektywy stosuje się definicje z dyrektywy 95/46/WE, dyrektywy 2002/21/WE⁷ oraz dyrektywy 2002/58/WE.
2. Dla celów niniejszej dyrektywy:
 - a) „dane” oznacza dane o ruchu i lokalizacji oraz powiązane dane niezbędne do identyfikacji abonenta lub zarejestrowanego użytkownika;
 - b) „użytkownik” oznacza każdą osobę fizyczną korzystającą z ogólnie dostępnych usług łączności elektronicznej do celów prywatnych lub handlowych, niekoniecznie na podstawie abonamentu na te usługi.

Artykuł 3

Obowiązek zatrzymywania danych

1. Na zasadzie odstępstwa od art. 5, 6 i 9 dyrektywy 2002/58/WE, Państwa Członkowskie przyjmują środki w celu zapewnienia, że dane generowane lub przetwarzane na ich terenie przez dostawców ogólnie dostępnych usług łączności

⁷ Dz.U. L 108 z 24.4.2002, str. 33.

elektronicznej lub publicznej sieci łączności w trakcie świadczenia usług komunikacyjnych są zatrzymywane zgodnie z przepisami niniejszej dyrektywy.

2. Państwa Członkowskie przyjmują środki w celu zapewnienia, że dane zatrzymywane w myśl niniejszej dyrektywy są udostępniane jedynie właściwym organom krajowym, w szczególnych przypadkach i zgodnie z krajowym ustawodawstwem w celu zapobiegania, dochodzenia, wykrywania i karania poważnych przestępstw, takich jak terroryzm i przestępczość zorganizowana.

Artykuł 4

Kategorie danych przeznaczonych do zatrzymywania

Państwa Członkowskie zapewniają zatrzymywanie następujących kategorii danych zgodnie z postanowieniami niniejszej dyrektywy:

- (a) dane niezbędne do ustalenia źródła połączenia;
- (b) dane niezbędne do ustalenia odbiorcy połączenia;
- (c) dane niezbędne do określenia daty, godziny i czasu trwania połączenia;
- (d) dane niezbędne do określenia rodzaju połączenia;
- (e) dane niezbędne do określenia narzędzia komunikacji lub tego, co może służyć za narzędzie komunikacji;
- (f) dane niezbędne do identyfikacji lokalizacji urządzenia komunikacji ruchomej.

Rodzaje danych przeznaczonych do zatrzymywania w ramach wyżej wymienionych kategorii zostały wyszczególnione w załączniku.

Artykuł 5

Weryfikacja załącznika

Załącznik jest weryfikowany regularnie, tak często jak to jest niezbędne, zgodnie z procedurą, o której mowa w art. 6 ust. 2.

Artykuł 6

Komitet

1. Komisja wspierana jest przez komitet składający się z przedstawicieli Państw Członkowskich, na którego czele stoi przedstawiciel Komisji.
2. W każdym przypadku, gdy dokonywane jest odniesienie do niniejszego ustępu, stosuje się art. 5 i 7 decyzji 1999/468/WE, uwzględniając przepisy jej art. 8.
3. Okres ustanowiony w art. 5 ust. 6 decyzji 1999/468/WE wynosi trzy miesiące.

Artykuł 7
Okresy zatrzymywania

Państwa Członkowskie zapewniają, że wymienione w art. 4 kategorie danych są zatrzymywane na okres jednego roku od daty połączenia, z wyjątkiem danych odnoszących się do łączności elektronicznych, które odbywają się w całości lub w przeważającej części za pośrednictwem protokołu internetowego. Te ostatnie są zatrzymywane przez okres sześciu miesięcy.

Artykuł 8
Wymogi dotyczące zatrzymywania danych

Państwa Członkowskie zapewniają zatrzymywanie danych zgodnie z przepisami niniejszej dyrektywy, w sposób umożliwiający przekazanie bez niepotrzebnej zwłoki zatrzymywanych danych i wszelkich informacji odnoszących się do takich danych właściwym organom na ich wnioski.

Artykuł 9
Statystyka

Państwa Członkowskie zapewniają dostarczanie Komisji Europejskiej corocznych statystyk na temat zatrzymywania danych przetwarzanych w ramach świadczenia publicznych usług łączności elektronicznej. Statystyki takie obejmują:

- przypadki, w których właściwym organom udzielone zostały informacje zgodnie z odpowiednim prawem krajowym,
- czas, jaki upłynął między datą zarejestrowania zatrzymywanych danych, a datą wniosku o przekazanie danych złożonego przez właściwy organ;
- przypadki, w których wnioski o dane nie mogły zostać zrealizowane.

Statystyki tego rodzaju nie zawierają danych osobowych.

Artykuł 10
Koszty

Państwa Członkowskie zapewnią dostawcom ogólnie dostępnych usług łączności elektronicznej lub publicznej sieci łączności zwrot wykazanych dodatkowych kosztów powstałych na skutek spełniania wymogów nałożonych na nie niniejszą dyrektywą.

Artykuł 11
Zmiana dyrektywy 2002/58/WE

W art. 15 dyrektywy 2002/58/WE dodaje się ust. 1a w brzmieniu:

„1a. Ustęp 1 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 2005/./WE. * * Dz.U. L ... z dnia ..”.

Artykuł 12

Ocena

1. Nie później niż trzy lata od daty, o której mowa w art. 13 ust. 1 Komisja przedstawia Parlamentowi Europejskiemu i Radzie ocenę wdrożenia niniejszej dyrektywy i jej wpływu na podmioty gospodarcze i konsumentów, uwzględniając dane statystyczne dostarczone Komisji zgodnie z art. 9 w celu określenia ewentualnej potrzeby zmiany przepisów niniejszej dyrektywy zwłaszcza w odniesieniu do okresu zatrzymywania ustalonego na mocy art. 7.
2. W tym celu Komisja bada wszystkie uwagi wniesione przez Państwa Członkowskie lub grupę roboczą ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołaną na mocy art. 29 dyrektywy 95/46/WE.

Artykuł 13

Transpozycja

1. Państwa Członkowskie wprowadzają w życie przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy [najpóźniej w terminie 15 miesięcy od jej przyjęcia]. Państwa Członkowskie przekazują niezwłocznie Komisji tekst przepisów oraz tabelę korelacji między tymi przepisami a niniejszą dyrektywą.

Przepisy przyjęte przez Państwa Członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia określane są przez Państwa Członkowskie.

2. Państwa Członkowskie przedstawiają Komisji teksty głównych przepisów prawa krajowego, które przyjmą w dziedzinie objętej niniejszą dyrektywą.

Artykuł 14

Wejście w życie

Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 15

Adresaci

Niniejsza dyrektywa skierowana jest do Państw Członkowskich.

Sporządzono w Brukseli, dnia

*W imieniu Parlamentu Europejskiego
Przewodniczący*

*W imieniu Rady
Przewodniczący*

ZAŁĄCZNIK

Rodzaje danych przeznaczonych do zatrzymywania w kategoriach ustalonych na podstawie art. 4 niniejszej dyrektywy:

- a) Dane niezbędne do ustalenia źródła połączenia:
 - (1) W przypadku telefonii stacjonarnej:
 - (a) Numer nadawcy połączenia;
 - (b) Nazwisko i adres abonenta lub zarejestrowanego użytkownika;
 - (2) W przypadku telefonii komórkowej:
 - (a) Numer nadawcy połączenia;
 - (b) Nazwisko i adres abonenta lub zarejestrowanego użytkownika;
 - (3) W przypadku dostępu internetowego, elektronicznej poczty internetowej i telefonii internetowej:
 - (a) Adres IP, dynamiczny lub statyczny, przydzielony dla połączenia przez dostawcę dostępu internetowego;
 - (b) Identyfikator użytkownika (*user ID*) źródła połączenia;
 - (c) Etykieta połączenia lub numer telefonu przydzielony każdemu przychodzącemu połączeniu w sieci telefonii publicznej;
 - (d) Nazwisko i adres abonenta lub zarejestrowanego użytkownika, do którego w momencie połączenia należał adres IP, etykieta połączenia lub identyfikator użytkownika.

- b) Dane niezbędne do ustalenia odbiorcy połączenia:
 - (1) W przypadku telefonii stacjonarnej:
 - (a) Numer odbiorcy / numery odbiorców połączenia;
 - (b) Nazwisko(a) i adres(y) abonenta(ów) lub zarejestrowanego(ych) użytkownika(ów);
 - (2) W przypadku telefonii komórkowej:
 - (a) Numer odbiorcy / numery odbiorców połączenia;
 - (b) Nazwisko(-a) i adres(-y) abonenta(ów) lub zarejestrowanego(ych) użytkownika(ów);
 - (3) Dotyczy dostępu internetowego, elektronicznej poczty internetowej i telefonii internetowej:

- (a) Etykieta połączenia lub identyfikator użytkownika (*user ID*) planowanego odbiorcy połączenia;
 - (b) Nazwisko(-a) i adres(-y) abonenta(ów) lub zarejestrowanego(-ych) użytkownika(-ów), który jest (są) planowanym(-ymi) odbiorcą(-ami) połączenia.
- c) Dane niezbędne do określenia daty, godziny i czasu trwania połączenia:
 - (1) W przypadku telefonii stacjonarnej i telefonii komórkowej:
 - (a) Data i dokładny czas rozpoczęcia i zakończenia połączenia.
 - (2) W przypadku dostępu internetowego, elektronicznej poczty internetowej i telefonii internetowej:
 - (a) Data i godzina zalogowania i wylogowania sesji internetowej na podstawie danej strefy czasowej.
- d) Dane niezbędne do określenia rodzaju połączenia:
 - (1) W przypadku telefonii stacjonarnej:
 - (a) Wykorzystane usługi telefoniczne, np. połączenie głosowe, konferencyjne, faks i usługi przekazywania wiadomości.
 - (2) W przypadku telefonii komórkowej:
 - (a) Wykorzystane usługi telefoniczne, np. połączenie głosowe, konferencyjne, krótka wiadomość tekstowa (SMS), rozszerzone wiadomości tekstowe (EMS) lub wiadomości multimedialne (MMS).
- e) Dane niezbędne do identyfikacji urządzenia komunikacji lub co może służyć za takie urządzenie;
 - (1) W przypadku telefonii komórkowej:
 - (a) Międzynarodowy numer abonenta mobilnego (IMSI) strony dzwoniącej i strony do której się dzwoni;
 - (b) Międzynarodowy numer fabryczny mobilnego aparatu telefonicznego (IMEI) nadawcy i odbiorcy połączenia.
 - (2) W przypadku dostępu internetowego, elektronicznej poczty internetowej i telefonii internetowej:
 - (a) Numer telefonu przy dostępie za pośrednictwem dial-up;
 - (b) Identyfikator DSL lub inny identyfikator końcowy inicjatora połączenia;
 - (c) Adres MAC (sterowany dostęp do nośnika) lub inny maszynowy identyfikator inicjatora połączenia.

- f) Danie niezbędne do identyfikacji lokalizacji urządzenia komunikacji mobilnej:
- (1) Etykieta lokalizacji (identyfikator komórki) na początku i na końcu połączenia;
 - (2) Nakładanie danych między identyfikatorami komórki oraz ich geograficzna lokalizacja na początku i na końcu połączenia;