I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady zmieniającej m.in. dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)

(2008/C 181/01)

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]),

uwzględniając 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 ([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, w szczególności jego art. 41 ([3]),

uwzględniając wniosek o wydanie opinii zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001, otrzymany od Komisji Europejskiej w dniu 16 listopada 2007 r.,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. **WPROWADZENIE**

1. W dniu 13 listopada 2007 r. Komisja przyjęła wniosek dotyczący dyrektywy zmieniającej, m.in. dyrektywę 2002/58/WE dotyczącą przetwarzania danych i ochrony prywatności w sektorze łączności elektronicznej (dalej zwany „wnioskiem" lub „proponowanymi zmianami"). Obowiązująca wersja dyrektywy 2002/58/WE jest zwykle, również w niniejszej opinii, zwana dyrektywą o prywatności i łączności elektronicznej.

([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.

2. Wniosek ma na celu poprawienie ochrony prywatności osób fizycznych i ich danych osobowych w sektorze łączności elektronicznej. Dokonuje się tego nie poprzez nadanie zupełnie nowego kształtu obowiązującej dyrektywie o prywatności i łączności elektronicznej, lecz przez zaproponowanie doraźnych zmian, które służą przede wszystkim wzmocnieniu przepisów dotyczących bezpieczeństwa i poprawieniu mechanizmów ich egzekwowania.

3. Wniosek jest częścią szerzej zakrojonej reformy pięciu unijnych dyrektyw telekomunikacyjnych („pakietu telekomunikacyjnego"). Oprócz wniosków dotyczących przeglądu „pakietu telekomunikacyjnego" ([1]) Komisja przyjęła również w tym samym czasie wniosek dotyczący rozporządzenia ustanawiającego Europejski Urząd ds. Rynku Łączności Elektronicznej ([2]).

4. Uwagi zawarte w niniejszej opinii ograniczają się do proponowanych zmian do dyrektywy o prywatności i łączności elektronicznej, chyba że takie proponowane zmiany odwołują się do pojęć lub przepisów zawartych we wnioskach dotyczących przeglądu pakietu telekomunikacyjnego. Niektóre z uwag zawartych w niniejszej opinii odnoszą się ponadto do przepisów dyrektywy o prywatności i łączności elektronicznej, które w myśl wniosku nie zostaną zmienione.

5. W niniejszej opinii poruszane są następujące kwestie: (i) zakres zastosowania dyrektywy o prywatności i łączności elektronicznej, w szczególności, usługi, których ma ona dotyczyć (proponowana zmiana do art. 3 ust. 1); (ii) powiadamianie o przypadkach naruszenia bezpieczeństwa (proponowana zmiana wprowadzająca art. 4 ust. 3 i ust. 4); (iii) przepisy dotyczące plików *cookie*, oprogramowania szpiegującego i podobnych urządzeń (proponowana zmiana w art. 5 ust. 3); (iv) występowanie na drogę sądową przez dostawców usług łączności elektronicznej i inne osoby prawne (proponowana zmiana wprowadzająca art. 13 ust. 6) oraz (v) usprawnienie egzekwowania przepisów (proponowana zmiana wprowadzająca art. 15a).

Zasięgnięcie opinii EIOD-a i szersze konsultacje publiczne

6. Komisja przesłała EIOD-owi wniosek w dniu 16 listopada 2007 r. EIOD sądzi, że przekazanie tego wniosku oznacza prośbę o doradzenie wspólnotowym instytucjom i organom, zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (zwanego dalej „rozporządzeniem (WE) nr 45/2001").

7. Przed przyjęciem wniosku Komisja nieformalnie zwróciła się do EIOD-a o wydanie opinii na temat projektu wniosku; EIOD przychylnie odniósł się do tego działania, ponieważ dało mu to sposobność poczynienia pewnych sugestii dotyczących projektu wniosku, zanim został on przyjęty przez Komisję. EIOD cieszy się, że niektóre z tych sugestii zostały uwzględnione we wniosku.

8. Przyjęcie wniosku poprzedziły szeroko zakrojone konsultacje publiczne, praktyka ceniona przez EIOD-a. W czerwcu 2006 roku Komisja zapoczątkowała konsultacje publiczne w sprawie swojego komunikatu dotyczącego przeglądu pakietu telekomunikacyjnego, w którym Komisja przedstawiła swój pogląd na sytuację i przedstawiła propozycje zmian ([3]). Grupa Robocza ds. Ochrony Danych powołana na mocy art. 29 („GR 29"), której członkiem jest EIOD, skorzystała z tej sposobności, by w opinii przyjętej w dniu 26 września 2006 r. ([4]) wyrazić swoje poglądy na temat proponowanych zmian.

([1]) Proponowane zmiany do dyrektyw telekomunikacyjnych są przedstawione w następujących wnioskach: (i) wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywy: 2002/21/WE w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej, 2002/19/WE w sprawie dostępu do sieci łączności elektronicznej oraz wzajemnych połączeń i 2002/20/WE w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej, 13 listopada 2007 r., COM(2007) 697 wersja ostateczna; (ii) wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników oraz dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy w dziedzinie ochrony konsumentów, 13 listopada 2007 r., COM(2007) 698 wersja ostateczna.

([2]) Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego Europejski Urząd ds. Rynku Łączności Elektronicznej, 13 listopada 2007 r., COM(2007) 699 wersja ostateczna.

([3]) Komunikat w sprawie ram regulacyjnych UE dotyczących sieci i usług łączności elektronicznej (SEC(2006) 816) przyjęty w dniu 29 czerwca 2006 r. Komunikatowi towarzyszył dokument roboczy służb Komisji — (COM(206) 334 wersja ostateczna).

([4]) Opinia 8/2006 na temat przeglądu ram regulacyjnych dla łączności i usług elektronicznych, z naciskiem na dyrektywę o prywatności i łączności elektronicznej, przyjęta w dniu 26 września 2006 r.

Ogólna opinia EIOD-a

9. Ogólnie rzecz biorąc, EIOD pozytywnie postrzega wniosek. W pełni popiera cele, do osiągnięcia których dążyła Komisja, przyjmując wniosek zwiększający ochronę prywatności osób fizycznych i danych osobowych w sektorze łączności elektronicznej. Szczególne zadowolenie EIOD-a wzbudza propozycja istnienia systemu obowiązkowego powiadamiania o przypadkach naruszenia bezpieczeństwa (zmiana do art. 4 dyrektywy o prywatności i łączności elektronicznej, wprowadzająca ust. 3 i 4). Gdy dochodzi do naruszenia bezpieczeństwa danych, powiadamianie o tym fakcie wiąże się z wyraźnymi korzyściami, wzmacnia odpowiedzialność organizacji, sprawia, że firmy wdrażają rygorystyczne środki bezpieczeństwa i umożliwia stwierdzenie, przy użyciu jakich technologii najlepiej można chronić informacje. Poza tym daje poszkodowanym osobom fizycznym możliwość podjęcia kroków, które pozwolą im uchronić się przed kradzieżą tożsamości lub innym niezgodnym z prawem wykorzystaniem dotyczących ich informacji osobowych.

10. EIOD z zadowoleniem odnosi się do innych zmian zaproponowanych we wniosku, np. zadbania o to, by każda osoba prawna mająca uzasadniony interes mogła wystąpić na drogę sądową przeciwko osobom, które naruszają niektóre z przepisów dyrektywy o prywatności i łączności elektronicznej (zmiana do art. 13, wprowadzająca ust. 6). Pozytywnie należy również postrzegać wzmocnienie uprawnień do prowadzenia dochodzeń, którymi dysponują krajowe organy regulacyjne, ponieważ umożliwi im to ocenę, czy dany przypadek przetwarzania danych ma miejsce zgodnie z prawem, i pozwoli wskazać naruszenia (dodany art. 15a ust. 3). Posiadanie przez nie uprawnień do jak najszybszego powstrzymania niezgodnego z prawem przetwarzania danych osobowych i naruszeń prywatności, jest konieczne, by chronić prawa i swobody osób fizycznych. Z tego względu z dużym zadowoleniem przyjmuje się proponowany art. 15a ust. 2, który uznaje uprawnienia krajowych organów regulacyjnych do doprowadzenia do zaprzestania naruszeń, ponieważ umożliwi im on natychmiastowe powstrzymanie poważnych przepadków niezgodnego z prawem przetwarzania danych.

11. Podejście, którego wyrazem jest wniosek i większość proponowanych w nim zmian, jest zgodne z poglądami na temat planowanej polityki w zakresie ochrony danych, które przedstawione zostały we wcześniejszych opiniach EIOD-a, takich jak opinia w sprawie wdrażania dyrektywy o ochronie danych ([1]). Podejście opiera się m.in. na poglądzie, że choć nie są konieczne żadne nowe zasady ochrony danych, potrzeba bardziej precyzyjnych przepisów, by zaradzić problemom związanym z ochroną danych, które powstały wskutek pojawienia się nowych technologii, takich jak Internet, identyfikacja radiowa itp., a także narzędzi, które pomagają egzekwować i uczynić skutecznym ustawodawstwo w zakresie ochrony danych, takie jak narzędzie umożliwiające podmiotom prawnym wszczynanie działań, gdy nastąpiło naruszenie ochrony danych, lub zobowiązujące kontrolerów danych do powiadamiania o przypadkach naruszenia bezpieczeństwa.

12. Ogólnie rzecz biorąc, wniosek ma pozytywny wydźwięk, EIOD wyraża jednak żal, że nie idzie on tak daleko, jak byłoby to możliwe. Już bowiem od 2003 roku ze stosowania przepisów zawartych w dyrektywie o prywatności i łączności elektronicznej, a także z uważnej analizy przedmiotu możliwe było wysnucie wniosku, że niektórym z jej przepisów daleko do bycia klarownymi, co powoduje niepewność prawną i problemy z ich przestrzeganiem. Tak jest np. jeśli chodzi o stopień, w jakim wspomniana dyrektywa dotyczy półpublicznych dostawców usług łączności. Można było mieć nadzieję, że Komisja wykorzysta przegląd pakietu telekomunikacyjnego, a w szczególności przegląd dyrektywy o prywatności i łączności elektronicznej, by rozwiązać niektóre z tych wciąż istniejących problemów. Poza tym zajmując się nowymi kwestiami, jak choćby ustanowieniem systemu obowiązkowego powiadamiania o naruszeniach bezpieczeństwa, wniosek proponuje tylko częściowe rozwiązanie, gdyż w zakres organizacji zobowiązanych do powiadamiania o przypadkach naruszeń bezpieczeństwa nie zostały włączone podmioty, które przetwarzają wyjątkowo sensytywne dane, takie jak banki internetowe czy podmioty świadczące elektroniczne usługi opieki zdrowotnej. EIOD z żalem przyjmuje takie podejście.

13. EIOD wyraża nadzieję, że w procesie legislacyjnym prawodawca uwzględni uwagi i propozycje zawarte w niniejszej opinii, tak by zaradzić problemom, którymi nie zajmuje się wniosek Komisji.

([1]) Opinia Europejskiego Inspektora Ochrony Danych z dnia 25 lipca 2007 r. w sprawie komunikatu Komisji dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych (Dz.U. C 255 z 27.10.2007, str. 1).

II. ANALIZA WNIOSKU

II.1. Zakres zastosowania dyrektywy o prywatności i łączności elektronicznej, w szczególności usługi, które są nim objęte

14. Zasadniczym zagadnieniem, jeśli chodzi o obecną dyrektywę o prywatności i łączności elektronicznej, jest zakres jej zastosowania. Wniosek zawiera pewne konstruktywne elementy pomocne w zdefiniowaniu i wyjaśnieniu zakresu dyrektywy, w szczególności w odniesieniu do usług nią objętych, które omówiono poniżej w części (i). Niestety, proponowane zmiany nie rozwiązują wszystkich istniejących problemów. Jak wspomniano w części (ii) poniżej, zmiany niestety nie mają na celu poszerzenia zakresu zastosowania dyrektywy na usługi łączności elektronicznej w sieciach prywatnych.

15. W art. 3 dyrektywy o prywatności i łączności elektronicznej podano opis usług, których ona dotyczy, innymi słowy usług, do których zastosowanie mają wymogi przedstawione w dyrektywie: „niniejszą dyrektywę stosuje się do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności".

16. Zatem dyrektywę tę stosuje się do usług świadczonych przez dostawców publicznie dostępnych usług łączności elektronicznej w sieciach publicznych (ang. „PPECS"). Definicja usługi PPECS podana została w art. 2 lit. c) dyrektywy ramowej ([1]). Definicję publicznych sieci łączności podano w art. 2 lit. d) tej dyrektywy ramowej ([2]). Przykładami działań w ramach usługi PPECS są: dostarczanie dostępu do Internetu, przesyłanie informacji poprzez sieci elektroniczne, połączenia telefonii mobilnej i stacjonarnej itp.

(i) *Proponowana zmiana w art. 3 dyrektywy o prywatności i łączności elektronicznej: „Usługi wchodzące w zakres zastosowania dyrektywy mają obejmować sieci łączności służące do zbierania danych i obsługi urządzeń identyfikacyjnych"*

17. Wniosek wprowadza zmianę w art. 3 dyrektywy o prywatności i łączności elektronicznej i precyzuje, że publiczne sieci łączności obejmują „publiczne sieci łączności służące do zbierania danych i obsługi urządzeń identyfikacyjnych". W motywie 28 wyjaśniono, że rozwój urządzeń do zbierania informacji, w tym danych osobowych, wykorzystujących częstotliwości radiowe, w tym urządzeń do identyfikacji radiowej (RFID), musi podlegać dyrektywie o prywatności i łączności elektronicznej, jeśli urządzenia te są podłączone do publicznych sieci łączności elektronicznej lub korzystają z publicznie dostępnych usług łączności elektronicznej.

18. EIOD pozytywnie ocenia ten przepis, ponieważ wyjaśniono w nim, że pewne zastosowania urządzeń RFID wchodzą w zakres zastosowania dyrektywy o prywatności i łączności elektronicznej, a tym samym rozwiano pewne wątpliwości co do tej kwestii i ostatecznie usunięto przyczynę niewłaściwego rozumienia lub nieprawidłowej wykładni przepisów prawa.

19. Na mocy art. 3 dyrektywy o prywatności i łączności elektronicznej, w jego obecnym brzmieniu, pewne zastosowania urządzeń RFID są już objęte zakresem tej dyrektywy. Dzieje się tak z wielu łączących się ze sobą przyczyn. Po pierwsze, ponieważ stosowanie urządzeń RFID wchodzi w zakres definicji usług łączności elektronicznej. Po drugie, ponieważ odbywa się ono przy użyciu sieci łączności elektronicznej, jako że działanie tych urządzeń opiera się na systemie transmisji, który bezprzewodowo

([1]) Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (Dz.U. L 108 z 24.4.2002, str. 33). Ta dyrektywa ramowa określa, co należy rozumieć pod pojęciem usługi łączności elektronicznej, a mianowicie: (i) usługa łączności elektronicznej to usługa zwykle świadczona odpłatnie, która polega na przekazywaniu sygnałów w sieciach i obejmuje usługi telekomunikacyjne i usługi transmisyjne świadczone poprzez sieci; (ii) z definicji usług łączności elektronicznej wyłączone są usługi związane z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci lub usług łączności elektronicznej; (iii) świadczenie usług oznacza ustanowienie, obsługę, kontrolowanie i udostępnianie sieci; (iv) usługi łączności elektronicznej nie obejmują usług społeczeństwa informacyjnego, za które w dyrektywie o handlu elektronicznym uznaje się usługi zwykle świadczone odpłatnie, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług.

([2]) „Publiczna sieć łączności" oznacza sieć łączności elektronicznej wykorzystywaną całkowicie lub częściowo do świadczenia publicznie dostępnych usług łączności elektronicznej.

przekazuje sygnały. I wreszcie, sieć ta może być zarówno publiczna, jak i prywatna. Jeśli jest publiczna, stosowanie urządzeń RFID zostanie uznane za „usługi, których dyrektywa dotyczy", i tym samym wejdzie w zakres zastosowania dyrektywy o prywatności i łączności elektronicznej. Jednak proponowana zmiana usunie utrzymujące się wątpliwości co do tej kwestii i zagwarantuje większą pewność prawną.

20. Oczywiście, jak już wspomniano we wcześniejszej opinii EIOD-a na temat urządzeń RFID ([1]), przepis ten nie wyklucza, że konieczne będzie wprowadzenie dodatkowych aktów prawnych w odniesieniu do tych urządzeń. Takie jednak środki należy przyjąć przy innej okazji, nie jako część omawianego wniosku.

(ii) *Potrzeba uwzględnienia usług łączności elektronicznej w sieciach prywatnych lub półprywatnych*

21. EIOD cieszy się z wyjaśnienia kwestii przedstawionej powyżej, żałuje jednak, że we wniosku nie zajęto się kwestią coraz mniej wyraźnej granicy między sieciami prywatnymi i publicznymi. EIOD wyraża też żal, że nie poszerzono zakresu definicji usług objętych dyrektywą o prywatności i łączności elektronicznej, by dotyczyła ona również prywatnych sieci. W swoim obecnym brzmieniu art. 3 ust. 1 dyrektywy o prywatności i łączności elektronicznej dotyczy wyłącznie *usług łączności elektronicznej w publicznych sieciach łączności*.

22. EIOD zauważa tendencję, że usługi coraz częściej stają się kombinacją usług prywatnych i publicznych. Weźmy choćby uniwersytety, które umożliwiają tysiącom swoich studentów korzystanie z Internetu i poczty elektronicznej. Oczywiste jest, że te półpubliczne (lub półprywatne) sieci mają możliwość naruszenia prywatności osób fizycznych, i dlatego tego typu usługi także powinny podlegać tym samym przepisom, które stosuje się do wyłącznie publicznych sieci. Ponadto prywatne sieci, jak sieci pracodawców umożliwiających pracownikom dostęp do Internetu, sieci hoteli i właścicieli mieszkań, których goście mogą korzystać z telefonu i poczty elektronicznej, a także sieci wykorzystywane przez kafejki internetowe mają wpływ na ochronę danych i prywatności ich użytkowników, z czego wynika, że również powinny zostać objęte zakresem zastosowania dyrektywy o prywatności i łączności elektronicznej.

23. W rzeczywistości w niektórych państwach członkowskich zapadały już orzeczenia stwierdzające, że usługi łączności elektronicznej świadczone w sieciach prywatnych podlegają tym samym wymogom co usługi w sieciach publicznych ([2]). Na mocy niemieckich przepisów organy ochrony danych uznały również, że umożliwianie pracownikom korzystania z prywatnego konta poczty elektronicznej w danym przedsiębiorstwie może spowodować, że przedsiębiorstwo to zostanie uznane za operatora publicznych usług telekomunikacyjnych, a zatem wejdzie w zakres przepisów dyrektywy o prywatności i łączności elektronicznej.

24. W skrócie — rosnące znaczenie mieszanych (prywatno-publicznych) i prywatnych sieci w codziennym życiu, a co za tym idzie rosnące zagrożenie dla danych osobowych i prywatności, uzasadnia potrzebę stosowania do takich usług tych samych zasad, które obowiązują publiczne usługi łączności elektronicznej. Z tego względu EIOD uważa, że dyrektywę należy zmienić tak, by zakresem jej zastosowania zostały objęte tego typu usługi prywatne; pogląd ten podziela grupa robocza ([3]).

II.2. **Powiadamianie o przypadkach naruszenia bezpieczeństwa: zmiana do art. 4**

25. Artykuł 4 dyrektywy o prywatności i łączności elektronicznej zmieniono, dodając dwa nowe ustępy (3 i 4), które wprowadzają obowiązek powiadamiania o przypadkach naruszenia bezpieczeństwa. Zgodnie z art. 4 ust. 3 dostawcy publicznie dostępnych usług łączności elektronicznej w sieciach publicznych są zobowiązani z jednej strony bez zbędnej zwłoki powiadamiać krajowe organy regulacyjne o każdym przypadku naruszenia bezpieczeństwa, które prowadzi do przypadkowego lub bezprawnego zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych przekazywanych, przechowywanych lub przetwarzanych w inny sposób w związku ze świadczeniem publicznie dostępnych usług łączności (które to naruszenie jest ogólnie nazywane „narażeniem danych"); z drugiej strony dostawcy ci mają również obowiązek powiadomić swoich abonentów.

([1]) Opinia Europejskiego Inspektora Ochrony Danych z dnia 20 grudnia 2007 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie „Identyfikacji radiowej (RFID) w Europie: w stronę ram polityki", COM(2007) 96.

([2]) Na przykład w wyroku paryskiego Sądu Apelacyjnego, który zapadł 4 lutego 2005 r. w sprawie *BNP Paribas* przeciwko *World Press Online*, stwierdza się, że nie ma różnicy między dostawcami usługi internetowej, którzy komercyjnie oferują dostęp do Internetu, a pracodawcami, którzy umożliwiają dostęp do Internetu swojemu personelowi.

([3]) Opinia 8/2006 na temat przeglądu ram regulacyjnych dla łączności i usług elektronicznych, z naciskiem na dyrektywę o prywatności i łączności elektronicznej, przyjęta w dniu 26 września 2006 r.

Korzyści płynące z wprowadzenia takiego obowiązku

26. EIOD z zadowoleniem przyjmuje przepisy art. 4 ust. 3 i 4, które wprowadzają obowiązek powiadamiania o przypadkach naruszenia bezpieczeństwa. Powiadamianie o takich przypadkach ma pozytywne skutki, jeśli chodzi o ochronę danych osobowych i prywatności, co już przetestowano w Stanach Zjednoczonych, gdzie przepisy dotyczące powiadamiania o przypadkach naruszenia obowiązują już od wielu lat na poziomie poszczególnych stanów.

27. Po pierwsze, przepisy dotyczące powiadamiania o przypadkach naruszeń wpływają na zwiększenie odpowiedzialności dostawców PPECS za informacje, które zostały narażone. Na mocy regulacji dotyczących ochrony danych lub prywatności odpowiedzialność oznacza, że każda organizacja jest odpowiedzialna za informacje, które znajdują się pod jej opieką i kontrolą. Obowiązek powiadamiania jest równoznaczny z ponownym stwierdzeniem, że z jednej strony dane, które zostały narażone, były pod kontrolą danego dostawcy PPECS, a z drugiej strony że na organizacji tej ciąży odpowiedzialność za przedsięwzięcie niezbędnych działań w stosunku do takich danych.

28. Po drugie, istnienie obowiązku powiadamiania o naruszeniu bezpieczeństwa okazało się czynnikiem, który prowadzi do inwestycji w systemy bezpieczeństwa podejmowanych przez organizacje, które przetwarzają dane osobowe. Już sam wymóg publicznego powiadamiania o przypadkach naruszenia bezpieczeństwa powoduje, że organizacje stosują bardziej rygorystyczne normy bezpieczeństwa, służące ochronie informacji osobowych i zapobieżeniu naruszeniom. Ponadto powiadamianie o przypadkach naruszenia bezpieczeństwa pomoże zidentyfikować i przeprowadzić wiarygodną analizę statystyczną dotyczącą najskuteczniejszych rozwiązań i mechanizmów w zakresie bezpieczeństwa. Przez długi czas brakowało twardych danych na temat przypadków niedostatecznego zabezpieczania danych i najstosowniejszych technologii służących ochronie informacji. Problem ten ma szansę zostać rozwiązany dzięki nałożeniu obowiązków w zakresie powiadamiania o przypadkach naruszenia bezpieczeństwa, jak to miało miejsce w przypadku amerykańskich ustaw o zgłaszaniu naruszeń bezpieczeństwa, ponieważ powiadamianie sprawi, że wiadomym stanie się, które technologie obarczone są większym ryzykiem naruszenia bezpieczeństwa danych ([1]).

29. Poza tym powiadamianie o przypadkach naruszenia bezpieczeństwa sprawia, że osoby fizyczne są świadome ryzyka, gdy narażone zostały ich dane osobowe, i pomaga im podjąć konieczne działania, by ograniczyć takie ryzyko. Na przykład jeśli narażone zostały dane bankowe, osoba fizyczna, która została o tym poinformowana, może podjąć decyzję o zmianie danych odnoszących się do jej konta bankowego, by zapobiec przejęciu tych informacji i wykorzystaniu ich do celów niezgodnych z prawem (zwykle określanych mianem „kradzieży tożsamości"). Podsumowując — obowiązek ten zmniejsza prawdopodobieństwo, że dana osoba padnie ofiarą kradzieży tożsamości i może pomóc ofiarom w podjęciu działań niezbędnych do rozwiązania problemów.

Niedostatki proponowanej zmiany

30. EIOD cieszy się, że w art. 4 ust. 3 i 4 wprowadza się system powiadamiania o przypadkach naruszenia bezpieczeństwa, opowiadałby się jednak za objęciem tymi przepisami także dostawców usług społeczeństwa informacyjnego. Oznaczałoby to, że banki internetowe, firmy internetowe i podmioty świadczące elektroniczne usługi opieki zdrowotnej zostałyby także objęte tym prawem ([2]).

31. Powody, dla których uzasadnione jest nałożenie na dostawców publicznie dostępnych usług łączności elektronicznej w sieciach publicznych wymogu powiadamiania o przypadkach naruszenia bezpieczeństwa, są prawdziwe również w przypadku innych organizacji, także przetwarzających masowe ilości danych osobowych, których ujawnienie byłoby dla podmiotów tych danych wyjątkowo szkodliwe. Dotyczy to banków internetowych, brokerów danych i innych dostawców internetowych, którzy przetwarzają dane sensytywne (w tym dane o zdrowiu, poglądach politycznych itd.). Narażenie informacji przechowywanych przez banki i przedsiębiorstwa internetowe, wśród których mogą być nie tylko numery kont bankowych, ale również dane karty kredytowej, może doprowadzić do kradzieży tożsamości, w którym to przypadku sprawą zasadniczą jest, by dane osoby były tego świadome i mogły podjąć niezbędne działania. W tym ostatnim przypadku (elektroniczne usługi zdrowotne), jeśli narażone zostaną informacje sensytywne, to nawet o ile dana osoba nie ucierpi finansowo, może doznać szkody pozaekonomicznej.

([1]) Zob. sprawozdanie pt. „Security Economics and the Internal Market", którego sporządzenie zleciła prof. Rossowi Andersonowi, Rainerowi Böhme, Richardowi Claytonowi i Tylerowi Moore Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA).Sprawozdanie jest dostępne pod adresem http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Za usługi społeczeństwa informacyjnego w dyrektywie o handlu elektronicznym uznaje się usługi zwykle świadczone odpłatnie, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług.

32. Ponadto wymienione powyżej korzyści, których oczekuje się w związku z wprowadzeniem tego obowiązku, dzięki poszerzeniu jego zakresu nie będą się ograniczać tylko do jednego sektora działalności, czyli dostawców publicznie dostępnych usług łączności elektronicznej, ale obejmą ogół usług społeczeństwa informacyjnego. Nałożenie bowiem na usługi społeczeństwa informacyjnego, takie jak banki internetowe, obowiązku powiadamiania o przypadkach naruszenia bezpieczeństwa nie tylko zwiększy odpowiedzialność tych podmiotów, ale również zmotywuje je do wzmocnienia stosowanych środków bezpieczeństwa, a tym samym umożliwi im uniknięcie potencjalnych naruszeń bezpieczeństwa.

33. Istnieją inne precedensy, gdy dyrektywa o prywatności i łączności elektronicznej ma zastosowanie także do podmiotów innych niż dostawcy PPECS, jak choćby w przypadku art. 5 dotyczącego poufności komunikacji i art. 13 dotyczącego komunikatów niezamówionych (spamu). Potwierdza to, że w przeszłości prawodawca podjął bardzo mądrą decyzję, by poszerzyć zakres zastosowania pewnych przepisów dyrektywy o prywatności i łączności elektronicznej, ponieważ uznał, że jest to celowe i konieczne. EIOD wyraża nadzieję, że w chwili obecnej prawodawca nie zawaha się przyjąć podobne, rozsądne i elastyczne podejście i rozszerzy zakres zastosowania art. 4 na dostawców usług społeczeństwa informacyjnego. W tym celu wystarczyłoby dodać do art. 4 ust. 3 wzmiankę o dostawcach usług społeczeństwa informacyjnego w brzmieniu: „W przypadku naruszenia bezpieczeństwa, prowadzącego do przypadkowego lub … dostawca publicznie dostępnych usług łączności i dostawca usług społeczeństwa informacyjnego … powiadamiają o takim naruszeniu zainteresowanego abonenta i krajowy organ regulacyjny".

34. EIOD uważa wprowadzenie tego obowiązku i jego przestrzeganie zarówno przez dostawców PPECS, jak i dostawców usług społeczeństwa informacyjnego za pierwszy etap zmian, które ostatecznie można by stosować ogółem do wszystkich kontrolerów danych.

Konkretne ramy prawne dotyczące naruszeń bezpieczeństwa, którymi należy zająć się w procedurze komitetowej

35. Wniosek nie porusza pewnych kwestii związanych z obowiązkiem powiadamiania o przypadkach naruszenia bezpieczeństwa. Takimi kwestiami, którymi należy się zająć, są np. okoliczności powiadomienia, jego forma i stosowane procedury. Zamiast tego w art. 4 ust. 4 pozostawia się podejmowanie takich decyzji komitetowi działającemu w myśl procedury komitetowej ([1]), a mianowicie Komitetowi ds. Łączności ustanowionemu w art. 22 dyrektywy ramowej, zgodnie z decyzją Rady z dnia 28 czerwca 1999 r. Dokładniej rzecz biorąc, środki takie byłyby przyjmowane zgodnie z art. 5 decyzji Rady z dnia 28 czerwca 1999 r., która ustanawia zasady procedury regulacyjnej w odniesieniu do „środków o ogólnym zasięgu mających na celu stosowanie istotnych przepisów aktów podstawowych".

36. EIOD nie sprzeciwia się wyborowi, polegającemu na pozostawieniu wszystkich tych kwestii przepisom wykonawczym. Przyjęcie przepisów w procedurze komitetowej prawdopodobnie skróci procedurę legislacyjną. Procedura komitetowa pomoże również zapewnić harmonizację, będącą celem, do którego zdecydowanie należy dążyć.

37. Biorąc pod uwagę dużą liczbę kwestii, które trzeba będzie rozstrzygnąć w drodze przepisów wykonawczych, i znaczenie tych kwestii, które podkreślono poniżej, wydaje się, że należy się nimi zająć w jednym akcie prawnym, a nie każdej z nich poświęcać odrębny przepis, co doprowadziłoby do tego, że niektóre z tych kwestii wyjaśniałaby dyrektywa o prywatności i łączności elektronicznej, a inne — przepisy wykonawcze. Cieszyć zatem powinno podejście Komisji, chcącej pozostawić podjęcie tych decyzji przepisom wykonawczym, które będą przyjęte pod zasięgnięciu opinii EIOD-a, a także, miejmy nadzieję, innych podmiotów (zob. punkt poniżej).

Kwestie, które należy rozstrzygnąć w przepisach wykonawczych

38. Znaczenie środków wykonawczych docenia się zwłaszcza, jeśli można przewidzieć w miarę szczegółowo, jakie kwestie trzeba będzie rozstrzygnąć w przepisach wykonawczych. W środkach wykonawczych można bowiem ustalić normy przekazywania informacji. Na przykład można w nich sprecyzować, co stanowi naruszenie bezpieczeństwa, warunki, jakie muszą spełnić przekazywane osobom fizycznymi i organom informacje, termin przekazania informacji i powiadomienia.

([1]) Procedury legislacyjne w WE, w które zaangażowane są komitety składające się z przedstawicieli rządów państw członkowskich na szczeblu urzędników państwowych.

39. EIOD uważa, że dyrektywa o prywatności i łączności elektronicznej, w szczególności jej art. 4, nie powinna zawierać żadnych wyjątków od obowiązku powiadomienia. Z tego względu EIOD wyraża zadowolenie z przyjętego przez Komisję podejścia, wyrażonego w art. 4, który wprowadza obowiązek powiadomienia i nie przewiduje od tego obowiązku żadnych wyjątków, pozwala jednak, by tę i inne kwestie rozstrzygały przepisy wykonawcze. Choć EIOD jest świadomy argumentów, które mogłyby uzasadniać wprowadzenie pewnych wyjątków od tego obowiązku, opowiada się za tym, by tę i inne kwestie szczegółowo rozstrzygnięto w przepisach wykonawczych, po przeprowadzeniu dogłębnej i kompleksowej debaty na temat wszystkich odpowiednich kwestii. Jak napisano powyżej, złożony charakter tych kwestii związany z obowiązkiem powiadomienia o przypadkach naruszenia bezpieczeństwa, w tym z zasadnością istnienia wyłączeń lub ograniczeń, wymaga ich traktowania w spójny sposób, tj. w jednym akcie prawnym, który jest poświęcony wyłącznie tym kwestiom.

Zasięgnięcie opinii EIOD-a i potrzeba poszerzenia konsultacji

40. Zważywszy na to, w jakim stopniu środki wykonawcze wpłyną na ochronę danych osobowych osób fizycznych, ważnym jest, by przed przyjęciem tych środków Komisja przeprowadziła odpowiednie konsultacje. Z tego powodu EIOD wyraża zadowolenie z art. 4 ust. 4 wniosku, w którym jednoznacznie stwierdza się, że przed przyjęciem środków wykonawczych Komisja zasięgnie opinii Europejskiego Inspektora Ochrony Danych. Środki takie będą nie tylko dotyczyć ochrony danych osobowych i prywatności osób fizycznych, ale również wywrą na nią poważny wpływ. Ważne jest zatem, by uzyskać opinię EIOD-a, zgodnie z wymogiem zawartym w art. 41 rozporządzenia (WE) nr 45/2001.

41. Poza koniecznością zasięgnięcia opinii EIOD-a zasadne może być wprowadzenie przepisu przewidującego, że planowane środki wykonawcze będą podlegać konsultacjom publicznym, które pozwolą uzyskać opinię społeczeństwa i będą zachętą do podzielenia się doświadczeniami wzorcowych rozwiązań w tej dziedzinie. Konsultacje takie będą nie tylko dla branży, ale także innych zainteresowanych stron, w tym innych organów ochrony danych i grupy roboczej art. 29, odpowiednim kanałem komunikacji, którym umożliwi im przedstawienie swoich poglądów. Potrzeba konsultacji publicznych nabiera jeszcze większego znaczenia, jeśli weźmiemy pod uwagę, że przepisy zostaną przyjęte w procedurze komitetowej, w której możliwość interwencji Parlamentu Europejskiego jest ograniczona.

42. EIOD zwraca uwagę, że w art. 4 ust. 4 wniosku przewiduje się, że przed przyjęciem przepisów wykonawczych Komisja zasięgnie również opinii Urzędu ds. Rynku Łączności Elektronicznej. W tym względzie EIOD docenia zasadę zasięgania opinii Urzędu ds. Rynku Łączności Elektronicznej, będącego spadkobiercą doświadczenia i wiedzy na temat kwestii sieci i bezpieczeństwa informacji, które zgromadziła Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA). Do czasu utworzenia Urzędu ds. Rynku Łączności Elektronicznej być może należałoby — jako rozwiązanie tymczasowe — przewidzieć w proponowanej zmianie (art. 4 ust. 4) konsultacje z ENISA.

II.3. **Przepis dotyczący plików *cookie*, oprogramowania szpiegującego i podobnych urządzeń: zmiana w art. 5 ust. 3**

43. W art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej poruszono kwestię technologii, które umożliwiają dostęp do informacji i przechowywanie informacji w urządzeniu końcowym użytkownika za pośrednictwem sieci łączności elektronicznej. Przykładem zastosowania art. 5 ust. 3 jest korzystanie z plików *cookie* ([1]). Innym przykładem jest wykorzystanie takich technologii, jak oprogramowanie szpiegujące i trojany (programy ukryte w wiadomościach lub innych, pozornie nieszkodliwych programach). Założenia takich technologii i ich cele bardzo się różnią, i o ile niektóre są dla użytkownika zupełnie nieszkodliwe czy nawet użyteczne, o tyle inne są wyraźnie szkodliwe i groźne.

([1]) Pliki *cookie* są umieszczane przez dostawców usług społeczeństwa informacyjnego (strony internetowe) w urządzeniach końcowych użytkowników w różnych celach, również w celu rozpoznania użytkownika, gdy po raz kolejny odwiedza daną stronę internetową. W praktyce, gdy plik *cookie* jest przesyłany do użytkownika Internetu przez stronę internetową, komputerowi użytkownika jest nadawany niepowtarzalny numer (tzn. komputer, który otrzymał plik *cookie* od strony internetowej A, staje się „komputerem, w którym przechowywany jest plik *cookie* nr 111"). Strona internetowa zachowuje ten numer jako odniesienie. Jeśli użytkownik komputera, który otrzymał plik *cookie* nr 111, nie wykasuje tego pliku, to gdy po raz kolejny odwiedzi tę samą stronę internetową, będzie ona mogła zidentyfikować komputer jako ten, w którym przechowywany jest plik *cookie* nr 111. Z czego strona internetowa wyciąga oczywisty wniosek, że używając tego komputera odwiedzano ją już wcześniej. Mechanizm, który umożliwia stronie internetowej rozpoznanie komputera jako tego, z którego korzystano już przy wcześniejszych wizytach, jest prosty. Gdy komputer, z którego korzysta odwiedzający, przechowuje pliki *cookie*, takie jak *cookie* nr 111, i używany jest do odwiedzenia strony, która przy wcześniejszych odwiedzinach wygenerowała ten plik *cookie*, strona ta przeszuka twardy dysk tego komputera, by odnaleźć nr pliku *cookie*. Jeśli przeglądarka użytkownika odnajdzie plik *cookie* odpowiadający numerowi odniesienia zachowanemu na tej stronie internetowej, informuje tę stronę, że komputer przechowuje plik *cookie* nr 111.

44. W art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej przedstawiono warunki, które należy spełnić, gdy wykorzystuje się wspomniane powyżej technologie, by uzyskać dostęp informacji w urządzeniach końcowych użytkowników lub przechowywać je tam. Konkretniej mówiąc, zgodnie z art. 5 ust. 3: (i) użytkownikom Internetu należy przekazać jasne i wyczerpujące informacje zgodnie z dyrektywą 95/46/WE, m.in. na temat celów przetwarzania i (ii) użytkownicy Internetu muszą mieć możliwość niewyrażenia zgody na takie przetwarzanie, tj. powinni mieć do wyboru opcję, zgodnie z którą informacje uzyskane z ich urządzeń końcowych nie będą podlegać przetwarzaniu.

Korzyści płynące z proponowanej zmiany

45. Zakres zastosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej w jego obecnym brzmieniu jest ograniczony do sytuacji, w których dostęp do informacji i przechowywanie informacji w urządzeniu końcowym użytkownika odbywa się za pośrednictwem *sieci łączności elektronicznej*. Obejmuje to sytuację opisaną powyżej, jeśli chodzi o korzystanie z plików *cookie*, a także z innych technologii, takich jak oprogramowanie szpiegujące dostarczane przez sieci łączności elektronicznej. Niejasne jest jednak, czy art. 5 ust. 3 dotyczy sytuacji, w których podobne technologie (pliki *cookie*, oprogramowanie szpiegujące itp.) są przekazywane za pośrednictwem oprogramowania dostarczanego przez zewnętrzne nośniki danych i ściągniętego na urządzenie końcowe użytkownika. Zważywszy, że zagrożenie dla prywatności istnieje bez względu na kanał łączności, ograniczenie zakresu zastosowania art. 5 ust. 3 do jednego kanału łączności jest rozwiązaniem niefortunnym.

46. Dlatego EIOD cieszy się z wprowadzenia zmiany do art. 5 ust. 3, która — dzięki usunięciu wzmianki o „elektronicznych sieciach łączności" — poszerza w istocie zakres zastosowania tego artykułu. W swej zmienionej wersji art. 5 ust. 3 obejmuje bowiem sytuacje, w których dostęp do informacji i ich przechowywanie w urządzeniu końcowym użytkownika odbywa się za pośrednictwem sieci łączności elektronicznej, ale także za pośrednictwem innych zewnętrznych nośników danych, takich jak płyty kompaktowe, CD-ROM-y, pamięci USB itd.

Techniczne przechowywanie danych w celu ułatwienia transmisji komunikatu

47. Ostatnie zdanie art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej zachowało swoje brzmienie w zmienionej postaci artykułu. W myśl tego zdania, konieczność przestrzegania wymogów określonych w art. 5 ust. 3 zdanie pierwsze „nie stanowi (to) przeszkody dla technicznego przechowywania danych ani dostępu do nich jedynie w celu wykonania lub ułatwiania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej, lub gdy jest to szczególnie niezbędne w celu świadczenia usługi społeczeństwa informacyjnego …". A zatem obowiązkowe zasady określone w art. 5 ust. 3 (konieczność poinformowania i możliwość niewyrażenia zgody) nie mają zastosowania, gdy jedynym celem dostępu do urządzenia końcowego użytkownika lub przechowywanie informacji jest *ułatwienie* transmisji lub gdy jest to ściśle niezbędne, aby świadczyć usługi społeczeństwa informacyjnego zażądane przez tego użytkownika.

48. Dyrektywa nie podaje, kiedy jedynym celem dostępu lub przechowywania informacji jest ułatwienie transmisji lub dostarczenie informacji. Jedną z sytuacji, które bez wątpienia podlegałyby temu wyłączeniu, jest przyłączenie komputera do Internetu. Dzieje się tak, ponieważ aby przyłączyć komputer do Internetu konieczny jest adres IP ([1]). Komputer użytkownika końcowego zostanie poproszony o podanie dostawcy usługi dostępu do Internetu pewnych informacji na swój temat, a w zamian dostawca ten przyzna mu adres IP. W tym przypadku informacje przechowywane w urządzeniu końcowym użytkownika zostaną przekazane dostawcy usługi dostępu do Internetu po to, aby użytkownik zyskał możliwość dostępu do Internetu. W tej sytuacji dostawca usługi dostępu do Internetu jest zwolniony zarówno z wymogu powiadomienia o gromadzeniu informacji, jak i z obowiązku zapewnienia prawa do odmowy, o ile gromadzenie informacji jest konieczne do świadczenia usługi.

49. Po podłączeniu do Internetu, jeśli użytkownik chce obejrzeć daną stronę internetową, musi wysłać zapytanie do serwera, na którym ta strona się znajduje. Ten ostatni odpowie, jeśli będzie wiedział, dokąd przesłać informacje, tj. jeśli zna adres IP użytkownika. Ze względu na sposób, w jaki przechowywany jest ten adres, oznacza to, że strona internetowa, którą użytkownik chce odwiedzić, będzie musiała ponownie uzyskać dostęp do informacji zgromadzonych w urządzeniu końcowym użytkownika Internetu. Taka wymiana oczywiście również podlegałaby wyłączeniu. I rzeczywiście, wydaje się, że te przypadki powinny znaleźć się poza zakresem zastosowania wymogów w art. 5 ust. 3.

([1]) Adres IP (*Internet Protocol address*) to niepowtarzalny adres, którego używają niektóre urządzenia elektroniczne, by dokonać wzajemnej identyfikacji i komunikować się ze sobą w sieci komputerowej wykorzystującej standard IP (*Internet Protocol standard*) — mówiąc prościej, jest to adres komputera. Każde urządzenie podłączone do sieci — również routery, przełączniki, komputery, serwery infrastrukturalne (np. NTP, DNS, DHCP, SNMP itd.), drukarki, faksy internetowe i niektóre telefony — może mieć własny adres, który jest niepowtarzalny w ramach danej sieci. Niektóre adresy IP mają być niepowtarzalne w ramach całego Internetu, inne powinny być niepowtarzalne jedynie w ramach danego przedsiębiorstwa.

50. EIOD uważa za słuszne zwolnienie z wymogu powiadomienia i umożliwienia odmowy w sytuacjach przedstawionych powyżej, gdy techniczne przechowywanie i dostęp do urządzenia końcowego użytkownika jest *konieczne* jedynie po to, by przeprowadzić transmisję komunikatu przez sieć łączności elektronicznej. To samo odnosi się do sytuacji, w której techniczne przechowywanie lub dostęp jest ściśle konieczny, by świadczyć usługę społeczeństwa informacyjnego. EIOD nie widzi jednak potrzeby zwolnienia z obowiązku przekazania informacji i przyznania prawa do odmowy w sytuacjach, w których celem technicznego przechowywania czy dostępu jest tylko *ułatwienie* transmisji komunikatu. Na przykład w myśl ostatniego zdania omawianego artykułu podmiot danych nie może skorzystać z prawa do otrzymania informacji ani z prawa do niewyrażenia zgody na przetwarzanie swoich danych, jeśli plik *cookie* zbiera dane na temat jego preferencji językowych lub lokalizacji (np. Belgia, Chiny), ponieważ tego typu plik *cookie* można by przedstawić jako taki, którego celem jest ułatwienie transmisji komunikatu. EIOD jest świadomy, że na poziomie oprogramowania podmioty danych dysponują praktyczną możliwością niewyrażenia zgody na przechowywanie plików *cookie* lub możliwością jego modulowania. Nie stoi za tym jednak jednoznacznie żaden przepis prawny, który formalnie upoważniłby podmiot danych do obrony swoich praw w opisanej powyżej sytuacji.

51. Aby uniknąć takiego obrotu sprawy, EIOD sugeruje, by do ostatniej części art. 5 ust. 3 wprowadzić niewielką zmianę, która polega na wykreśleniu słów „lub ułatwiania" ze zdania: „nie stanowi to przeszkody dla technicznego przechowywania danych ani dostępu do nich jedynie w celu wykonania lub ułatwiania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej, lub gdy jest to szczególnie niezbędne w celu świadczenia usługi społeczeństwa informacyjnego …".

II.4. **Występowanie na drogę sądową przez dostawców PPECS i podmioty prawne: dodanie ust. 6 do art. 13**

52. Proponowany art. 13 ust. 6 przewiduje, że każda osoba fizyczna lub prawna mająca w tym uzasadniony interes, w szczególności dostawcy usług łączności elektronicznej chroniący swój interes gospodarczy, mogą podejmować kroki prawne, by walczyć z tymi, którzy naruszają art. 13 dyrektywy o prywatności i łączności elektronicznej. Artykuł ten dotyczy wysyłania niezamówionych komunikatów komercyjnych.

53. Proponowana zmiana umożliwi np. dostawcom usługi dostępu do Internetu uporanie się ze autorami spamu niewłaściwie wykorzystującymi ich sieci, pozywanie podmiotów podrabiających adresy nadawcy lub przejmujących kontrolę nad serwerami, by wykorzystywać je do wysyłania spamu itd.

54. Dyrektywa o prywatności i łączności elektronicznej nie mówiła jasno, czy dostawcom PPECS przysługuje prawo do podejmowania działań przeciwko autorom spamu, a dostawcy ci w odosobnionych przypadkach wnosili pozwy do sądu za naruszenie art. 13 wdrożonego przez przepisy państwa członkowskiego ([1]). Przyznając, że powodem wejścia na drogę sądową może być dla dostawców usług łączności elektronicznej ochrona ich interesu gospodarczego, wniosek potwierdza, że dyrektywa o prywatności i łączności elektronicznej ma na celu nie tylko ochronę poszczególnych abonentów, ale również dostawców usług łączności elektronicznej.

55. EIOD wyraża zadowolenie, że wniosek dopuszcza, by dostawcy usług łączności elektronicznej w ochronie swojego interesu gospodarczego mogli występować na drogę sądową przeciwko autorom spamu. O ile nie zajdą wyjątkowe okoliczności, poszczególni abonenci nie mają środków na wszczynanie tego typu działań sądowych ani nic ich do tego zachęca. Z drugiej strony dostawcy usługi dostępu do Internetu i inni dostawcy PPECS dysponują zapleczem finansowym i technicznym, by dokładnie zbadać przypadki masowego wysyłania spamu i stwierdzić, kim są sprawcy, a zatem wydaje się słuszne, by przyznać im prawo występowania na drogę sądową przeciwko autorom spamu.

56. Zdaniem EIOD-a proponowana zmiana jest cenna o tyle, że pozwoliłaby również stowarzyszeniom konsumenckim i związkom zawodowym reprezentującym interesy konsumentów będących celem działań autorów spamu występowanie na drogę sądową w imieniu tych konsumentów. Jak stwierdzono powyżej, szkody wyrządzone podmiotowi danych, który był adresatem spamu, rozpatrywane indywidualnie, zwykle nie są same w sobie na tyle dotkliwe, by wszczynał on kroki sądowe. EIOD już zaproponował ten środek, by zaradzić naruszeniom prywatności i ochrony danych, gdy ogólnie

([1]) Jednym z takich przypadków była sprawa korporacja Microsoft przeciwko Paul McDonald t/a Bizards UK (2006 All Er (D) 153).

wypowiadał się w swojej opinii w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych ([1]). Zdaniem EIOD-a wniosek powinien był pójść dalej i zaproponować pozwy zbiorowe, umożliwiając grupom obywateli wspólnie wnosić spory sądowe w sprawach dotyczących ochrony danych osobowych. W przypadku spamu, gdy otrzymuje go spora liczba osób, grupy osób powinny móc połączyć siły i wnosić pozwy zbiorowe przeciwko autorom spamu.

57. EIOD ze szczególnym żalem przyjmuje fakt, że wniosek ogranicza prawo osób prawnych do wystąpienia na drogę sądową do sytuacji, w których nastąpiło naruszenie art. 13 dyrektywy, tj. sytuacji, w których pogwałcony został przepis dotyczący niechcianych wiadomości elektronicznych. W myśl proponowanej zmiany osoby prawne nie będą mogły wszczynać działań sądowych w przypadku naruszenia innych przepisów dyrektywy o prywatności i łączności elektronicznej. Na przykład, w swej obecnej postaci przepis ten nie pozwala osobie prawnej, np. stowarzyszeniu konsumenckiemu, wystąpić na drogę sądową przeciwko dostawcy usługi dostępu do Internetu, który ujawnił dane osobowe milionów konsumentów. Wykonywanie całej dyrektywy o prywatności i łączności elektronicznej, nie tylko danego artykułu, znacznie by się poprawiło, gdyby przepisowi art. 13 ust. 6 nadano ogólny charakter, by umożliwić osobom prawnym podejmowanie działań sądowych w przypadku naruszenia któregokolwiek przepisu tej dyrektywy.

58. Aby zaradzić temu problemowi, EIOD proponuje, by przekształcić art. 13 ust. 6 w odrębny artykuł (art. 14). Ponadto brzmienie art. 13 ust. 6 należałoby nieznacznie zmodyfikować: zamiast „na podstawie niniejszego artykułu" powinno być „na podstawie niniejszej dyrektywy".

II.5. **Wzmocnienie przepisów dotyczących egzekwowania: dodany art. 15a**

59. Dyrektywa o prywatności i łączności elektronicznej nie zawiera jednoznacznych przepisów dotyczących egzekwowania. Zamiast tego, zawiera ona odniesienie do części dyrektywy o ochronie danych ([2]) poświęconej egzekwowaniu. EIOD z zadowoleniem przyjmuje nowy art. 15a wniosku, w którym jednoznacznie wyjaśnione są kwestie dotyczące egzekwowania na mocy tej dyrektywy.

60. Po pierwsze, EIOD zwraca uwagę, że skuteczna strategia egzekwowania w tej dziedzinie zakłada, zgodnie z wymogiem zawartym w art. 15a ust. 3, że organy krajowe mają uprawnienia do prowadzenia dochodzeń koniecznych do zgromadzenia niezbędnych informacji. Bardzo często dowód naruszenia przepisów dyrektywy o prywatności i łączności elektronicznej będzie miał postać elektroniczną i może być przechowywany w różnych komputerach i urządzeniach lub sieciach. Z tego względu ważne jest, by agencje odpowiedzialne za egzekwowanie prawa mogły uzyskiwać nakaz przeszukania, dający im prawo do wejścia, przeszukania i zajęcia.

61. Po drugie, EIOD szczególnie przychylnie przyjmuje proponowaną zmianę, tzn. art. 15a ust. 2, zgodnie z którym krajowe organy regulacyjne muszą dysponować uprawnieniami do wydania nakazu, tj. do doprowadzenia do zaprzestania naruszeń, i uprawnieniami i zasobami niezbędnymi do prowadzenia dochodzeń. Krajowe organy regulacyjne, także krajowe organy ochrony danych, powinny dysponować uprawnieniami do wydawania nakazu sądowego zmuszającego sprawców do zaprzestania działalności, która narusza dyrektywę o prywatności i łączności elektronicznej. Nakaz lub uprawnienie, by nakazać zaprzestanie naruszania przepisów jest użytecznym narzędziem w przypadku uporczywego postępowania, które narusza prawa osób fizycznych. Nakazy będą bardzo użyteczne, by powstrzymać przypadki nieprzestrzegania dyrektywy o prywatności i łączności elektronicznej, np. naruszania art. 13 dotyczącego niezamówionych komunikatów komercyjnych, które to naruszenie z natury rzeczy jest postępowaniem uporczywym.

62. Po trzecie, wniosek umożliwia Komisji wprowadzenie technicznych środków wykonawczych, które pozwolą zapewnić skuteczną współpracę transgraniczną przy egzekwowaniu przepisów krajowych (proponowany art. 15a ust. 4). Dotychczas współpraca ta obejmuje porozumienie, ustanowione z inicjatywy Komisji, w sprawie opracowania wspólnej procedury rozpatrywania transgranicznych skarg dotyczących spamu.

([1]) Opinia Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych (Dz.U. C 255 z 27.10.2007, str. 1).

([2]) Dyrektywa 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.

63. EIOD uważa, że jeśli pomagając swojemu odpowiednikowi w innym kraju organ regulacyjny będzie miał przepisy po swojej stronie, niewątpliwie pomoże to egzekwować przepisy w sytuacjach transgranicznych. Zatem właściwe jest, by wniosek umożliwiał Komisji stworzenie warunków do zapewnienia współpracy transgranicznej, w tym procedur dzielenia się informacjami.

III. **WNIOSKI I ZALECENIA**

64. EIOD całkowicie popiera wniosek. Proponowane zmiany poprawiają ochronę prywatności i danych osobowych osób fizycznych w sektorze łączności elektronicznej, a proces ten przebiega z wyczuciem, bez nieuzasadnionego i zbędnego obciążania organizacji. Ściślej mówiąc, EIOD uważa, że większość proponowanych zmian nie wymaga modyfikacji, ponieważ dobrze odpowiadają one zamierzonemu celowi. W pkt 69 poniżej przedstawiono zmiany, co do których EIOD wyraża nadzieję, że nie ulegną modyfikacji.

65. Choć EIOD ogólnie bardzo pozytywnie ocenia wniosek, uważa, że niektóre z zaproponowanych w nim zmian należy poprawić, tak by dopilnować, że faktycznie zapewniają one odpowiednią ochronę danych osobowych i prywatności osób fizycznych. Odnosi się to w szczególności do przepisów dotyczących powiadamiania o przypadkach naruszenia bezpieczeństwa oraz przepisów mówiących o występowaniu na drogę sądową przez dostawców usług łączności elektronicznej w związku z pogwałceniem przepisów o niezamówionych komunikatach komercyjnych. Ponadto EIOD wyraża żal, że we wniosku nie poruszono pewnych kwestii, które nie są też dokładnie wyjaśnione w obowiązującej dyrektywie o prywatności i łączności elektronicznej; nie skorzystano tym samym ze sposobności, jaką daje ten przegląd, by zaradzić nierozwiązanym problemom.

66. Aby rozwiązać oba problemy, czyli kwestie niedostatecznie wyjaśnione we wniosku i wcale w nim nieporuszone, w niniejszej opinii zaproponowano pewne zmiany redakcyjne. W pkt 67 i 68 podsumowano te problemy i zaproponowano konkretne sformułowania. EIOD apeluje do prawodawcy o ich uwzględnienie w trakcie procesu legislacyjnego.

67. Zmiany zawarte we wniosku, w przypadku których EIOD zdecydowanie opowiada się za modyfikacją, to:

(i) **Powiadamianie o przypadkach naruszenia bezpieczeństwa**: W obecnym brzmieniu proponowana zmiana, dodająca *art. 4 ust. 4*, ma zastosowanie do dostawców publicznie dostępnych usług łączności elektronicznej w sieciach publicznych (dostawcy usługi dostępu do Internetu, operatorzy sieci), którzy mają obowiązek powiadamiać krajowe organy regulacyjne i swoich klientów o przypadkach naruszenia bezpieczeństwa. EIOD w pełni popiera istnienie takiego obowiązku. Uważa jednak, że obowiązek ten powinien dotyczyć również dostawców usług społeczeństwa informacyjnego, którzy często przetwarzają sensytywne dane osobowe. Tak więc banki internetowe, dostawcy elektronicznych usług zdrowotnych i wszystkie pozostałe firmy internetowe także musieliby się wywiązywać z tego obowiązku.

W tym celu EIOD proponuje, by dodać do art. 4 ust. 3 wzmiankę o dostawcach usług społeczeństwa informacyjnego w brzmieniu: „W przypadku naruszenia bezpieczeństwa, prowadzącego do przypadkowego lub … dostawca publicznie dostępnych usług łączności *i dostawca usług społeczeństwa informacyjnego* … powiadamiają o takim naruszeniu zainteresowanego abonenta i krajowy organ regulacyjny".

(ii) **Występowanie na drogę sądową przez dostawców publicznie dostępnych usług łączności elektronicznej w sieciach publicznych**: W obecnym brzmieniu proponowana zmiana, dodająca *art. 13 ust. 6*, przewiduje, że aby zwalczać przypadki naruszenia art. 13 dyrektywy o prywatności i łączności elektronicznej, który zajmuje się kwestią spamu, środki cywilnoprawne może podejmować każda osoba fizyczna lub prawna, w szczególności dostawcy usług łączności elektronicznej. EIOD wyraża zadowolenie z tego przepisu. Nie może jednak zrozumieć, dlaczego to nowe uprawnienie ma się ograniczać do przypadków naruszenia art. 13. EIOD proponuje, aby osoby prawne miały prawo występować na drogę sądową w przypadku naruszenia któregokolwiek z przepisów dyrektywy o prywatności i łączności elektronicznej.

Aby osiągnąć zamierzony skutek, EIOD proponuje, by art. 13 ust. 6 został przekształcony w odrębny artykuł (art. 14). Ponadto brzmienie art. 13 ust. 6 należałoby nieznacznie zmodyfikować: zamiast „na podstawie niniejszego artykułu" powinno być „na podstawie niniejszej dyrektywy".

68. Zakres zastosowania dyrektywy o prywatności i łączności elektronicznej, który jest obecnie ograniczony do dostawców publicznych sieci łączności elektronicznej, pozostaje jednym z najbardziej niepokojących problemów, których wniosek nie rozwiązuje. Zdaniem EIOD-a dyrektywa o prywatności i łączności elektronicznej powinna zostać zmieniona tak, by jej stosowanie obowiązywało dostawców usług łączności elektronicznej również w sieciach mieszanych (publiczno-prywatnych) i prywatnych.

69. EIOD stoi zdecydowanie na stanowisku, że poniższe zmiany nie powinny ulec modyfikacji:

(i) **Identyfikacja radiowa**: Proponowana zmiana w *art. 3*, zgodnie z którą sieci łączności elektronicznej obejmują również „publiczne sieci łączności służące do zbierania danych i obsługi urządzeń identyfikacyjnych", jest w pełni zadowalająca. Przepis ten ma bardzo pozytywny wymiar, ponieważ wyjaśnia, że pewne zastosowania identyfikacji radiowej muszą być zgodne z dyrektywą o prywatności i łączności elektronicznej, i tym samym zmniejsza niepewność prawną w tym względzie.

(ii) **Pliki cookie/oprogramowanie szpiegujące**: Należy cieszyć się z proponowanej zmiany w art. 5 ust. 3, ponieważ dzięki niej obowiązek poinformowania danego użytkownika i dania mu możliwości niewyrażenia zgody na przechowywanie plików *cookie*/oprogramowania szpiegującego w jego urządzeniu końcowym będzie istniał również wtedy, gdy takie pliki/oprogramowanie są przekazywane za pośrednictwem zewnętrznych nośników danych, takich jak CD-ROM-y czy pamięci USB. EIOD sugeruje jednak, by do ostatniej części art. 5 ust. 3 wprowadzić niewielką zmianę, która polega na wykreśleniu słów „lub ułatwiania" ze zdania.

(iii) **Wybór procedury komitetowej z zasięgnięciem opinii EIOD-a oraz warunki/ograniczenia obowiązku powiadamiania**: Proponowana zmiana, w której dodaje się art. 4 ust. 4 dotyczący powiadamiania o przypadkach naruszenia bezpieczeństwa, pozostawia komitetowi — po zasięgnięciu opinii EIOD-a — decyzję w sprawie złożonych kwestii dotyczących okoliczności/formy/procedur systemu powiadamiania o przypadkach naruszenia bezpieczeństwa. EIOD wyraża zdecydowane poparcie dla takiego ujednoliconego podejścia. Przepisy dotyczące powiadamiania o przypadkach naruszenia bezpieczeństwa są same w sobie tematem, którym należy się zająć, po dogłębnej dyskusji i analizie.

Z tą sprawą wiąże się apel do niektórych podmiotów o zaproponowanie, w jakich sytuacjach nie istniałby obowiązek powiadamiania o przypadkach naruszenia bezpieczeństwa zgodnie z art. 4 ust. 4. EIOD stanowczo sprzeciwia się takiemu podejściu. Opowiada się raczej za tym, by zagadnienie ogólnego obowiązku powiadomienia, sposobów powiadamiania czy tego, w jakich okolicznościach treść powiadomienia mogłaby zostać skrócona lub ograniczona, było przedmiotem całościowej analizy poprzedzonej rzeczywistą dyskusją.

(iv) **Egzekwowanie**: Proponowana zmiana dotycząca dodania *art. 15a* zawiera wiele pomocnych elementów, które należy zachować, ponieważ przyczynią się one do faktycznego przestrzegania przepisów; elementy te to m.in. wzmocnienie uprawnień do prowadzenia dochodzeń, którymi dysponują krajowe organy regulacyjne (art. 15a ust. 3), oraz przyznanie krajowym organom regulacyjnym uprawnienia do nakazania zaprzestania naruszeń.

Sporządzono w Brukseli, dnia 10 kwietnia 2008 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych