I

(Informacje)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych na temat wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie zatrzymywania danych przetwarzanych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej zmieniającej dyrektywę 2002/58/WE (COM(2005) 438 wersja ostateczna)

(2005/C 298/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 286,

uwzględniając Kartę Praw Podstawowych Unii Europejskiej, w szczególności jej art. 8,

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych ([1]) oraz dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywę o prywatności i łączności elektronicznej) ([2]),

uwzględniając rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych ([3]), w szczególności jego art. 41,

uwzględniając wniosek o wydanie opinii zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 otrzymany od Komisji w dniu 23 września 2005 r.,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. Wstęp

1. Europejski Inspektor Ochrony Danych (EIOD) przyjmuje z zadowoleniem wniosek o wydanie opinii na podstawie art. 28 ust. 2 rozporządzenia (WE) nr 45/2001. Jednak uwzględniając wiążący charakter art. 28 ust. 2 rozporządzenia (WE) nr 45/2001, niniejsza opinia powinna zostać wspomniana w preambule dyrektywy.

2. EIOD uznaje wagę dysponowania przez organy ścigania Państw Członkowskich wszelkimi niezbędnymi instrumentami prawnymi, służącymi w szczególności do walki z terroryzmem i innymi poważnymi przestępstwami. Należna

([1]) Dz.U. L 281 z 23.11.1995, str. 31.

([2]) Dz.U. L 201 z 31.7.2002, str. 37.

([3]) Dz.U. L 8 z 12.1.2001, str. 1.

dostępność pewnych danych dotyczących ruchu oraz danych dotyczących lokalizacji związanych z publicznymi usługami łączności elektronicznej może być dla tych organów ścigania kluczowym narzędziem i może przyczynić się do zapewnienia fizycznego bezpieczeństwa ludności. Ponadto należy zauważyć, że nie łączy się to automatycznie z koniecznością wprowadzenia nowych instrumentów, jak przewidziano w omawianym wniosku.

3. Jest również oczywiste, że wniosek ma znaczny wpływ na kwestie ochrony danych osobowych. Jeżeli rozważa się wniosek wyłącznie z perspektywy ochrony danych osobowych, dane dotyczące ruchu oraz dane dotyczące lokalizacji nie powinny w ogóle być zatrzymywane do celów ścigania przestępstw. Właśnie z powodów ochrony danych dyrektywa 2002/58/WE ustanawia zasadę prawną przewidującą, że dane dotyczące ruchu muszą zostać usunięte, gdy tylko ich przechowywanie przestaje być niezbędne do celów ściśle związanych z komunikacją (w tym naliczania płatności). Wyjątki od tej zasady prawnej są obwarowane ścisłymi ograniczeniami.

4. W niniejszej opinii EIOD naświetli wpływ wniosku na ochronę danych osobowych. EIOD uwzględni ponadto fakt, że – niezależnie od wagi wniosku dla ścigania przestępstw – jego wprowadzenie w życie nie może skutkować pozbawieniem obywateli ich podstawowego prawa do ochrony prywatności.

5. Niniejsza opinia EIOD musi być rozważana w świetle tych uwag. EIOD zakłada zrównoważone podejście, w którym główną rolę odgrywa konieczność i proporcjonalność ingerencji w ochronę danych.

6. Sam wniosek musi być rozważany jako reakcja na zgłoszoną przez Republiką Francuską, Irlandię, Królestwo Szwecji oraz Zjednoczone Królestwo inicjatywę dotyczącą wprowadzenia decyzji ramowej w sprawie zatrzymywania danych przetwarzanych i przechowywanych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej lub danych w publicznych sieciach łączności do celów zapobiegania, dochodzenia, wykrywania i ścigania przestępczości i przestępstw, w tym terroryzmu („projekt decyzji ramowej"), która została odrzucona przez Parlament Europejski (w ramach procedury konsultacji).

7. Do EIOD nie zwrócono się z wnioskiem o wydanie opinii w sprawie projektu decyzji ramowej ani też nie wydał on takiej opinii z własnej inicjatywy. EIOD nie zamierza obecnie wydawać opinii dotyczącej projektu decyzji ramowej, ale w niniejszej decyzji będzie się odnosić do tego projektu, o ile uzna to za stosowne.

II. **Uwagi ogólne**

Wpływ wniosku na kwestie ochrony danych osobowych

8. Sprawą kluczową dla EIOD jest poszanowanie we wniosku praw podstawowych. Środek legislacyjny naruszający ochronę zagwarantowaną w prawie wspólnotowym, a w szczególności w orzecznictwie Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka, jest nie tylko niemożliwy do przyjęcia, ale także niezgodny z prawem. Warunki życia społecznego mogły ulec zmianie z powodu ataków terrorystycznych, lecz nie może to skutkować narażeniem na szwank wysokich standardów ochrony w państwie prawa. Ochrona jest gwarantowana prawem niezależnie od potrzeb związanych ze ściganiem przestępstw w danej chwili. Ponadto samo orzecznictwo umożliwia wyjątki, o ile są one konieczne w społeczeństwie demokratycznym.

9. Omawiany wniosek wpływa w sposób bezpośredni na ochronę gwarantowaną art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (EKPC). Zgodnie z orzecznictwem Europejskiego Trybunału Praw Człowieka:

— przechowywanie informacji o poszczególnych osobach zostało uznane za ingerencję w życie prywatne, nawet jeżeli nie zawierają one informacji wrażliwych (Amann ([1])),

— to samo dotyczy praktyki „meteringu" połączeń telefonicznych polegającego na użyciu urządzenia elektronicznego rejestrującego w sposób automatyczny numery wybierane przez dany telefon oraz daty, godziny i czas trwania każdego połączenia (Malone ([2])),

— uzasadnienie ingerencji powinno być bardziej istotne niż szkodliwy wpływ, jaki samo istnienie omawianych przepisów mogłoby mieć na osoby, których dotyczą dane (Dudgeon ([3])).

10. Artykuł 6 ust. 2 Traktatu o UE stanowi, że Unia respektuje prawa podstawowe, gwarantowane w EKPC. W poprzednim ustępie wykazano, że, zgodnie z orzecznictwem Europejskiego Trybunału Praw Człowieka, obowiązek zatrzymywania danych wchodzi w zakres zastosowania art. 8 EKPC i konieczne jest bardzo pilne uzasadnienie z poszanowaniem kryteriów orzeczenia w sprawie

([1]) Orzeczenie ETPC z dnia 16 lutego 2000 r., Amann, 2000-II, skarga 27798/95.

([2]) Orzeczenie ETPC z dnia 2 sierpnia 1984 r., Malone, A82, skarga 8691/79.

([3]) Orzeczenie ETPC z dnia 22 października 1981 r., Dudgeon, A45, skarga 7525.

Dudgeon. Musi zostać dowiedziona konieczność i proporcjonalność obowiązkowego zatrzymywania danych w pełnym zakresie.

11. Ponadto omawiany wniosek wywiera bardzo znaczący wpływ na zasady ochrony danych uznane w prawodawstwie wspólnotowym:

— dane muszą być zatrzymywane przez okres o wiele dłuższy od okresu ich zatrzymywania przez dostawców publicznych usług łączności elektronicznej lub publiczne sieci łączności (obydwie te kategorie są dalej zwane „dostawcami usług"),

— na mocy dyrektywy 2002/58/WE, a w szczególności jej art. 6, dane mogą być zbierane i przechowywane z powodów bezpośrednio związanych z samym procesem komunikacji, w tym naliczania płatności ([1]). Następnie dane muszą zostać usunięte (z zastrzeżeniem wyjątków). Zgodnie z omawianym wnioskiem zatrzymywanie danych do celów ścigania przestępstw jest obowiązkowe. Wychodzi się więc z przeciwnego założenia,

— dyrektywa 2002/58/WE zapewnia bezpieczeństwo i poufność danych. Omawiany wniosek nie może prowadzić do luk prawnych w tym zakresie; wymagane są ścisłe gwarancje oraz wyjaśnienie ograniczeń związanych z celami ich zatrzymywania,

— wprowadzenie obowiązku zatrzymywania danych, przewidziane w omawianym wniosku, prowadzi do powstania dużych baz danych i skutkuje powstaniem szczególnego ryzyka dla osoby, której dotyczą dane. Można tutaj wspomnieć o komercyjnym wykorzystaniu danych oraz ich użyciu do oszukańczego pozyskiwania poufnych informacji osobistych (*phishing*) lub eksploracji danych (*data mining*) przez organy ścigania lub krajowe służby bezpieczeństwa.

12. Wreszcie ochrona życia prywatnego wraz z ochroną danych osobowych zostały uznane w Karcie Praw Podstawowych, jak wspomniano w memorandum wyjaśniającym.

13. Wpływ omawianego wniosku na ochronę danych osobowych wymaga szczegółowego zbadania. W niniejszej analizie EIOD uwzględni powyższe elementy oraz przedstawi we wnioskach konieczność wprowadzenia większej ilości gwarancji. Zwykłe odniesienie do istniejących ram prawnych dotyczących ochrony danych (w szczególności dyrektyw 95/46/WE i 2002/58/WE) nie jest wystarczające.

Konieczność zatrzymywania danych dotyczących ruchu oraz danych dotyczących lokalizacji

14. EIOD przypomina wnioski Zespołu Roboczego ds. Ochrony Danych art. 29 z dnia 9 listopada 2004 r. dotyczące projektu decyzji ramowej. Zespół Roboczy stwierdził, że obowiązkowe zatrzymywanie danych dotyczących ruchu na warunkach przewidzianych decyzją ramową jest nie do przyjęcia. Wnioski te były oparte między innymi na niedostarczeniu jakichkolwiek dowodów istnienia potrzeby zatrzymywania danych do celów utrzymania porządku publicznego, gdyż analiza wykazała, iż najbardziej znacząca ilość danych dotyczących ruchu, których przekazania żądały organy ścigania, dotyczyła danych nie starszych niż sześć miesięcy.

15. W opinii EIOD powyższe rozważania Zespołu Roboczego ds. Ochrony Danych art. 29 powinny być punktem wyjścia dla oceny omawianego wniosku. Wynik tych rozważań jednakże nie może być po prostu przeniesiony na omawiany wniosek. Należy wziąć pod uwagę możliwą zmianę warunków. W opinii EIOD następujące zmiany mogą być istotne dla oceny wniosku.

16. Po pierwsze, przedstawiono pewne informacje, by dowieść, że w praktyce organy ścigania żądają przedstawienia danych dotyczących ruchu z ostatniego roku. Komisja oraz Prezydencja Rady przywiązują wagę do wyników badań przeprowadzonych przez policję Zjednoczonego Królestwa ([2]), które wskazują, że chociaż 85 % danych dotyczących ruchu wykorzystywanych przez policję pochodziło z ostatnich sześciu miesięcy, dane mające sześć miesięcy do roku wykorzystywano w skomplikowanych dochodzeniach dotyczących poważniejszych przestępstw. Przytoczono również przykłady dochodzeń. Okres zatrzymywania danych ujęty we wniosku – 1 rok dla danych dotyczących łączności telefonicznej – opiera się na praktyce organów ścigania.

17. EIOD nie jest przekonany, by te informacje rzeczywiście świadczyły o konieczności zatrzymywania danych dotyczących ruchu za okres jednego roku. Fakt, że w niektórych przypadkach dostępność danych dotyczących ruchu lub lokalizacji pomogła w dochodzeniu dotyczącym przestępstwa, nie oznacza automatycznie, że dane te są konieczne (ogólnie rzecz biorąc) jako narzędzie organów ścigania. Informacji tych jednakże nie można ignorować. Stanowią one co najmniej poważną próbę dowiedzenia konieczności zatrzymywania danych. Ponadto wspomniane informacje jasno wskazują, że okres zatrzymania danych przekraczający jeden rok nie jest wymagany z punktu widzenia bieżącej praktyki organów ścigania.

18. Po drugie, nie zawsze wykorzystuje się możliwości zatrzymywania danych dotyczących ruchu przez dostawców usług do celów naliczania płatności na mocy dyrektywy 2002/58/WE, jako że coraz częściej dane do celów naliczania płatności nie są w ogóle zatrzymywane (wykorzystuje się przedpłacone karty w telefonii komórkowej, abonamenty

([1]) Patrz: także pkt 3 niniejszej opinii.

([2]) Wolność a bezpieczeństwo – w poszukiwaniu należnej równowagi. Dokument brytyjskiej Prezydencji Unii Europejskiej z dnia 7 września 2005 r.

z opłatą ryczałtową itp.). W takich przypadkach, które stają się coraz częstsze, dane dotyczące ruchu i lokalizacji nie będą w ogóle przechowywane, lecz zostaną usunięte natychmiast po zakończeniu połączenia. To samo odnosi się do połączeń niezrealizowanych. Może to oddziaływać na skuteczność ścigania przestępstw.

19. Ponadto rozwój usług telekomunikacyjnych może prowadzić do zaburzeń w funkcjonowaniu rynku wewnętrznego między innymi z powodu (rychłego) przyjęcia przez Państwa Członkowskie środków legislacyjnych na mocy art. 15 dyrektywy 2002/58/WE. Na przykład rząd Włoch opublikował ostatnio dekret zobowiązujący dostawców usług do przechowywania danych dotyczących telefonii przez 4 lata. Obowiązek ten pociąga za sobą znaczne koszty dla Państw Członkowskich, takich jak Włochy.

20. Po trzecie, także metody pracy organów ścigania zostały udoskonalone: większe znaczenie mają proaktywne techniki śledcze oraz wykorzystanie wsparcia technicznego. Udoskonalenia te wymagają od władz dysponowania odpowiednimi i precyzyjnie sformułowanymi narzędziami umożliwiającymi im pracę z należnym poszanowaniem zasad ochrony danych. Jednym z narządzi, którymi zwykle dysponują władze w Państwach Członkowskich, jest zachowywanie lub zamrażanie danych dotyczących połączeń dokonywane na wniosek w związku z konkretnym dochodzeniem. Stwierdzono uprzednio, że to narzędzie, samo w sobie mające mniejszy wpływ na zasady ochrony danych niż narzędzie przedstawione we wniosku (zatrzymywanie danych), mogłoby nie być wystarczające w pewnych sytuacjach, w szczególności do śledzenia osób zaangażowanych w działalność terrorystyczną lub inne poważne przestępstwa, których wcześniej nie podejrzewano o prowadzenie działalności przestępczej. Konieczna jest jednak większa liczba dowodów, by stwierdzić, czy to stwierdzenie jest prawdziwe.

21. Po czwarte, wzrosły obawy związane z atakami terrorystycznymi. EIOD podziela opinię wyrażoną w kontekście wniosku dotyczącego zatrzymywania danych, że fizyczne bezpieczeństwo ludności jest bez wątpienia czynnikiem najistotniejszym. Społeczeństwo potrzebuje ochrony. Dlatego też rządy są zobowiązane, w przypadku ataków skierowanych przeciw ludności, do wykazania, że w sposób poważny traktują potrzebę ochrony oraz do zbadania, czy muszą zareagować na zagrożenia wprowadzając nowe środki legislacyjne. Oczywiste jest, że EIOD w pełni popiera zadania rządów, na szczeblu krajowym oraz europejskim, polegające na ochronie społeczeństwa i wykazaniu, że dokładają wszelkich starań, by tę ochronę zapewnić, również poprzez przyjmowanie nowych, uzasadnionych prawnie i skutecznych środków w wyniku przeprowadzonych badań.

22. EIOD uznaje zmianę warunków, ale jak dotąd nie jest przekonany co do konieczności zatrzymywania danych dotyczących ruchu i lokalizacji do celów ścigania przestępstw, którą przewiduje tekst omawianego wniosku. EIOD podkreśla wagę zasady prawnej ustanowionej dyrektywą 2002/58/WE, określającej, że dane dotyczące ruchu muszą zostać usunięte, gdy tylko ich przechowywanie przestaje być niezbędne do celów samej łączności. Ponadto przedstawione informacje nie dowodzą, że istniejące ramy prawne nie oferują narzędzi niezbędnych do ochrony fizycznego bezpieczeństwa ani że Państwa Członkowskie w pełni wykorzystują swoje zgodne z prawem europejskim kompetencje dotyczące współpracy, przyznane im w obrębie istniejących ram prawnych (bez wymaganych rezultatów).

23. Jednak jeżeli Parlament Europejski i Rada, po uważnym rozważeniu wszystkich wchodzących w grę interesów, dojdą do wniosku, że konieczność zatrzymywania danych dotyczących ruchu i lokalizacji jest wystarczająco dowiedziona, EIOD uzna, że zatrzymywanie danych może być usprawiedliwione na mocy prawa Wspólnoty jedynie przy poszanowaniu zasady proporcjonalności i z zapewnieniem odpowiednich gwarancji zgodnie z niniejszą opinią.

Proporcjonalność

24. Proporcjonalność nowego wnioskowanego środka legislacyjnego zależy od treści składających się nań przepisów: czy stanowi należną i proporcjonalną reakcję na potrzeby społeczeństwa?

25. Pierwsza uwaga odnosi się do adekwatności wniosku: czy można się spodziewać, że wniosek zwiększy fizyczne bezpieczeństwo osób zamieszkujących terytorium Unii Europejskiej? Powodem wątpliwości w odniesieniu do adekwatności, często wspominanym w debatach publicznych, jest fakt, że dane dotyczące ruchu i lokalizacji nie zawsze są powiązane z konkretną osobą, więc poznanie numeru telefonu (lub adresu IP) niekoniecznie prowadzi do poznania tożsamości osoby. Innym, nawet poważniejszym powodem wątpliwości jest to, czy istnienie gigantycznych baz danych umożliwi organom ścigania łatwe znalezienie danych potrzebnych w danym dochodzeniu, czy też nie.

26. EIOD jest zdania, że zatrzymywanie danych dotyczących ruchu i lokalizacji samo w sobie nie stanowi adekwatnej ani skutecznej reakcji. Potrzebne są dodatkowe środki w celu zapewnienia władzom ukierunkowanego i szybkiego dostępu do danych potrzebnych w danym dochodzeniu. Zatrzymywanie danych jest adekwatne i skuteczne, tylko jeżeli istnieją skuteczne wyszukiwarki.

27. Druga uwaga odnosi się do proporcjonalności reakcji. Aby zachować proporcjonalność, wniosek powinien:

— ograniczyć okresy zatrzymywania danych. Okresy te muszą odpowiadać udokumentowanym potrzebom organów ścigania,

— ograniczyć ilość danych, które mają być przechowywane. Ilość ta musi odpowiadać udokumentowanym potrzebom organów ścigania oraz należy uniemożliwić dostęp do zawartości informacyjnej komunikatu,

— zawierać odpowiednie środki bezpieczeństwa w celu ograniczenia dostępu do danych i ich dalszego wykorzystania, zagwarantowania ich bezpieczeństwa oraz zapewnienia, że osoby, których dotyczą te dane, mogą korzystać ze swoich praw w stosunku do nich.

28. EIOD podkreśla wagę tych ścisłych ograniczeń wraz z odpowiednimi gwarancjami w celu ograniczenia dostępu. Uważa, że uwzględniając znaczenie trzech wspomnianych powyżej elementów, Państwa Członkowskie mogą – w odniesieniu do tych trzech elementów – powstrzymać się od zastosowania dodatkowych krajowych środków, które negatywnie wpływają na proporcjonalność. Ta potrzeba harmonizacji zostanie szerzej omówiona w części IV.

Odpowiednie środki bezpieczeństwa

29. Skutkiem wniosku będzie dysponowanie przez dostawców usług bazami danych, w których przechowywane będą znaczące ilości danych dotyczących ruchu i lokalizacji.

30. Po pierwsze, wniosek będzie musiał zapewnić ograniczenie dostępu do danych i ich dalszego wykorzystania wyłącznie na określonych warunkach i do ograniczonej liczby określonych celów.

31. Po drugie, bazy danych będą musiały podlegać odpowiedniej ochronie (bezpieczeństwo danych). W tym celu należy zapewnić, że w chwili zakończenia okresu zatrzymania dane zostaną skutecznie usunięte. Nie powinno mieć miejsca zrzucanie danych (ang. *dumping*) ani też ich eksploatacja. Podsumowując, konieczne jest zapewnienie wysokiego poziomu bezpieczeństwa danych oraz odpowiednich technicznych i organizacyjnych środków bezpieczeństwa.

32. Wysoki poziom bezpieczeństwa danych staje się jeszcze bardziej istotny z tego powodu, że samo istnienie danych mogłoby prowadzić do żądań dostępu do nich i ich wykorzystania stawianych przez co najmniej trzy zainteresowane grupy:

— samych dostawców usług. Mogą oni odczuwać pokusę wykorzystania danych do własnych celów komercyjnych. Konieczne są gwarancje uniemożliwiające kopiowanie plików danych,

— organy ścigania: wniosek oferuje im prawo dostępu, ale tylko w szczególnych wypadkach i zgodnie z przepisami prawa krajowego (art. 3 ust. 2 wniosku). Nie powinien być możliwy dostęp do danych w celach ich eksploracji lub pozyskiwania poufnych informacji osobistych. Wymiana danych z organami innych Państw Członkowskich powinna być jasno uregulowana,

— służby wywiadowcze (odpowiedzialne za bezpieczeństwo narodowe).

33. W odniesieniu do dostępu służb wywiadowczych EIOD zauważa, że, zgodnie z art. 33 Traktatu o UE oraz art. 64 Traktatu WE, interwencje w obrębie trzeciego i pierwszego filaru nie naruszają wykonywania przez Państwa Członkowskie obowiązków dotyczących utrzymania poszanowania prawa i porządku publicznego oraz ochrony bezpieczeństwa wewnętrznego. Zgodnie z opinią EIOD w wyniku tych przepisów Unii Europejskiej brak kompetencji do kontrolowania dostępu służb bezpieczeństwa lub wywiadu do danych zatrzymanych przez dostawców usług. Innymi słowy, ani dostęp tych służb do danych dotyczących ruchu i lokalizacji zatrzymywanych przez dostawców usług, ani dalsze wykorzystanie informacji uzyskanych przez wspomniane służby nie są regulowane przez prawo Unii Europejskiej. Ten element musi zostać uwzględniony podczas oceny wniosku. Państwa Członkowskie powinny przyjąć niezbędne środki w celu uregulowania dostępu do danych przez służby wywiadowcze.

34. Po trzecie, zagadnienia opisane w poprzednich punktach mają potencjalne implikacje dla osób, których dotyczą zatrzymywane dane. Niezbędne są dodatkowe gwarancje zapewniające osobom, których wspomniane dane dotyczą, możliwość łatwego i szybkiego wykonywania swoich praw w tym zakresie. EIOD wskazuje na potrzebę skutecznej kontroli dostępu do danych i ich dalszego wykorzystania, najlepiej wykonywanej przez organy sądowe w Państwach Członkowskich. Gwarancje takie powinny mieć również zastosowanie w przypadkach dostępu do danych dotyczących ruchu i dalszego wykorzystania tych danych przez organy w innych Państwach Członkowskich.

35. W tym kontekście EIOD odwołuje się do inicjatyw mających na celu stworzenie nowych ram prawnych dla ochrony danych mających zastosowanie do organów ścigania (w trzecim filarze Traktatu UE). W opinii EIOD takie ramy prawne wymagają dodatkowych gwarancji i nie mogą się ograniczać do potwierdzenia ogólnych zasad ochrony danych zawartych w pierwszym filarze ([1]).

36. Po czwarte, istnieje bezpośredni związek pomiędzy adekwatnością środków bezpieczeństwa a ich kosztami. Adekwatne przepisy prawa dotyczące zatrzymywania danych muszą więc zawierać bodźce zachęcające dostawców usług do inwestowania w infrastrukturę techniczną. Mogłyby nimi być zwroty dodatkowych kosztów adekwatnych środków bezpieczeństwa wprowadzanych przez dostawców usług.

37. Podsumowując, adekwatne środki bezpieczeństwa powinny:

— ograniczać dostęp do danych i ich dalsze wykorzystanie,

— zapewniać odpowiednie techniczne i organizacyjne środki bezpieczeństwa w celu ochrony baz danych. Obejmuje to odpowiednie usunięcie danych na koniec okresu zatrzymania oraz informacje o żądaniach dostępu

([1]) Patrz: Stanowisko w sprawie ścigania przestępstw i wymiany informacji w UE (*Position Paper on Law Enforcement and Information Exchange in the EU*) przyjęte podczas Wiosennej Konferencji Europejskich Organów Ochrony Danych w Krakowie w dniach 25–26 kwietnia 2005 r.

do danych i ich wykorzystania zgłaszanych przez różne grupy zainteresowanych podmiotów,

— zapewnić wykonywanie praw osób, których dotyczą dane, nie tylko poprzez potwierdzenie ogólnych zasad ochrony danych,

— zawierać bodźce zachęcające dostawców usług do inwestowania w infrastrukturę techniczną.

III. **Podstawa prawna a projekt decyzji ramowej**

38. Wniosek jest oparty na Traktacie WE, a w szczególności na jego art. 95, zaś jego celem, zgodnie z art. 1 wniosku, jest harmonizacja zobowiązań dostawców usług w stosunku do przetwarzania i zatrzymywania danych dotyczących ruchu i lokalizacji. Artykuł ten określa, że dane udostępnia się wyłącznie właściwym organom krajowym w indywidualnych przypadkach, związanych z przestępstwami kryminalnymi, ale pozostawia bardziej precyzyjną definicję celu oraz dostępu do danych i ich dalszego wykorzystania w gestii Państw Członkowskich z zastrzeżeniem gwarancji zawartych w istniejących wspólnotowych ramach ochrony danych.

39. Pod tym względem omawiany wniosek ma bardziej ograniczony zakres zastosowania niż projekt decyzji ramowej, oparty na art. 31 ust. 1 lit. c) Traktatu UE i zawierający dodatkowe przepisy dotyczące dostępu do zatrzymanych danych oraz wnioskach o udostępnienie składanych przez inne Państwa Członkowskie. W memorandum wyjaśniającym zawarto uzasadnienie tego ograniczenia zakresu zastosowania wniosku. Określa ono, że dostęp do informacji i ich wymiana pomiędzy odpowiednimi organami ścigania nie wchodzi w zakres zastosowania Traktatu WE.

40. EIOD nie jest przekonany co do zasadności tego stwierdzenia zawartego w memorandum wyjaśniającym. Interwencja Wspólnoty na podstawie art. 95 Traktatu WE (rynek wewnętrzny) musi mieć na celu przede wszystkim usunięcie przeszkód handlowych. Zgodnie z orzecznictwem Trybunału Sprawiedliwości interwencja musi rzeczywiście przyczyniać się do usunięcia takich przeszkód. W swojej interwencji organ prawodawczy Wspólnoty musi jednakże zapewnić poszanowanie praw podstawowych (art. 6 ust. 2 Traktatu UE; patrz: sekcja II niniejszej opinii). Ze wszystkich powyższych powodów ustanowienie na szczeblu Wspólnoty zasad zatrzymywania danych w interesie rynku wewnętrznego może wymagać również zajęcia się poszanowaniem praw podstawowych na szczeblu Wspólnoty Europejskiej. Jeżeli organ prawodawczy Wspólnoty nie mógłby ustanowić zasad dostępu do danych i ich wykorzystania, nie byłby on w stanie wypełniać swoich obowiązków określonych w art. 6 Traktatu UE, gdyż zasady te są konieczne do zapewnienia, że dane są zatrzymywane z należnym poszanowaniem praw podstawowych. Innymi słowy, zdaniem EIOD, zasady dostępu do danych, ich wykorzystania i wymiany są nierozdzielnie złączone z samym obowiązkiem ich zatrzymywania.

41. Odnośnie do ustanowienia właściwych organów EIOD przyznaje, że leży ono w gestii Państw Członkowskich, podobnie jak organizacja ścigania przestępstw i ochrony sądowej. Akt prawny Wspólnoty może jednak nałożyć na Państwa Członkowskie warunki dotyczące wyznaczania właściwych organów, kontroli sądowej oraz dostępu obywateli do wymiaru sprawiedliwości. Przepisy te zapewniają istnienie na szczeblu krajowym odpowiednich mechanizmów gwarantujących pełną skuteczność aktu, w tym pełną zgodność z prawodawstwem dotyczącym ochrony danych.

42. EIOD pragnie zwrócić uwagę na inne zagadnienie związane z podstawą prawną. W gestii organów prawodawczych Wspólnoty leży wybór odpowiedniej podstawy prawnej oraz, zgodnie z nią, odpowiedniej procedury legislacyjnej. Wybór ten pozostaje poza zakresem zadań EIOD. Jednak w świetle ważnych, a wręcz zasadniczych kwestii, o których mowa, w obecnej sytuacji EIOD zdecydowanie opowiada się za procedurą współdecydowania. Tylko ta procedura stanowi przejrzysty proces podejmowania decyzji z pełnym zaangażowaniem wszystkich trzech biorących w niej udział instytucji i z należnym poszanowaniem zasad, na których oparta jest Unia.

IV. **Potrzeba harmonizacji**

43. Wniosek w sprawie dyrektywy harmonizuje rodzaje danych, jakie mają być zatrzymywane, okresy zatrzymania danych oraz cele, w jakich dane mogą zostać przekazywane właściwym organom. Wniosek przewiduje pełną harmonizację tych elementów. Pod tym względem różni się on zasadniczo od projektu decyzji ramowej, który przewidywał zasady minimalne.

44. EIOD podkreśla potrzebę pełnej harmonizacji wspomnianych elementów, mając na względzie funkcjonowanie rynku wewnętrznego, potrzebę ścigania przestępstw oraz, nie mniej ważnych, EKPC oraz zasad ochrony danych.

45. W odniesieniu do funkcjonowania rynku wewnętrznego harmonizacja obowiązku zatrzymywania danych uzasadnia wybór podstawy prawnej dla wniosku (art. 95 Traktatu WE). Przyzwolenie na istnienie zasadniczych różnic pomiędzy ustawodawstwem poszczególnych Państw Członkowskich nie usunęłoby istniejących problemów na wewnętrznym rynku łączności elektronicznej, które wynikają, między innymi, z (rychłego) przyjęcia przez Państwa Członkowskie środków legislacyjnych na mocy art. 15 dyrektywy 2002/58/WE (patrz: pkt 19 niniejszej opinii).

46. Jest to nawet ważniejsze, gdyż znaczna część łączności elektronicznej podlega jurysdykcji więcej niż jednego Państwa Członkowskiego. Przykładem tego są: międzynarodowe połączenia telefoniczne, *roaming*, przekraczanie granicy *podczas* połączenia komórkowego oraz korzystanie z usług dostawcy działającego w innym Państwie Członkowskim niż państwo zamieszkania osoby korzystającej z tych usług.

47. Ponadto w tym kontekście brak harmonizacji wpłynąłby negatywnie na potrzeby organów ścigania o tyle, że właściwe organy musiałyby dostosować się do różnych wymogów prawnych. Mogłoby to uniemożliwić wymianę informacji pomiędzy organami różnych Państw Członkowskich.

48. Na koniec EIOD podkreśla – odwołując się do swoich obowiązków na mocy art. 41 rozporządzenia 45/2001/WE – że pełna harmonizacja zasadniczych elementów zawartych we wniosku jest niezbędna do zachowania zgodności z EKPC oraz zasadami ochrony danych. Jakikolwiek środek legislacyjny zobowiązujący do zatrzymywania danych dotyczących ruchu i lokalizacji musi jasno ograniczać ilość zatrzymywanych danych, okresy zatrzymania oraz dostęp do danych i ich dalsze wykorzystanie (ich cele), aby być możliwym do przyjęcia z punktu widzenia ochrony danych oraz spełniać wymogi konieczności i proporcjonalności.

V. Uwagi dotyczące poszczególnych artykułów wniosku

Artykuł 3: Obowiązek zatrzymywania danych

49. Artykuł 3 stanowi kluczowy przepis wniosku. Artykuł 3 ust. 1 wprowadza obowiązek zatrzymywania danych dotyczących ruchu i lokalizacji, zaś art. 3 ust. 2 odnosi się do zasady ograniczenia celu. Artykuł 3 ust. 2 ustanawia trzy istotne ograniczenia. Zatrzymane dane są udostępniane wyłącznie:

— właściwym organom krajowym,

— w określonych przypadkach;

— do celów zapobiegania, dochodzenia, wykrywania i ścigania poważnych przestępstw, takich jak terroryzm i przestępczość zorganizowana.

Artykuł 3 ust. 2 odwołuje się do ustawodawstwa krajowego Państw Członkowskich w celu szczegółowego określenia dalszych ograniczeń.

50. EIOD z zadowoleniem przyjmuje art. 3 ust. 2 jako istotny przepis, ale stwierdza, że ograniczenia nie są wystarczająco precyzyjne oraz że dostęp do danych i ich dalsze wykorzystanie powinny być jasno uregulowane dyrektywą, a także że niezbędne są dodatkowe gwarancje. Jak wspomniano w sekcji III niniejszej opinii, EIOD nie jest przekonany co do tego, że niewłączenie (precyzyjnych) przepisów dotyczących dostępu do danych dotyczących ruchu i lokalizacji oraz ich dalszego wykorzystania jest nieuniknionym skutkiem wyboru podstawy prawnej wniosku (art. 95 Traktatu WE). Prowadzi to do następujących uwag:

51. Po pierwsze, nie wyszczególniono, że inne zainteresowane podmioty, jak sami dostawcy usług, nie mają dostępu do danych. Na mocy art. 6 dyrektywy 2002/58/WE dostawcy usług mogą przetwarzać dane dotyczące ruchu wyłącznie do końca okresu ich zatrzymania do celów naliczania płatności. Według EIOD nie ma innego uzasadnienia dla dostępu do danych ze strony dostawców usług lub innych zainteresowanych podmiotów niż dostęp przewidziany na mocy dyrektywy 2002/58/WE, z zastrzeżeniem warunków określonych tą dyrektywą.

52. EIOD zaleca dodanie do tekstu przepisu zapewniającego, że osoby inne niż właściwe organy nie mają dostępu do danych. Przepis ten może mieć następujące brzmienie: „dostęp do danych lub ich przetwarzanie jest możliwe wyłącznie w celach określonych w art. 3 ust. 2" lub „dostawcy usług skutecznie zapewniają możliwość dostępu wyłącznie właściwym organom".

53. Po drugie, ograniczenie do określonych przypadków wydaje się zabraniać rutynowego dostępu w celu oszukańczego pozyskiwania poufnych informacji osobistych (*phishing*) lub eksploracji danych (*data mining*). Tekst wniosku powinien jednakże określać, że dane mogą być udostępnione wyłącznie w związku z określonym przestępstwem.

54. Po trzecie, EIOD z zadowoleniem przyjmuje fakt, że cel dostępu został ograniczony do poważnych przestępstw, takich jak terroryzm i przestępczość zorganizowana. W innych, mniej poważnych przypadkach, trudno jest o zapewnienie proporcjonalności dostępu do danych dotyczących ruchu i lokalizacji. EIOD wyraża jednak swoje wątpliwości co do wystarczającej precyzyjności tego ograniczenia, szczególnie w przypadku wniosku o umożliwienie dostępu w związku z poważnymi przestępstwami innymi niż terroryzm i przestępczość zorganizowana. Praktyki w poszczególnych Państwach Członkowskich będą się różnić. EIOD podkreślił w sekcji IV niniejszej opinii potrzebę pełnej harmonizacji zasadniczych elementów wniosku. EIOD zaleca więc ograniczenie przepisu do *niektórych* poważnych przestępstw.

55. Po czwarte, w przeciwieństwie do projektu decyzji ramowej omawiany wniosek nie zawiera przepisu dotyczącego dostępu. Zdaniem EIOD dostęp do danych i ich dalsze wykorzystanie nie powinny zosta zignorowane w dyrektywie. Stanowią one nieodłączną część jej podstawowego zagadnienia (patrz: sekcja III niniejszej opinii).

56. EIOD zaleca dodanie do wniosku jednego lub więcej artykułów dotyczących dostępu właściwych organów do danych dotyczących ruchu i lokalizacji oraz dalszego wykorzystania tych danych. Celem tych artykułów powinno być zapewnienie, że dane są wykorzystywane wyłącznie w celach określonych w art. 3 ust. 2 oraz że właściwe organy zapewniają jakość, poufność i bezpieczeństwo uzyskanych przez nie danych, a także że dane zostaną usunięte, gdy przestaną być niezbędne w celu zapobiegania, dochodzenia,

wykrywania i ścigania konkretnego przestępstwa. Ponadto powinno zostać określone, że dostęp w określonych przypadkach powinien być kontrolowany przez organy sądowe Państw Członkowskich.

57. Po piąte, wniosek nie zawiera dodatkowych gwarancji ochrony danych. Motywy odnoszą się po prostu do gwarancji zawartych w istniejącym prawodawstwie, w szczególności w dyrektywach 95/46/WE i 2002/58/WE. EIOD nie zgadza się z tym ograniczonym podejściem do ochrony danych pomimo szczególnej wagi (dodatkowych) gwarancji (zob. sekcja II niniejszej opinii).

58. Dlatego też EIOD zaleca dodanie ustępu poświęconego ochronie danych. Do ustępu tego mogą zostać włączone wcześniejsze zalecenia dotyczące art. 3 ust. 2 oraz inne przepisy dotyczące ochrony danych, takie jak przepisy związane z wykonywaniem swoich praw przez osoby, których dotyczą dane (zob. sekcja II niniejszej opinii), z jakością danych i ich bezpieczeństwem oraz z danymi dotyczącymi ruchu i lokalizacji odnoszącymi się do osób niepodejrzanych o popełnienie przestępstwa.

Artykuł 4: Kategorie danych, które mają być zatrzymywane

59. Ogólnie rzecz biorąc, EIOD z zadowoleniem przyjmuje ten artykuł i załącznik z powodu:

— umieszczenia wybranej techniki legislacyjnej z opisami funkcji w tekście samej dyrektywy, a szczegółów technicznych w załączniku. To rozwiązanie jest wystarczająco elastyczne, by adekwatnie dostosować się do rozwoju technologii, oraz oferuje obywatelom pewność prawną,

— rozróżnienia pomiędzy danymi telekomunikacyjnymi i internetowymi, pomimo faktu, że to rozróżnienie z technologicznego punktu widzenia traci na znaczeniu. Jednak z perspektywy ochrony danych rozróżnienie to jest istotne, gdyż w Internecie granica pomiędzy zawartością informacyjną komunikatu a danymi dotyczącymi ruchu nie jest jednoznaczna (patrz na przykład: uznanie w art. 1 ust. 2 dyrektywy, że informacje konsultowane za pomocą Internetu stanowią zawartość informacyjną komunikatu),

— poziomu harmonizacji: wniosek przewiduje wysoki poziom harmonizacji wraz z wyczerpującym wykazem kategorii danych, które podlegają zatrzymaniu (w przeciwieństwie do projektu decyzji ramowej, który zawiera wykaz minimalny z szerokim marginesem umożliwiającym dodawanie danych przez Państwa Członkowskie). Z perspektywy ochrony danych pełna harmonizacja jest kwestią podstawową (patrz: sekcja IV).

60. EIOD zaleca wprowadzenie następujących poprawek:

— artykuł 4 akapit drugi powinien zawierać bardziej szczegółowe kryteria w celu zapewnienia wyłączenia zawartości informacyjnej komunikatu. Należy dodać następujące zdanie: „Załącznik nie może zawierać danych, które ujawniałyby zawartość komunikatu",

— artykuł 5 otwiera możliwość wprowadzenia zmian do Załącznika za pomocą dyrektywy Komisji („procedura komitologii"). EIOD zauważa, że zmiany do Załącznika mające znaczący wpływ na ochronę danych powinny raczej zostać wprowadzone za pomocą dyrektywy, zgodnie z procedurą współdecydowania ([1]).

Artykuł 7: Okresy zatrzymywania

61. EIOD z zadowoleniem przyjmuje fakt, że okresy zatrzymywania danych we wniosku zostały znacznie skrócone w stosunku do okresów przewidzianych w projekcie decyzji ramowej:

— nie zapominając o wątpliwościach wyrażonych w niniejszej opinii w stosunku do konieczności zatrzymywania danych dotyczących ruchu przez okres do jednego roku, okres jednego roku odzwierciedla praktyki organów ścigania, *jak wskazują* dane przekazane przez Komisję i Prezydencję Rady,

— dane te pokazują również, że, z wyjątkiem szczególnych przypadków, zatrzymywania danych przez okres dłuższy niż jeden rok nie odzwierciedla praktyk organów ścigania,

— krótszy okres wynoszący 6 miesięcy dla danych związanych z łącznością elektroniczną zachodzącą z wykorzystaniem wyłącznie lub przede wszystkim protokołu IP jest istotny z punktu widzenia ochrony danych, gdyż zatrzymywanie komunikatów internetowych prowadzi do tworzenia ogromnych baz danych (data te zwykle nie są zatrzymywane do celów naliczania płatności), granica oddzielająca je od zawartości informacyjnej komunikatu jest niejednoznaczna, a zatrzymywanie przez okres dłuższy niż 6 miesięcy nie odzwierciedla praktyk organów ścigania.

62. W tekście należy umieścić wyjaśnienie, że:

— odpowiednio 6 miesięcy i jeden rok stanowią maksymalne okresy zatrzymywania danych,

([1]) Patrz: opinia EIOD z dnia 23 marca 2005 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Systemu Informacji Wizowej (VIS) oraz wymiany danych pomiędzy Państwami Członkowskimi na temat wiz krótkoterminowych (pkt 3.12).

— dane są usuwane na koniec okresu zatrzymania. Tekst powinien również jasno określać sposób usuwania danych. Zdaniem EIOD dostawca usług musi usunąć dane za pomocą środków automatycznych, przynajmniej w codziennej praktyce.

Artykuł 8: Wymagania dotyczące przechowywania zatrzymanych danych

63. Ten artykuł jest ściśle związany z art. 3 ust. 2 i zawiera istotny przepis mogący zapewnić, że dostęp w szczególnych przypadkach może zostać ograniczony wyłącznie do danych, które są niezbędne w danej sytuacji. Artykuły 8 i 3 ust. 2 zakładają, że wymagane dane są przekazywane przez dostawców usług właściwym organom i że organy te nie mają bezpośredniego dostępu do baz danych. EIOD zaleca jasne włączenie tego założenia do tekstu.

64. Przepis powinien zostać uszczegółowiony poprzez włączenie informacji, że:

— wymagane dane są przekazywane przez dostawców usług właściwym organom (patrz: pkt 63),

— dostawcy usług powinni zainstalować niezbędne wyposażenie techniczne, w tym wyszukiwarki, w celu ułatwienia ukierunkowanego dostępu do określonych danych,

— dostawcy usług powinni zapewnić, że wyłącznie członkowie ich personelu o określonych kompetencjach technicznych mają dostęp do baz danych z przyczyn technicznych oraz że ci członkowie personelu są świadomi wrażliwego charakteru danych i pracują zgodnie ze ścisłymi wewnętrznymi zasadami poufności,

— przesyłanie danych powinno zachodzić nie tylko bez nieuzasadnionych opóźnień, ale także bez ujawniania innych danych dotyczących ruchu i lokalizacji niż dane niezbędne do spełnienia wnioskowanych celów.

Artykuł 9: Statystyka

65. Zobowiązanie dostawców usług do corocznego przekazywania danych statystycznych pomaga instytucjom Wspólnoty w monitorowaniu skuteczności wdrażania i stosowania omawianego wniosku. Niezbędne są adekwatne dane.

66. Zdaniem EIOD zobowiązanie to realizuje zasadę przejrzystości. Obywatele Europy mają prawo wiedzieć, jak skuteczne jest zatrzymywanie danych. Z tego powodu dostawca usług powinien dodatkowo zostać zobowiązany do przechowywania list logowania oraz do przeprowadzania systematycznych audytów własnych umożliwiających kontrolę stosowania w praktyce zasad ochrony danych ([1]) krajowym organom ochrony danych. Do omawianego wniosku należy więc wprowadzić odpowiednie poprawki.

Artykuł 10: Koszty

67. Jak wspomniano wcześniej w sekcji II, istnieje bezpośredni związek pomiędzy adekwatnością środków bezpieczeństwa a ich kosztami, inaczej mówiąc – pomiędzy bezpieczeństwem i kosztami. Dlatego EIOD uznaje art. 10, przewidujący zwrot dowiedzionych dodatkowych kosztów, za istotny przepis, który mógłby służyć jako zachęta do inwestowania w infrastrukturę techniczną przez dostawców usług.

68. Zgodnie z danymi szacunkowymi dotyczącymi oceny oddziaływania przekazanymi EIOD przez Komisję koszty zatrzymywania danych są znaczne. Dla dużej sieci i dostawcy usług koszty tę wyniosłyby ponad 150 mln EUR w rocznym okresie zatrzymania, podczas gdy roczne koszty eksploatacyjne wynoszą ok. 50 mln EUR ([2]). Nie podano jednak danych o kosztach dodatkowych środków bezpieczeństwa takich jak drogie wyszukiwarki (patrz: komentarz do art. 6), ani też o (szacunkowych) skutkach finansowych pełnego zwrotu dodatkowych kosztów poniesionych przez dostawców usług.

69. Zdaniem EIOD niezbędne są dokładniejsze dane, by móc ocenić wniosek w całej jego rozciągłości. EIOD sugeruje wyjaśnienie skutków finansowych wniosku w memorandum wyjaśniającym.

70. Co do przepisów samego art. 10, związek pomiędzy adekwatnością środków bezpieczeństwa a ich kosztami powinien zostać wyjaśniony w tekście artykułu. Ponadto wniosek powinien przedstawiać minimalne standardy środków bezpieczeństwa, jakie powinni przyjąć dostawcy usług, by kwalifikować się do zwrotu kosztów przez Państwo Członkowskie. Zdaniem EIOD ustalenie tych standardów nie

([1]) Patrz: opinia EIOD z dnia 23 marca 2005 r.w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Systemu Informacji Wizowej (VIS) oraz wymiany danych pomiędzy Państwami Członkowskimi na temat wiz krótkoterminowych (pkt 3.9).

([2]) Komisja odwołuje się do danych podanych przez ETNO (European Telecommunications Network Operators' Association) oraz sprawozdania posła do Parlamentu Europejskiego A. Alvaro dotyczącego projektu decyzji ramowej.

powinno leżeć całkowicie w gestii Państw Członkowskich. Mogłoby to wpłynąć negatywnie na poziom harmonizacji przewidziany dyrektywą. Ponadto należy uwzględnić fakt, że Państwa Członkowskie ponoszą finansowe konsekwencje takich zwrotów.

Artykuł 11: Zmiana dyrektywy 2002/58/WE

71. Należy wyjaśnić związek z art. 15 ust. 1 dyrektywy 2002/58/WE, gdyż omawiany wniosek pozbawia ten przepis większej części jego zawartości. Odniesienia do art. 6 i 9 (tej samej dyrektywy) umieszczone w art. 15 ust. 1 dyrektywy 2002/58/WE należy skreślić lub przynajmniej zmodyfikować w celu wyjaśnienia, że Państwa Członkowskie nie posiadają już kompetencji pozwalającej na przyjmowanie aktów prawnych związanych z przestępstwami, innych niż omawiany wniosek. Wszelka niejednoznaczność ich pozostałych kompetencji, na przykład dotyczących zatrzymywania danych do celów ścigania „mniej poważnych" przestępstw, musi zostać usunięta.

Artykuł 12: Ocena

72. EIOD przyjmuje z zadowoleniem fakt, że omawiany wniosek zawiera artykuł dotyczący oceny dyrektywy w terminie trzech lat od jej wejścia w życie. Ocena taka staje się jeszcze bardziej istotna w obliczu wątpliwości dotyczących samego wniosku oraz jego proporcjonalności.

73. Z tego punktu widzenia EIOD radzi wprowadzenie jeszcze ściślejszych zobowiązań zawierających następujące elementy:

— ocena powinna obejmować ocenę skuteczności wdrażania dyrektywy z perspektywy organów ścigania oraz ocenę oddziaływania na podstawowe prawa osób, których dotyczą zatrzymywane dane. Komisja powinna przedstawić wszelkie dowody, które mogłyby wpłynąć na wyniki oceny,

— ocena powinna się odbywać regularnie (co najmniej raz na dwa lata),

— Komisja powinna zostać zobowiązana do zgłaszania poprawek do wniosku w uzasadnionych przypadkach (podobnie jak w art. 18 dyrektywy 2002/58/WE).

VI. **Wnioski**

Warunki wstępne

74. Sprawą podstawową dla EIOD jest poszanowanie we wniosku praw podstawowych. Środek legislacyjny naruszający ochronę zagwarantowaną w prawie wspólnotowym, a w szczególności w orzecznictwie Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka, jest nie tylko niemożliwy do przyjęcia, ale także niezgodny z prawem.

75. Musi zostać dowiedziona konieczność i proporcjonalność obowiązkowego zatrzymywania danych w pełnym zakresie.

76. W odniesieniu do konieczności: EIOD uznaje zmianę warunków, ale jak dotąd nie jest przekonany co do konieczności zatrzymywania danych dotyczących ruchu i lokalizacji do celów ścigania przestępstw, którą stwierdza tekst omawianego wniosku.

77. EIOD przedstawia jednak w niniejszej opinii swoje poglądy na temat proporcjonalności wniosku. Przede wszystkim, zatrzymywanie danych dotyczących ruchu i lokalizacji samo w sobie nie stanowi adekwatnej ani skutecznej odpowiedzi. Potrzebne są dodatkowe środki w celu zapewnienia władzom ukierunkowanego i szybkiego dostępu do danych potrzebnych w danym dochodzeniu. Po drugie, wniosek powinien:

— ograniczyć okresy zatrzymywania danych. Okresy te muszą odpowiadać udokumentowanym potrzebom organów ścigania,

— ograniczyć ilość danych, które mają być przechowywane. Ilość ta musi odpowiadać potrzebom organów ścigania oraz należy uniemożliwić dostęp do zawartości informacyjnej komunikatu,

— zawierać adekwatne środki bezpieczeństwa.

Całościowa ocena wniosku

78. EIOD podkreśla wagę tego, że omawiany tekst wniosku przewiduje pełną harmonizację jego głównych elementów, w szczególności rodzajów danych, jakie mają być zatrzymywane, okresów zatrzymania danych oraz (celów) dostępu do danych i ich dalszego wykorzystania.

79. W odniesieniu do niektórych zagadnień niezbędne są dalsze wyjaśnienia, na przykład w celu zapewnienia odpowiedniego usuwania danych na koniec okresu zatrzymania lub skutecznego zapobiegania dostępowi do danych i ich dalszemu wykorzystaniu przez różne grupy zainteresowanych podmiotów.

80. By wniosek był do przyjęcia z perspektywy ochrony danych, EIOD uważa za fundamentalne następujące kwestie:

— dodanie do wniosku szczegółowych przepisów dotyczących dostępu właściwych organów do danych dotyczących ruchu i lokalizacji oraz dalszego wykorzystania tych danych jako podstawowej i nierozdzielnej części podstawowego zagadnienia,

— dodanie do wniosku dalszych dodatkowych gwarancji ochrony danych (w przeciwieństwie do prostego odniesienie do gwarancji zawartych w istniejącym prawodawstwie, a w szczególności w dyrektywach 95/46/EC i 2002/58/EC), między innymi w celu zapewnienia wykonania praw osób, których dotyczą dane,

— dodanie do wniosku dalszych bodźców zachęcających dostawców usług do inwestowania w odpowiednią infrastrukturę techniczną, w tym bodźców finansowych. Ta infrastruktura może być odpowiednia wyłącznie pod warunkiem istnienia skutecznych wyszukiwarek.

Zalecenia dotyczące modyfikacji wniosku

81. W odniesieniu do art. 3 ust. 2:

— dodanie przepisu zapewniającego, że osoby inne niż właściwe organy nie mają dostępu do danych. Przepis ten może mieć następujące brzmienie: „dostęp do danych lub ich przetwarzanie jest możliwe wyłącznie w celach określonych w art. 3 ust. 2" lub „dostawcy usług skutecznie zapewniają możliwość dostępu wyłącznie właściwym organom",

— jasne wskazanie, że dane mogą być udostępnione wyłącznie w związku z określonym przestępstwem,

— ograniczenie przepisu do *niektórych* poważnych przestępstw,

— dodanie do wniosku jednego lub więcej artykułów dotyczących dostępu właściwych organów do danych dotyczących ruchu i lokalizacji oraz dalszego wykorzystania tych danych, a także przepisu określającego, że dostęp w określonych przypadkach powinien być kontrolowany przez organy sądowe Państw Członkowskich,

— dodanie ustępu poświęconego ochronie danych.

82. W odniesieniu do art. 4 i 5:

— dodanie do art. 4 akapit drugi następującego zdania: „Załącznik nie może zawierać danych, które ujawniałyby zawartość komunikatu",

— jasne wskazanie, że zmiany do Załącznika mające znaczący wpływ na ochronę danych, powinny zostać wprowadzone za pomocą dyrektywy, zgodnie z procedurą współdecydowania.

83. W odniesieniu do art. 7 jasne określenie w tekście, że:

— odpowiednio 6 miesięcy i jeden rok stanowią maksymalne okresy zatrzymywania danych,

— dane są usuwane na koniec okresu zatrzymania. Tekst powinien również wyjaśniać sposób usuwania danych, to znaczy przez dostawcę usług za pomocą środków automatycznych, przynajmniej w codziennej praktyce.

84. W odniesieniu do art. 8 jasne określenie w tekście, że:

— wymagane dane są przekazywane przez dostawców usług właściwym organom,

— dostawcy usług powinni zainstalować niezbędne wyposażenie techniczne, w tym wyszukiwarki, w celu ułatwienia ukierunkowanego dostępu do określonych danych,

— dostawcy usług powinni zapewnić, że wyłącznie członkowie ich personelu o określonych kompetencjach technicznych mają dostęp do baz danych z przyczyn technicznych oraz że ci członkowie personelu są świadomi wrażliwego charakteru danych i pracują zgodnie ze ścisłymi wewnętrznymi zasadami poufności,

— przesyłanie danych powinno zachodzić nie tylko bez nieuzasadnionych opóźnień, ale także bez ujawniania innych danych dotyczących ruchu i lokalizacji niż dane niezbędne do spełnienia celów określonych we wniosku.

85. W odniesieniu do art. 9:

— dodanie przepisu zobowiązującego dostawcę usług do przechowywania list logowania oraz do przeprowadzania systematycznych audytów własnych umożliwiających kontrolę stosowania w praktyce zasad ochrony danych krajowym organom ochrony danych.

86. W odniesieniu do art. 10:

— związek pomiędzy adekwatnością środków bezpieczeństwa a ich kosztami powinien zostać wyjaśniony w tekście przepisu,

— dodanie minimalnych standardów środków bezpieczeństwa, jakie powinni przyjąć dostawcy usług, by kwalifikować się do zwrotu kosztów przez Państwo Członkowskie,

— wyjaśnienie skutków finansowych wniosku w memorandum wyjaśniającym.

87. W odniesieniu do art. 11:

— wprowadzenie zmiany do art. 15 ust. 1 dyrektywy 2002/58/WE w celu skreślenia odniesień do art. 6 i 9 (tej samej dyrektywy) lub przynajmniej zmodyfikowania tych odniesień w celu wyjaśnienia, że Państwa Członkowskie nie posiadają już kompetencji pozwalającej na przyjmowanie aktów prawnych związanych z przestępstwami, innych niż omawiany wniosek.

88. W odniesieniu do art. 12, wprowadzenie poprawki do przepisu dotyczącego oceny:

— powinien on zawierać ocenę skuteczności wdrażania dyrektywy,

— ocena powinna się odbywać regularnie (co najmniej raz na dwa lata),

— Komisja powinna zostać zobowiązana do zgłaszania poprawek do wniosku w uzasadnionych przypadkach (podobnie jak w art. 18 dyrektywy 2002/58/WE).

Sporządzono w Brukseli dnia 26 września 2005 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych