RADA UNII EUROPEJSKIEJ

Bruksela, 19 października 2004 r. (OR. en)

8958/04
EXT 1 (en,cs,et,lv,lt,hu,mt,pt,sl,sk)

CRIMORG 36
TELECOM 82

PISMO PRZEWODNIE

od:	Republika Francuska, Irlandia, Królestwo Szwecji i Zjednoczone Królestwo
data otrzymania:	28 kwietnia 2004 r.
do:	Pan Javier SOLANA, Sekretarz Generalny/Wysoki Przedstawiciel
Dotyczy:	Projekt decyzji ramowej w sprawie zabezpieczania danych przetwarzanych i przechowywanych w związku ze świadczeniem publicznie dostępnych usług komunikacji elektronicznej lub danych w publicznych sieciach komunikacyjnych w celu zapobiegania, dochodzenia, wykrywania i ścigania przestępczości i przestępstw kryminalnych, w tym terroryzmu

W załączeniu delegacje otrzymują inicjatywę Republiki Francuskiej, Irlandii, Królestwa Szwecji i Zjednoczonego Królestwa mającą na celu przyjęcie decyzji ramowej w sprawie zabezpieczania danych przetwarzanych i przechowywanych w związku ze świadczeniem publicznie dostępnych usług komunikacji elektronicznej lub danych w publicznych sieciach komunikacyjnych w celu zapobiegania, dochodzenia, wykrywania i ścigania przestępczości i przestępstw kryminalnych, w tym terroryzmu.

Projekt decyzji ramowej

w sprawie zabezpieczania danych przetwarzanych i przechowywanych w związku ze świadczeniem publicznie dostępnych usług komunikacji elektronicznej lub danych w publicznych sieciach komunikacyjnych w celu zapobiegania, dochodzenia, wykrywania i ścigania przestępczości i przestępstw kryminalnych, w tym terroryzmu.

RADA UNII EUROPEJSKIEJ

Uwzględniając Traktat o Unii Europejskiej, a w szczególności jego art. 31 ust. 1 lit. c) oraz art. 34 ust. 2 lit. b),

Uwzględniając inicjatywę Republiki Francuskiej, Irlandii, Królestwa Szwecji oraz Zjednoczonego Królestwa,

Uwzględniając opinię Parlamentu Europejskiego,

a także mając na uwadze, co następuje:

1. Dla zapewnienia wysokiego poziomu ochrony na obszarze wolności, bezpieczeństwa i sprawiedliwości, konieczne jest, by zapobieganie, dochodzenie, wykrywanie i ściganie przestępczości i przestępstw kryminalnych było prowadzone w sposób właściwy

2. Plan działania Rady i Komisji w sprawie optymalnych metod realizacji postanowień Traktatu Amsterdamskiego dotyczących ustanowienia obszaru wolności, bezpieczeństwa i sprawiedliwości, konkluzje Rady Europejskiej z Tampere w dniach 15-16 października 1999 r., Rady Europejskiej z Santa Maria de Feira w dniach 19-20 czerwca 2000 r., Komisja Europejska w swojej tablicy wyników oraz Parlament Europejski w rezolucji z dnia 19 maja 2000 r., wzywają do podjęcia interwencji w dziedzinie przestępczości w obszarze wysokich technologii.

3. W konkluzjach Rady z 20 września 2001 r. zawarto wezwanie do zadbania o to, by organy sprawiedliwości mogły prowadzić dochodzenia w sprawie czynów kryminalnych popełnionych przy użyciu systemów komunikacji elektronicznej oraz do podjęcia środków przeciwko sprawcom tych przestępstw, przy zachowaniu równowagi pomiędzy wymogami związanymi z ochroną danych osobowych a potrzebami organów sprawiedliwości w zakresie dostępu do danych na cele prowadzenia dochodzeń karnych. W konkluzjach Rady z 19 grudnia 2002 r. odnotowano, że ze względu na istotne poszerzenie zakresu możliwości oferowanych przez komunikację elektroniczną, informacje dotyczące wykorzystywania komunikacji elektronicznej stanowią obecnie szczególnie istotne i użyteczne narzędzie w zapobieganiu, dochodzeniu, wykrywaniu i ściganiu przestępczości i przestępstw kryminalnych, w szczególności przestępczości zorganizowanej i terroryzmu.

4. Deklaracja w sprawie zwalczania terroryzmu, przyjęta przez Radę Europejską w dniu 25 marca 2004 r., powierzyła Radzie zadanie zbadania środków, dzięki którym możliwe byłoby przyjęcie do czerwca 2005 r. przepisów w zakresie zabezpieczania przez dostawców usług danych o ruchu.

5. Na cele zapobiegania, dochodzenia, wykrywania i ścigania przestępstw i czynów kryminalnych z wykorzystaniem systemów komunikacji elektronicznej niezbędne jest zabezpieczenie danych generowanych wskutek wysłania komunikatu (nazywanych dalej „danymi”). Projekt dotyczy wyłącznie danych generowanych w wyniku wysłania komunikatu, nie dotyczy natomiast danych stanowiących treść przekazanego komunikatu. Zabezpieczenie danych jest w szczególności niezbędne dla wykrycia źródła nielegalnej treści, takiej jak pornografia dziecięcia czy materiały rasistowskie lub ksenofobiczne; źródła ataków skierowanych na systemy informatyczne oraz do identyfikacji osób wykorzystujących sieci komunikacji elektronicznej na cele przestępczości zorganizowanej i terroryzmu.

6. Zabezpieczenie określonych danych dotyczących konkretnych osób nie wystarcza w pewnych przypadkach dla spełnienia powyższych wymogów. W trakcie prowadzonych dochodzeń mogą wystąpić sytuacje, w których stwierdzenie jakie dane są potrzebne lub jakie osoby były zaangażowane będzie możliwe dopiero po upływie miesięcy lub lat po wysłaniu pierwotnego komunikatu. Dlatego niezbędne jest zabezpieczenie określonych rodzajów danych - które już obecnie są przetwarzane i przechowywane na cele rozliczeniowe, handlowe albo na inne cele zgodne z prawem - przez określony, dodatkowy okres czasu, ze względu na to, że mogą one okazać się potrzebne na cele dochodzeń karnych lub postępowań sądowych prowadzonych w przyszłości. Z tej przyczyny niniejsza decyzja ramowa dotyczy zabezpieczenia danych a nie ich zachowywania.

7. W uznaniu wagi, jaką ma potrzeba zabezpieczenia danych, art. 15 dyrektywy 2002/58/WE pozwala na przyjęcie środków legislacyjnych zezwalających, pod pewnymi warunkami, na zabezpieczenie danych na potrzeby zapobiegania, dochodzenia, wykrywania i ścigania przestępczości i przestępstw kryminalnych. Niniejsza decyzja ramowa nie dotyczy innych celów określonych w art. 15 wymienionej dyrektywy i dlatego nie ustanawia przepisów regulujących zabezpieczenie danych na potrzeby ochrony bezpieczeństwa narodowego (tj. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego. Nie dotyczy także niedozwolonego wykorzystywania systemu komunikacji elektronicznej, jeżeli nie stanowi ono przestępstwa kryminalnego.

8. Szereg Państw Członkowskich ustanowiło przepisy dotyczące zabezpieczenia danych *a priori,* na cele zapobiegania, dochodzenia, wykrywania i ścigania przestępczości i przestępstw kryminalnych. W innych Państwach Członkowskich prowadzone są natomiast prace w tej dziedzinie. Pomiędzy przepisami w tym zakresie przyjętymi w poszczególnych Państwach Członkowskich występują istotne różnice co do treści.

9. Różnice występujące w przepisach Państw Członkowskich mają negatywny wpływ na współpracę pomiędzy właściwymi władzami w zakresie zapobiegania, dochodzenia, wykrywania i ścigania przestępczości i przestępstw kryminalnych. Dlatego, dla zagwarantowania efektywnej współpracy policyjnej i sądowej w sprawach karnych niezbędne jest zapewnienie, że wszystkie Państwa Członkowskie podejmą środki niezbędne dla zabezpieczenia określonych rodzajów danych przez wyznaczony czas na cele zapobiegania, dochodzenia, wykrywania i ścigania przestępczości i przestępstw kryminalnych, w tym terroryzmu. Do tych danych powinny mieć dostęp pozostałe Państwa Członkowskie, zgodnie z instrumentami regulującymi współpracę sądową w sprawach karnych, przyjętymi na podstawie tytułu VI Traktatu o Unii Europejskiej. Dostęp do danych powinien być także możliwy zgodnie z instrumentami, które wprawdzie nie zostały przyjęte na podstawie wymienionego tytułu, jednakże Państwa Członkowskie przystąpiły do nich i instrumenty regulujące współpracę sądową w sprawach karnych przyjęte na podstawie tytułu VI Traktatu o Unii Europejskiej zawierają do nich odesłanie.

10. Zabezpieczenie danych *a priori* i dostęp do nich opisane powyżej, mogą stanowić ingerencję w prywatne życie danej osoby. Jednakże, taka ingerencja nie stanowi naruszenia międzynarodowych norm w zakresie prawa do poszanowania prywatności i przetwarzania danych osobowych przewidzianych, w szczególności, w Europejskiej Konwencji o Ochronie Praw Człowieka z 4 listopada 1950 r., Konwencji Rady Europy nr 108 o ochronie osób w związku z przetwarzaniem danych osobowych z 28 stycznia 1981 r. oraz dyrektyw 95/46/WE, 97/66/WE i 2002/58/WE, o ile na taka ingerencja jest przewidziana w przepisach oraz jest odpowiednia, ściśle proporcjonalna w stosunku do zamierzonego celu i niezbędna w społeczeństwie demokratycznym, a także podlega odpowiednim zabezpieczeniom zgodnie z celami zapobiegania, dochodzenia, wykrywania i ścigania przestępczości i przestępstw kryminalnych, w tym terroryzmu.

11. Uwzględniając zarówno potrzebę zapewnienia by dane były zabezpieczane *a priori* w sposób efektywny i zharmonizowany, jak też potrzebę pozostawienia Państwom Członkowskim szerokiego marginesu na dokonywanie indywidualnych ocen, ze względu na różnice występujące w systemach wymiaru sprawiedliwości, właściwe jest ustanowienie norm w zakresie zabezpieczenia danych *a priori.*

12. Dane mogą być zabezpieczane *a priori* przez różne okresy czasu, zależnie od ich rodzaju. Okresy zabezpieczenia poszczególnych rodzajów danych będą zależeć od użyteczności danych dla zapobiegania, dochodzenia, wykrywania i ścigania przestępczości i przestępstw kryminalnych oraz kosztów zabezpieczenia danych. Okresy zabezpieczenia poszczególnych rodzajów danych muszą być proporcjonalne do ich przydatności w zapobieganiu, dochodzeniu, wykrywaniu i ściganiu przestępczości i przestępstw kryminalnych, z drugiej zaś strony uwzględniać stopień ingerencji w życie prywatne, jaki pociągało będzie za sobą ujawnienie takich zabezpieczonych danych.

13. Przy sporządzeniu jakichkolwiek wykazów rodzajów danych, które powinny podlegać zabezpieczeniu, należy w sposób równoważny uwzględnić korzyści, jakie wynikają z zabezpieczenia poszczególnych rodzajów danych dla zapobiegania, dochodzenia, wykrywania i ścigania przestępstw i przestępczości oraz z drugiej strony stopień ingerencji w życie prywatne, które spowoduje ich zabezpieczenie.

14. Decyzja ramowa nie obowiązuje w odniesieniu do dostępu do danych w momencie ich przekazywania, to znaczy kontrolowania, przechwytywania i nagrywania telekomunikacji.

15. Państwa Członkowskie zobowiązane są zapewnić, że dostęp do zabezpieczonych danych uzyskiwany jest przy poszanowaniu zasad prywatności, określonych w prawie międzynarodowym obowiązującym w zakresie ochrony danych osobowych.

16. Państwa Członkowskie zobowiązane są zapewnić, że w ramach implementacji niniejszej decyzji ramowej zostaną przeprowadzone odpowiednie konsultacje w sektorze komunikacji elektronicznej.

PRZYJĘŁA NINIEJSZĄ DECYZJĘ:

Artykuł 1

Zakres i cel

1. Zadaniem niniejszej decyzji ramowej jest ułatwienie współpracy sądowej w sprawach karnych poprzez zbliżenie obowiązujących w Państwach Członkowskich przepisów w zakresie zabezpieczenia danych przetwarzanych i przechowywanych przez dostawców publicznych usług komunikacji elektronicznej lub publiczne sieci komunikacyjne, na cele zapobiegania, dochodzenia, wykrywania i ścigania przestępczości lub przestępstw kryminalnych, w tym terroryzmu.

2. Niniejsza decyzja ramowa nie obowiązuje w stosunku do treści przekazywanych komunikatów, w tym informacji do których dostęp uzyskiwany jest przy pomocy sieci komunikacji elektronicznej o ile taka sieć jest określona w prawie krajowym.

3. Każde Państwo Członkowskie może podjąć decyzję o niestosowaniu ust. 1 niniejszego artykułu w zakresie uwzględnienia zapobiegania przestępczości lub przestępstw kryminalnych jako celów zabezpieczenia przetwarzanych i przechowywanych danych, jeżeli w następstwie przeprowadzenia krajowej procedury lub konsultacji Państwo Członkowskie uzna, że wymienione cele nie mogą zostać uwzględnione. Państwo Członkowskie, które podejmie decyzje o skorzystaniu z tego odstępstwa, musi w każdym przypadku poinformować o tym Radę i Komisję.

4. Niniejsza decyzja nie narusza:

- przepisów obowiązujących w zakresie współpracy sądowej w sprawach karnych w odniesieniu do przechwytywania i nagrywania telekomunikacji;

- działań podejmowanych na rzecz bezpieczeństwa publicznego, obronności i bezpieczeństwa narodowego (tj. bezpieczeństwa państwa);

- przepisów krajowych dotyczących zabezpieczenia tych rodzajów danych, których dostawcy usług komunikacyjnych nie przechowują na cele prowadzonej działalności.

Artykuł 2

Definicje

1. Do celów niniejszej decyzji ramowej:

   (a) Definicja pojęcia „dane” przyjęta w niniejszej decyzji ramowej obejmuje dane o ruchu oraz dane dotyczące lokalizacji, określone w art. 2 dyrektywy 2002/58/WE, co obejmuje również dane dotyczące abonentów i informacje o użytkownikach związane z tymi danymi.

   (b) Informacje o użytkownikach oznaczają dane dotyczące każdej osoby fizycznej używającej dostępnej publicznie usługi komunikacji elektronicznej, na cele osobiste lub prowadzonej działalności gospodarczej, przy czym nie musi być ona abonentem tej usługi.

   (c) Informacje o użytkownikach oznaczają dane dotyczące każdej osoby fizycznej używającej publicznie dostępnej usługi komunikacji elektronicznej, na cele osobiste lub prowadzonej działalności gospodarczej, przy czym nie musi być ona abonentem tej usługi.

2. Do celów niniejszej decyzji ramowej dane obejmują:

   (a) Dane niezbędne do namierzenia i określenia źródła komunikatu, co obejmuje dane osobiste, dane kontaktowe oraz informacje określające zakupione usługi.

   (b) Dane niezbędne do określenia trasy i przeznaczenia komunikatu.

   (c) Dane niezbędne do określenia godziny i daty oraz czasu trwania komunikatu.

   (d) Dane niezbędne do identyfikacji telekomunikatu.

(e) Dane niezbędne do identyfikacji aparatu służącego do komunikacji lub urządzenia, które prawdopodobnie jest do niej używane.

(f) Dane niezbędne do określenia lokalizacji przy rozpoczęciu przekazywania oraz w okresie trwania komunikatu.

3. Dane te obejmują dane generowane przez dostawcę usług w ramach następującej infrastruktury, architektury i protokołów komunikacyjnych:

(a) Telefonia, z wyłączeniem usług przesyłania krótkich wiadomości tekstowych (SMS), elektronicznych wiadomości medialnych (EMS) i wiadomości multimedialnych (MMS)

(b) Usług SMS, EMS i MMS świadczonych jako element usługi telefonicznej.

(c) Protokoły internetowe, w tym poczta elektroniczna (e-mail), protokoły przesyłania głosu przez Internet (VoIP), światowa sieć (WWW), protokoły transferu plików, protokoły transferu sieciowego, protokoły transferu hypertekstowego (HTTP), głos przesyłany szerokopasmowo oraz podzbiory numerów protokołów internetowych - dane dotyczące tłumaczenia adresów sieciowych.

4. Technologie ułatwiające przekazywanie komunikatów powstałe w przyszłości będą objęte zakresem niniejszej decyzji ramowej.

Artykuł 3

Zabezpieczenie danych

Każde Państwo Członkowskie podejmie odpowiednie środki aby zapewnić, że na cele realizacji współpracy sądowej w sprawach karnych, przetwarzane i przechowywane dane, które zachowują dostawcy publicznych sieci komunikacyjnych lub publicznie dostępnych usług komunikacji elektronicznej, obejmujące dane o abonentach usługi oraz informacje o użytkowniku związane z tymi danymi, podlegają zabezpieczeniu zgodnie z postanowieniami niniejszej decyzji ramowej w celu ułatwienia współpracy sądowej w sprawach karnych.

Artykuł 4

Okresy zabezpieczenia danych

1. Każde Państwo Członkowskie podejmie odpowiednie środki by zapewnić, że dane zabezpieczane są na okres równy przynajmniej 12 miesiącom i nieprzekraczający 36 miesięcy od ich wygenerowania. Państwa Członkowskie mogą ustanawiać dłuższe okresy zabezpieczenia danych w zależności od kryteriów krajowych, o ile takie zabezpieczenie stanowi niezbędny, właściwy i proporcjonalny środek w społeczeństwie demokratycznym.

2. Państwo Członkowskie może odstąpić od stosowania ust. 1 niniejszego artykułu, w odniesieniu do danych objętych przez art. 2 ust. 2 w zakresie metod komunikacji określonych w art. 2 ust. 3 lit b) i c), o ile w następstwie przeprowadzenia krajowej procedury lub konsultacji dane Państwo Członkowskie uzna, że nie może zaakceptować okresów zabezpieczenia wyznaczonych w ust. 1 niniejszego artykułu. Państwo Członkowskie, które podejmie decyzje o skorzystaniu z tego odstępstwa, musi w każdym przypadku poinformować o tym Radę i Komisję, wskazując równocześnie alternatywne terminy, jakie przyjęło w stosunku do przedmiotowych rodzajów danych. Każde takie odstępstwo podlega corocznej weryfikacji.

Artykuł 5

Dostęp do danych w ramach współpracy sądowej w sprawach karnych

Wniosek Państwa Członkowskiego skierowany do innego Państwa Członkowskiego o udostępnienie danych określonych w art. 2 podlega złożeniu i rozpatrzeniu zgodnie z instrumentami regulującymi współpracę sądową przyjętymi na podstawie tytułu VI Traktatu o Unii Europejskiej. Państwo Członkowskie, które otrzymało wniosek o udostępnienie danych, może uzależnić jego pozytywne rozpatrzenie od spełnienia warunków, jakie należałoby spełnić w podobnej sprawie krajowej.

Artykuł 6

Ochrona danych

Każde Państwo Członkowskie zapewnia, że zabezpieczenie danych zgodnie z niniejszą decyzją ramową odbywać się będzie przy poszanowaniu co najmniej zasad wyszczególnionych poniżej i zobowiązane jest ustanowić środki prawne zgodnie z postanowieniami rozdziału III dyrektywy 95/46/WE, dotyczącymi „Środków prawnych, odpowiedzialności i sankcji":

(a) właściwe władze uzyskują dostęp do danych jedynie ze względu na szczególne, jasno określone i prawne potrzeby, rozpatrywane indywidualnie, zgodnie z prawem krajowym oraz nie będą poddawać takich danych dalszemu przetworzeniu w sposób niezgodny z tymi potrzebami.

(b) dane muszą być odpowiednie, właściwe a ich zakres nie może wykraczać poza ten, jaki wynika z potrzeb na jakie są udostępniane. Dane muszą być przetwarzane w sposób rzetelny i zgodny z prawem.

(c) dane, do których dostęp uzyskują właściwe władze zachowywane są w formie pozwalającej na identyfikację osób których dotyczą nie dłużej, niż jest to niezbędne ze względu na potrzeby na jakie zostały zebrane albo wtórnie przetworzone;

(d) zapewnia się poufność i integralność danych.

(e) udostępniane dane muszą być dokładne i należy podjąć wszelkie racjonalne środki by zapewnić, że wszelkie niedokładne dane osobowe będą podlegały usunięciu lub poprawieniu, przy uwzględnieniu potrzeb, na jakie zostały zebrane lub wtórnie przetworzone.

Artykuł 7

Bezpieczeństwo danych

Każde Państwo Członkowskie zapewni, że zabezpieczenie danych zgodnie z niniejszą decyzją ramową, będzie odbywać się przy poszanowaniu co najmniej poniższych zasad bezpieczeństwa danych i uwzględnione zostaną postanowienia art. 4 dyrektywy:

(a) zabezpieczone dane będą tej samej jakości co dane w sieci;

(b) dane będą przechowywane przy użyciu odpowiednich środków technicznych i organizacyjnych, chroniących je przed przypadkowym lub bezprawnym zniszczeniem lub przypadkową utratą, zmianą, nieupoważnionym ujawnieniem lub udostępnieniem oraz przed wszelkimi innymi bezprawnymi formami przetwarzania;

(c) wszelkie dane muszą zostać zniszczone po upływie okresu przechowywania, za wyjątkiem danych, do które zostały udostępnione i zachowane;

(d) Każde Państwo Członkowskie określa w prawie krajowym procedurę udostępniania zabezpieczonych danych i zachowania ich.

Artykuł 8

Implementacja

Państwa Członkowskie podejmą środki niezbędne do realizacji postanowień niniejszej decyzji ramowej do […..czerwca 2007 r.] w terminie dwóch lat od daty jej przyjęcia.

W tym samym terminie Państwa Członkowskie zobowiązane są przekazać do generalnego sekretariatu Rady oraz do Komisji treść postanowień transponujących do prawa krajowego obowiązki, jakie niniejsza decyzja ramowa nakłada na Państwa Członkowskie. Sekretariat Generalny Rady zawiadomi Państwa Członkowskie o informacjach uzyskanych na podstawie niniejszego artykułu.

Komisja do [.... 1 stycznia 2008 r.] przekaże Radzie sprawozdanie w sprawie oceny w jakim zakresie Państwa Członkowskie podjęły środki niezbędne do realizacji postanowień niniejszej decyzji ramowej.

Artykuł 9

Wejście w życie

Niniejsza decyzja ramowa wchodzi w życie dwudziestego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej.

Sporządzono w Brukseli,

_____