Druga opinia Europejskiego Inspektora Ochrony Danych w sprawie przeglądu dyrektywy 2002/58/WE dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)

(2009/C 128/04)

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,

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,

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,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. **WPROWADZENIE**

Kontekst

1. W dniu 13 listopada 2007 r. Komisja Europejska przyjęła wniosek w sprawie zmiany m.in. dyrektywy o prywatności i łączności elektronicznej, zwykle zwanej dyrektywą o e-prywatności ([1]) (wniosek ten w dalszej części niniejszego dokumentu jest zwany wnioskiem lub wnioskiem Komisji). W dniu 10 kwietnia 2008 r. EIOD przyjął opinię w sprawie wniosku Komisji, w której przedstawił zalecenia dotyczące udoskonalenia wniosku, tak by wynikiem proponowanych w nim zmian była jak najlepsza ochrona prywatności i danych osobowych osób (pierwsza opinia EIOD-a) ([2]).

2. EIOD z zadowoleniem odniósł się do propozycji Komisji, by wprowadzić system obowiązkowego powiadamiania o przypadkach naruszenia bezpieczeństwa, zgodnie z którym firmy byłyby zobowiązane do powiadamiania osób w przypadku, gdyby ich dane osobowe zostały narażone. EIOD z uznaniem wyraził się również na temat nowego przepisu, który umożliwi osobom prawnym (np. stowarzyszeniom konsumenckim i dostawcom usługi dostępu do Internetu) podejmowanie działań przeciwko nadawcom niezamówionych komunikatów, by w ten sposób uzupełnić istniejące narzędzia walki ze tym zjawiskiem.

3. Podczas dyskusji parlamentarnych, które poprzedziły pierwsze czytanie w Parlamencie Europejskim, EIOD przedstawił dalsze wskazówki, sporządzając uwagi odnośnie do poszczególnych kwestii, które zasygnalizowano w sprawozdaniach opracowanych przez komisje Parlamentu Europejskiego zajmujące się przeglądem dyrektyw o usłudze powszechnej ([3]) i o e-prywatności (uwagi) ([4]). Uwagi dotyczą przede wszystkim kwestii związanych z przetwarzaniem danych o ruchu i ochroną praw własności intelektualnej.

4. W dniu 24 września 2008 r. Parlament Europejski (PE) przyjął uchwałę legislacyjną w sprawie dyrektywy o e-prywatności (pierwsze czytanie) ([5]). EIOD pozytywnie odniósł się do pewnych poprawek PE, które zostały przyjęte w związku z opinią i uwagami EIOD-a wspomnianymi powyżej. Wśród ważnych zmian było objęcie dostawców usług społeczeństwa informacyjnego (tj. firm działających w Internecie) obowiązkiem powiadamiania o przypadkach naruszenia bezpieczeństwa. EIOD z zadowoleniem odniósł się również do poprawki umożliwiającej osobom prawnym i fizycznym występowanie na drogę sądową w przypadku stwierdzenia naruszenia

([1]) Przegląd dyrektywy o e-prywatności jest częścią szerszego przeglądu, którego celem jest stworzenie unijnego urzędu ds. telekomunikacji, przegląd dyrektyw 2002/21/WE, 2002/19/WE, 2002/20/WE, 2002/22/WE i 2002/58/WE, a także przegląd rozporządzenia (WE) nr 2006/2004 (zwanego dalej „przeglądem pakietu telekomunikacyjnego").

([2]) Opinia z dnia 10 kwietnia 2008 r. w sprawie wniosku dotyczącego dyrektywy zmieniającej m.in. dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. C 181 z 18.7.2008, s. 1.

([3]) Dyrektywa 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników (dyrektywa o usłudze powszechnej), Dz.U. L 108 z 24.4.2002, s. 51.

([4]) Uwagi EIOD-a dotyczące poszczególnych kwestii zasygnalizowanych w sprawozdaniu Komisji Rynku Wewnętrznego i Ochrony Konsumentów na temat przeglądu dyrektywy 2002/22/WE (usługa powszechna) i dyrektywy 2002/58/WE (e-prywatność), 2 września 2008 r. Dostępne pod następującym adresem internetowym: www.edps.europa.eu

([5]) Rezolucja legislacyjna Parlamentu Europejskiego z dnia 24 września 2008 r. w sprawie wniosku dotyczącego 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 (COM(2007) 698 – C6-0420/2007 – 2007/0248(COD)).

któregokolwiek z przepisów dyrektywy o e-prywatności (a nie tylko – jak pierwotnie proponowała w swoim wniosku Komisja – w przypadku pogwałcenia przepisów dotyczących niezamówionych komunikatów). Po pierwszym czytaniu w Parlamencie Europejskim Komisja przyjęła zmieniony wniosek dotyczący dyrektywy o e-prywatności (dalej zwany zmienionym wnioskiem) ([6]).

5. W dniu 27 listopada 2008 r. Rada osiągnęła porozumienie polityczne w sprawie przeglądu zasad odnoszących się do pakietu telekomunikacyjnego, w tym do dyrektywy o e-prywatności, które stanie się wspólnym stanowiskiem Rady (wspólne stanowisko) ([7]). Na mocy art. 251 ust. 2 Traktatu ustanawiającego Wspólnotę Europejską o wspólnym stanowisku zostanie powiadomiony PE, który może zaproponować wprowadzenie do niego poprawek.

Ogólne uwagi na temat stanowiska Rady

6. Rada zmieniła istotne elementy tekstu wniosku i nie zaakceptowała wielu spośród poprawek przyjętych przez PE. Choć niewątpliwie wspólne stanowisko zawiera elementy, które należy ocenić pozytywnie, ogólnie rzecz biorąc, EIOD jest zaniepokojony jego treścią, przede wszystkim dlatego, że we wspólnym stanowisku nie uwzględniono niektórych spośród korzystnych poprawek zaproponowanych przez PE, zmienionego wniosku ani opinii EIOD-a i europejskich organów ochrony danych przekazanych za pośrednictwem Grupy Roboczej Art. 29 ([8]).

7. Wręcz przeciwnie, w niejednym przypadku przepisy zawarte w zmienionym wniosku i poprawki PE, oferujące obywatelom pewne gwarancje, zostały skreślone lub znacznie osłabione. W rezultacie poziom ochrony przyznanej osobom we wspólnym stanowisku jest znaczenie słabszy. Z tego właśnie względu EIOD wydaje niniejszym drugą opinię, mając nadzieję, że wmiarę postępu procesu legislacyjnego dotyczącego dyrektywy o e-prywatności nowe poprawki zostaną przyjęte, co przywróci gwarancje dotyczące ochrony danych.

8. W swojej drugiej opinii EIOD skupia się na pewnych podstawowych problemach i nie powtarza wszystkich zagadnień ujętych w pierwszej opinii czy w uwagach, które w całości pozostają w mocy. W niniejszej opinii omówiono w szczególności następujące zagadnienia:

— przepisy dotyczące powiadamiania o przypadkach naruszenia bezpieczeństwa;

— zakres zastosowania dyrektywy o e-prywatności do sieci prywatnych i publicznie dostępnych sieci prywatnych;

— przetwarzanie danych o ruchu do celów bezpieczeństwa;

— umożliwienie osobom prawnym podejmowania działań w przypadku stwierdzenia naruszenia dyrektywy o e-prywatności.

9. Poruszając powyższe kwestie, niniejsza opinia analizuje wspólne stanowisko Rady i porównuje je z tekstem będącym wynikiem pierwszego czytania w PE i ze zmienionym wnioskiem Komisji. W opinii zawarto zalecenia, które mają na celu udoskonalenie przepisów dyrektywy o e-prywatności i dopilnowanie, by dyrektywa ta nadal odpowiednio chroniła prywatność i dane osobowe osób.

II. **PRZEPISY DOTYCZĄCE POWIADAMIANIA O PRZYPADKACH NARUSZENIA BEZPIECZEŃSTWA**

10. EIOD popiera przyjęcie mechanizmu powiadamiania o przypadkach naruszenia bezpieczeństwa, zgodnie z którym organy i osoby będą powiadamiane, jeśli ich dane osobowe zostały narażone ([9]). Powiadomienia o przypadkach naruszenia bezpieczeństwa mogą pomóc danym osobom podjąć konieczne kroki pozwalające złagodzić ewentualne szkody, które mogą wyniknąć z narażenia danych. Ponadto obowiązek przesyłania powiadomień z informacją o naruszeniu bezpieczeństwa zachęci firmy do polepszenia ochrony danych i zwiększenia odpowiedzialności za dane osobowe, które powierzono ich pieczy.

11. Zmieniony wniosek Komisji, tekst powstały po pierwszym czytaniu w Parlamencie Europejskim i wspólne stanowisko Rady prezentują trzy różne podejścia do obecnie omawianej kwestii powiadamiania o przypadkach naruszenia bezpieczeństwa. Każde z tych podejść ma pewne zalety. EIOD uważa jednak, że każde z tych podejść można by jeszcze udoskonalić, i radzi uwzględnić zalecenia opisane poniżej, gdy rozważane będą końcowe działania w celu przyjęcia mechanizmu powiadomień o przypadkach naruszenia bezpieczeństwa.

([6]) Zmieniony 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, 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, Bruksela, 6.11.2008, COM(2008) 723 wersja ostateczna.

([7]) Dostępne na publicznej stronie internetowej Rady.

([8]) Opinia 2/2008 w sprawie przeglądu dyrektywy 2002/58/WE o prywatności i łączności elektronicznej (dyrektywy o e-prywatności), dostępna na stronie internetowej Grupy Roboczej Art. 29.

([9]) W niniejszej opinii wyrazu „narażenie" używa się dla określenia wszelkiego rodzaju naruszeń danych osobowych, które nastąpiły w wyniku przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmiany, niedozwolonego ujawnienia przekazywanych, przechowywanych lub w inny sposób przetwarzanych danych osobowych lub niedozwolonego dostępu do nich.

12. Gdy analizujemy wspomniane trzy podejścia do mechanizmów powiadamiania o naruszeniu, należy wziąć pod uwagę pięć niezmiernie ważnych punktów: *i)* definicję naruszenia bezpieczeństwa; *ii)* podmioty objęte obowiązkiem powiadamiania („podmioty objęte obowiązkiem"); *iii)* kryterium, którego spełnienie skutkuje koniecznością powiadomienia; *iv)* określenie podmiotu odpowiedzialnego za ustalenie, czy dane naruszenie bezpieczeństwa spełnia wspomniane kryterium oraz *v)* adresatów powiadomienia.

Ogólny opis podejść przyjętych przez Komisję, Radę i PE

13. Parlament Europejski, Komisja i Rada przyjęły różne podejścia do kwestii powiadamiania o naruszeniu bezpieczeństwa. W tekście będącym wynikiem pierwszego czytania w PE zmodyfikowano pierwotny mechanizm powiadamiania o naruszeniu bezpieczeństwa, zaproponowany przez Komisję w jej wniosku ([10]). W myśl podejścia PE, obowiązek powiadamiania mieliby nie tylko dostawcy publicznie dostępnych usług łączności elektronicznej (PPECS), ale również dostawcy usług społeczeństwa informacyjnego (ISSP). Ponadto, w myśl tego podejścia, o wszelkich przypadkach naruszenia danych osobowych należałoby powiadamiać krajowy organ regulacyjny lub właściwe organy (razem zwane „organami"). Gdyby te organy stwierdziły, że dane naruszenie jest poważne, wymagałyby od dostawców PPECS i dostawców ISSP bezzwłocznego powiadomienia o tym fakcie osoby, której dane zostały naruszone. W przypadku naruszeń, które stanowią natychmiastowe i bezpośrednie niebezpieczeństwo, dostawcy PPECS i dostawcy ISSP powiadamialiby dane osoby przed powiadomieniem organów i nie czekaliby na urzędowe rozstrzygnięcie. Wyjątek od obowiązku powiadamiania konsumentów dotyczy podmiotów, które przed organami mogą wykazać, że *„zastosowane zostały odpowiednie technologiczne środki ochrony"*, sprawiające, że dane te są nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich.

14. W myśl podejścia Rady, powiadamiani byliby zarówno abonenci, jak i organy, jednak wyłącznie w przypadkach, gdy dany podmiot objęty obowiązkiem uzna, że naruszenie stanowi *poważne zagrożenie* dla prywatności abonenta (tj. może doprowadzić do kradzieży lub sfałszowania tożsamości, szkód fizycznych, znaczącego upokorzenia lub naruszenia dobrego imienia).

15. W zmienionym wniosku Komisja podtrzymuje zaproponowany przez PE obowiązek powiadamiania organów o wszystkich przypadkach naruszenia bezpieczeństwa. W odróżnieniu od podejścia zaproponowanego w tekście PE zmieniony wniosek zawiera jednak wyłączenie z obowiązku powiadamiania osób, których dane zostały naruszone, jeśli dostawca PPECS może wykazać przed właściwym organem, że *i)* w następstwie naruszenia danych osobowych nie istnieje *„uzasadnione prawdopodobieństwo"* wystąpienia szkody (np. strat gospodarczych, szkody społecznej lub kradzieży tożsamości) lub że *ii)* do danych, których dotyczyło naruszenie bezpieczeństwa, zostały zastosowane *„odpowiednie technologiczne środki ochrony"*. A zatem podejście przyjęte przez Komisję zakłada analizę potencjalnych szkód, jeśli chodzi o powiadamianie poszczególnych osób.

([10]) Zagadnienia tego dotyczą w szczególności poprawek PE: 187, 124–127, a także 27, 21 i 32.

16. Trzeba zauważyć, że w myśl podejścia przyjętego przez PE ([11]) i Komisję ostatecznie to do *organów* należy ustalenie, czy naruszenie miało charakter poważny lub czy istnieje uzasadnione prawdopodobieństwo, że spowoduje ono szkody. Z kolei w myśl podejścia przyjętego przez Radę decyzję o powiadomieniu podejmują *zainteresowane podmioty*.

17. Zarówno podejście przyjęte przez Radę, jak i podejście przyjęte przez Komisję dotyczą wyłącznie dostawców PPECS, a nie, jak w przypadku podejścia przyjętego przez PE, także dostawców ISSP.

Definicja naruszenia bezpieczeństwa

18. EIOD z zadowoleniem zauważa, że wszystkie trzy propozycje legislacyjne zawierają tę samą definicję powiadomienia o naruszeniu bezpieczeństwa; jest ono opisane jako *„naruszenie bezpieczeństwa prowadzące do przypadkowego lub bezprawnego zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych przekazywanych, przechowywanych lub winny sposób przetwarzanych […]"* ([12]).

19. Jak wyjaśniono poniżej, EIOD przyjmuje z zadowoleniem tą definicję, ponieważ jest ona wystarczająca szeroka, by objąć większość stosownych sytuacji, w których można by uzasadnić obowiązek powiadamiania o naruszeniu.

20. Po pierwsze, definicja ta obejmuje przypadki, gdy strona trzecia uzyskała *nieuprawniony dostęp* do danych osobowych, np. włamała się do serwera zawierającego dane osobowe i wyszukała takie informacje.

21. Po drugie, definicja taka obejmowałaby także sytuacje, w których nastąpiła utrata lub ujawnienie danych osobowych, choć należy jeszcze wykazać, że stało się tak w wyniku nieuprawnionego dostępu. Chodziłoby o takie sytuacje, jak utrata danych osobowych (np. CD-ROM-ów, pamięci USB czy innych przenośnych urządzeń) lub ich publiczne udostępnienie przez regularnych użytkowników (np. gdy plik zawierający dane o pracownikach został przez nieuwagę czasowo udostępniony w dostępnym dla wszystkich miejscu w Internecie). Ponieważ często brak jest dowodów na to, że takie dane mogą lub nie mogą w jakimś momencie być dostępne nieuprawnionym stronom trzecim lub przez nie wykorzystane, wydaje się, że zakres definicji powinien obejmować także takie przypadki. Z tego względu EIOD zaleca, by zachować tę definicję. EIOD zaleca również, by definicję naruszenia bezpieczeństwa zawarto w art. 2 dyrektywy o e-prywatności, ponieważ przyczyniłoby się to do większej spójności z ogólną strukturą tej dyrektywy i zapewniło większą klarowność.

([11]) Z wyjątkiem przypadków, gdy istnieje natychmiastowe i bezpośrednie zagrożenie, w których to przypadkach podmioty muszą najpierw powiadomić konsumentów.

([12]) Art. 2 lit. i) wspólnego stanowiska i zmienionego wniosku oraz art. 3 ust. 3 tekstu będącego wynikiem pierwszego czytania w PE.

Podmioty, które należy objąć obowiązkiem powiadamiania

22. W myśl podejścia przyjętego przez PE obowiązkiem powiadamiania objęci są zarówno dostawcy PPECS, jak i dostawcy ISSP. Jednak w myśl mechanizmów przewidzianych przez Radę i Komisję wyłącznie dostawcy PPECS, tacy jak firmy telekomunikacyjne lub dostawcy usługi dostępu do Internetu, będą mieli obowiązek powiadamiania danych osób w przypadku, gdy miało miejsce naruszenie bezpieczeństwa prowadzące do narażenia ich danych osobowych. Inne sektory działalności, np. banki internetowe, sklepy internetowe, podmioty świadczące usługi zdrowotne przez Internet i inne, nie mają obowiązku powiadamiania. Z powodów wyjaśnionych poniżej EIOD uważa, że z punktu widzenia porządku publicznego, niesłychanie istotne jest dopilnowanie, by usługi społeczeństwa informacyjnego, w tym przedsiębiorstwa internetowe, banki internetowe, podmioty świadczące usługi zdrowotnie przez Internet itd. również objęte były obowiązkiem powiadamiania.

23. Po pierwsze, EIOD odnotowuje, że choć celem działań skutkujących naruszeniem bezpieczeństwa są z pewnością firmy telekomunikacyjne, co uzasadnia obowiązek powiadamiania, to samo odnosi się do pewnych typów firm/dostawców. Istnieje takie samo jeśli nie większe prawdopodobieństwo, że celem działań skutkujących naruszeniem bezpieczeństwa staną się internetowe sklepy, banki i apteki. A zatem, gdy rozważy się zagrożenie, nic nie przemawia za ograniczeniem zakresu obowiązku powiadomienia o naruszeniu bezpieczeństwa tylko do dostawców PPECS. Potrzebę szerszego podejścia unaoczniają doświadczenia innych państw. Na przykład w Stanach Zjednoczonych niemal wszystkie stany (w chwili obecnej ponad 40) wprowadziły ustawy dotyczące powiadamiania o naruszeniu bezpieczeństwa, które mają szerszy zakres zastosowania i obejmują nie tylko dostawców PPECS, lecz wszystkie podmioty przechowujące wymagane dane osobowe.

24. Po drugie, choć oczywistym jest, że naruszenie typów danych osobowych regularnie przetwarzanych przez dostawców PPECS może mieć wpływ na prywatność danej osoby, to samo odnosi się – jeśli nie w większym stopniu – do typów informacji osobowych przetwarzanych przez dostawców ISSP. Banki i inne instytucje finansowe mogą z pewnością posiadać bardzo poufne informacje (np. dane konta bankowego), których ujawnienie może spowodować wykorzystanie ich do kradzieży tożsamości. Również ujawnienie bardzo wrażliwych informacji dotyczących stanu zdrowia przez podmioty świadczące usługi zdrowotne przez Internet może być szczególnie szkodliwe dla danych osób. Dlatego też typy danych osobowych, które mogą zostać narażone, również przemawiają za szerszym stosowaniem obowiązku powiadamiania o naruszeniu bezpieczeństwa, tak by objąć nim przynajmniej również dostawców ISSP.

25. Rozszerzenie zakresu zastosowania tego artykułu, tj. zakresu podmiotów, które zostałyby objęte tym wymogiem, zakwestionowano z pewnych względów prawnych. Jako główną przeszkodę dla stosowania obowiązku powiadamiania również do dostawców ISSP podaje się fakt, że dyrektywa o e-prywatności ma jako taka zastosowanie wyłącznie do dostawców PPECS.

26. W tym kontekście EIOD pragnąłby przypomnieć, że: *i)* z punktu widzenia prawa nic nie stoi na przeszkodzie, by zakresem stosowania pewnych przepisów tej dyrektywy objąć również podmioty inne niż dostawcy PPECS. Prawodawca wspólnotowy dysponuje w tym zakresie pełną swobodą. *ii)* W obowiązującej dyrektywie o e-prywatności istnieją już precedensy polegające na zastosowaniu do podmiotów innych niż dostawcy PPECS.

27. Na przykład art. 13 ma zastosowanie nie tylko do dostawców PPECS, lecz również do każdej firmy, która wysyła niezamówione komunikaty; wymaga też od tych firm uprzedniego otrzymania zgody adresatów. Ponadto art. 5 ust. 3 dyrektywy o e-prywatności, zakazujący m.in. przechowywania informacji takich jak pliki *cookie* w urządzeniach końcowych użytkowników, obowiązuje nie tylko dostawców PPECS, lecz również każdego, kto próbuje przechowywać informacje lub uzyskać dostęp do informacji przechowywanych w urządzeniu końcowym danej osoby. Co więcej, w ramach obecnej procedury legislacyjnej Komisja zaproponowała nawet rozszerzenie zastosowania art. 5 ust. 3 na przypadki, w których podobne technologie (pliki cookie/oprogramowanie szpiegujące) nie są dostarczane jedynie za pośrednictwem systemów łączności elektronicznej, lecz wszelkimi innymi możliwymi metodami (w trakcie pobierania plików z Internetu lub za pośrednictwem zewnętrznych nośników danych, takich jak CD-ROM-y, pamięci USB itd.). Wszystkie te elementy należy pochwalić i powinny one zostać zachowane, stanowią one jednak również odpowiednie precedensy w ramach obecnej dyskusji dotyczącej zakresu zastosowania.

28. Poza tym w ramach obecnej procedury legislacyjnej Komisja, PE i zapewne Rada zaproponowały nowy art. 6 ust. 6a, omówiony poniżej, który ma zastosowanie do podmiotów innych niż dostawcy PPECS.

29. Na koniec, wziąwszy pod uwagę wszechstronne pozytywne aspekty obowiązku powiadamiania o przypadkach naruszenia bezpieczeństwa, obywatele prawdopodobnie będą oczekiwać takich korzyści, nie tylko gdy ich dane osobowe zostały narażone przez dostawców PPECS, lecz również przez dostawców ISSP. Oczekiwania obywateli mogą nie zostać spełnione, jeśli np. nie będą oni powiadamiani, gdy bank internetowy utracił informacje dotyczące ich konta bankowego.

30. Podsumowując, EIOD jest przekonany, że wyciągnięcie pełnych korzyści z powiadamiania o naruszeniu bezpieczeństwa będzie łatwiejsze, jedynie gdy w zakres podmiotów objętych obowiązkiem wejdą zarówno dostawcy PPECS, jak i dostawcy ISSP.

Kryterium, którego spełnienie skutkuje koniecznością powiadomienia

31. Jeśli chodzi o kryterium, którego spełnienie skutkuje koniecznością powiadomienia, to – jak wyjaśniono poniżej – EIOD jest zdania, że zawarte w zmienionym wniosku kryterium „*uzasadnionego prawdopodobieństwa wystąpienia szkody*" jest najwłaściwszym z trzech zaproponowanych kryteriów. Należy jednak dopilnować, by pojęcie „szkody" było wystarczające szerokie, by objąć wszystkie stosowne przypadki negatywnych skutków dla prywatności lub innych uzasadnionych interesów danych osób. W przeciwnym wypadku korzystniej byłoby stworzyć nowe kryterium, zgodnie z którym powiadomienie byłoby obowiązkowe, „*jeśli istnieje uzasadnione prawdopodobieństwo, że naruszenie będzie miało niekorzystne skutki dla danych osób*".

32. Jak opisano w poprzedniej części, PE, Komisja i Rada przyjęły różne podejścia, jeśli chodzi o warunki, po spełnieniu których dane osoby muszą zostać powiadomione (zwane „kryterium"). Oczywiście ilość powiadomień otrzymywanych przez dane osoby będzie w dużej mierze zależna od kryterium, którego spełnienie będzie skutkowało koniecznością powiadomienia.

33. W myśl mechanizmów zaproponowanych przez Radę i Komisję, powiadomienie musi być przekazane, gdy naruszenie stanowi „*poważne naruszenie prywatności abonenta*" (Rada) lub gdy „*w wyniku naruszenia istnieje uzasadnione prawdopodobieństwo wystąpienia szkody dla interesów konsumenta*" (Komisja). W myśl systemu zaproponowanego przez PE kryterium, którego spełnienie skutkuje koniecznością powiadomienia danych osób, jest „*powaga zagrożenia*" (tj. powiadomienie danych osób jest wymagane, jeśli naruszenie zostanie uznane za „*poważne*"). Jeśli to kryterium nie zostanie spełnione, powiadomienie nie jest wymagane ([13]).

34. EIOD rozumie, że można twierdzić, iż jeśli dane osobowe zostały narażone, osoby, do których te dane należą, mają prawo wiedzieć – w każdych okolicznościach – o tym zdarzeniu. Wypadałoby się jednak zastanowić, czy w świetle innych interesów i innych względów jest to właściwe rozwiązanie.

35. Pojawiły się sugestie, że obowiązek wysyłania powiadomienia za każdym razem, gdy narażone zostały dane osobowe – innymi słowy bez ograniczeń – może prowadzić do nadmiernej liczby powiadomień i zmęczenia nimi, a co za tym idzie zobojętnienia na nie. Jak opisano poniżej EIOD potrafi zrozumieć ten argument; niemniej jednak chciałby podkreślić swoją obawę, że nadmierna liczba powiadomień jest możliwym wskaźnikiem szeroko zakrojonego zjawiska niedostatecznego zabezpieczania informacji.

36. Jak wspomniano powyżej, EIOD dostrzega potencjalnie negatywne skutki nadmiernej liczby powiadomień i chciałby dopomóc w dopilnowaniu, by przyjęte ramy prawne dotyczące powiadamiania o naruszeniu bezpieczeństwa nie dały takiego skutku. Gdyby dane osoby miały otrzymywać częste powiadomienia o naruszeniu bezpieczeństwa nawet w sytuacjach, gdy takie naruszenie nie ma niekorzystnych skutków, takich jak szkoda czy cierpienie, mogłoby się to skończyć zaprzepaszczeniem jednego z kluczowych celów powiadamiania, gdyż – jak na ironię – osoby te mogłyby zignorować powiadomienia o takich przypadkach, w których faktycznie powinny podjąć działania, by się chronić. Znalezienie równowagi w przekazywaniu istotnych powiadomień jest zatem ważne, ponieważ jeśli dane osoby nie reagują na otrzymywane powiadomienia, skuteczność systemów powiadamiania bardzo maleje.

37. Aby wybrać odpowiednie kryterium, którego stosowanie nie doprowadzi do nadmiernej liczby powiadomień, obok samego kryterium należy wziąć pod uwagę inne czynniki, zwłaszcza definicję naruszenia bezpieczeństwa i informacje objęte obowiązkiem powiadamiania. Z tego względu EIOD odnotowuje, że w myśl trzech proponowanych podejść liczba powiadomień może być wysoka z uwagi na szeroką definicję naruszenia bezpieczeństwa, omówioną powyżej. Tę obawę przed nadmierną liczbą powiadomień zwiększa jeszcze fakt, że definicja naruszenia bezpieczeństwa dotyczy wszystkich typów danych osobowych. Choć EIOD uważa, że nieograniczanie typów danych osobowych podlegających powiadamianiu to słuszne podejście – w odróżnieniu od innych podejść, takich jak przyjęte w ustawach amerykańskich, w których wymogi są skupione na wrażliwym charakterze informacji – czynnik ten należy jednak wziąć pod uwagę.

38. W świetle powyższego i uwzględniając łącznie różne zmienne, EIOD uważa, że należałoby ustanowić pewne kryterium lub pewien próg, w przypadku niespełnienia lub nieprzekroczenia którego powiadomienie nie jest obowiązkowe.

39. Oba zaproponowane kryteria tj. fakt, że naruszenie stanowi poważne zagrożenie dla prywatności, lub fakt, że istnieje uzasadnione prawdopodobieństwo wyrządzenia przez to naruszenie szkód, wydają się uwzględniać np. szkodę społeczną lub szkodę dla dobrego imienia oraz straty gospodarcze. Takie kryteria uwzględniałyby np. przypadki narażenia na kradzież tożsamości wskutek ujawnienia elementów niedostępnych publicznie, pozwalających zidentyfikować daną osobę, takich jaki numery paszportu, a także przypadki ujawnienia informacji na temat prywatnego życia danej osoby. EIOD z zadowoleniem przyjmuje to podejście. Jest przekonany, że nie można by wyciągnąć pełni pożytku z powiadamiania o naruszeniu bezpieczeństwa, jeśli system powiadamiania dotyczyłby wyłącznie naruszeń prowadzących do strat gospodarczych.

([13]) Zob. przypis 11 dotyczący wyjątku od tej zasady.

40. Z dwóch zaproponowanych kryteriów EIOD opowiada się za zaproponowanym przez Komisję kryterium uzasadnionego prawdopodobieństwa powstania szkody, ponieważ zapewniłoby ono odpowiedniejszy poziom ochrony osób. Naruszenia znacznie łatwiej będzie zakwalifikować jako wymagające powiadomienia, jeśli będzie istnieć uzasadnione prawdopodobieństwo powstania szkody dla prywatności danych osób niż jeśli z naruszeniami takimi ma się wiązać poważne zagrożenie wystąpieniem takiej szkody. A zatem uwzględnianie wyłącznie naruszeń stanowiących poważne zagrożenie dla prywatności danych osób znacznie ograniczyłoby liczbę naruszeń objętych obowiązkiem powiadomienia. Uwzględnianie wyłącznie takich naruszeń pozostawiłoby dostawcom PPECS i ISSP nadmierną swobodę w podejmowaniu decyzji, czy wymagane jest powiadomienie, ponieważ o wiele łatwiej byłoby im stwierdzić, że nie istnieje poważne zagrożenie szkodą niż że nie istnieje uzasadnione prawdopodobieństwo powstania szkody. Oczywiście należy unikać nadmiernej liczby powiadomień, w sumie należy jednak docenić pożytek dla ochrony prywatności danych osób z istnienia wątpliwości, a osoby te należy chronić przynajmniej w przypadkach, w których istnieje uzasadnione prawdopodobieństwo, że dane naruszenie będzie miało dla nich niekorzystne skutki. Ponadto termin „*uzasadnione prawdopodobieństwo*" będzie skuteczniejszy w praktycznym stosowaniu, zarówno dla podmiotów objętych obowiązkiem powiadamiania, jak i dla właściwych organów, ponieważ wymaga on obiektywnej oceny przypadku i odpowiednich okoliczności jego zaistnienia.

41. Ponadto naruszenia danych osobowych mogą powodować szkody, które trudno jest zmierzyć i które mogą mieć różny charakter. W zależności bowiem od indywidualnych okoliczności ujawnienie tego samego typu danych może spowodować znaczne szkody dla jednej osoby, a mniejsze – dla innej. Niepoprawne byłoby kryterium, zgodnie z którym szkoda powinna być rzeczowa, znaczna lub poważna. I tak podejście zaproponowane przez Radę, zgodnie z którym naruszenie powinno poważnie naruszać czyjąś prywatność, nie zapewniałoby właściwej ochrony osób, ponieważ zawiera ono wymóg, by skutek dla prywatności miał poważny charakter. Daje to również pole do subiektywnej oceny.

42. Choć, jak opisano powyżej, uzasadnione prawdopodobieństwo powstania szkody wydaje właściwym kryterium powiadamiania o naruszeniu bezpieczeństwa, EIOD obawia się, że może ono nie obejmować wszystkich sytuacji, w których uzasadnione jest powiadomienie danych osób, tj. sytuacji, w których istnieje uzasadnione prawdopodobieństwo wystąpienia niegatywnych skutków dla prywatności lub innych zasadnych praw danych osób. Dlatego też można by rozważyć kryterium, zgodnie z którym powiadomienie byłoby konieczne, „*jeśli istnieje uzasadnione prawdopodobieństwo, że naruszenie będzie miało niekorzystne skutki dla danej osoby*".

43. To alternatywne kryterium jest na dodatek spójne z unijnymi przepisami dotyczącymi ochrony danych. Dyrektywa o ochronie danych często bowiem odwołuje się do niekorzystnych skutków dla praw i wolności osób, których dane dotyczą. Na przykład art. 18 i motyw 49, które dotyczą obowiązku prowadzenia rejestru operacji przetwarzania danych i udostępnienia go organom ochrony danych, upoważniają państwa członkowskie do zwolnienia z tego obowiązku w przypadkach, w których przetwarzanie danych „*nie wpłynie niekorzystnie na prawa wolności osób, których dane dotyczą*". Podobne sformułowanie jest użyte w art. 16 ust. 6 wspólnego stanowiska i ma umożliwić osobom prawnym podejmowanie działań prawnych przeciwko autorom niezamówionych komunikatów.

44. Ponadto, biorąc powyższe pod uwagę, można by również oczekiwać od podmiotów objętych obowiązkiem powiadamiania i w szczególności od organów właściwych do egzekwowania przepisów dotyczących ochrony danych, że będą lepiej zaznajomione z powyższym kryterium, dzięki czemu łatwiej im będzie dokonać oceny tego, czy dane naruszenie spełnia wyznaczone kryterium.

Podmiot, który podejmuje decyzję, czy dane naruszenie bezpieczeństwa spełnia wyznaczone kryterium

45. W myśl podejścia zaproponowanego przez PE (z wyjątkiem przypadków, gdy zagrożenie jest natychmiastowe) i w myśl zmienionego wniosku Komisji to organy państw członkowskich podejmują decyzję, czy dane naruszenie odpowiada kryterium, którego spełnienie pociąga za sobą obowiązek powiadomienia danych osób.

46. EIOD uważa, że zaangażowanie organu odgrywa istotną rolę w określaniu, czy kryterium zostało spełnione, ponieważ do pewnego stopnia stanowi to gwarancję właściwego stosowania przepisów. Taki system może zapobiec sytuacjom, w których firmy niewłaściwie ocenią, że naruszenie nie jest szkodliwe/poważne, i nie dokonają powiadomienia, choć w rzeczywistości jest ono konieczne.

47. Z drugiej strony EIOD obawia się, że system, w ramach którego organy mają przeprowadzać taką ocenę, może być niepraktyczny i trudny w stosowaniu lub w praktyce może przynieść efekt przeciwny do zamierzonego. Może zatem nawet ograniczyć danym osobom gwarancje ochrony danych.

48. W myśl takiego podejścia bowiem organy ochrony danych prawdopodobnie zostaną zalane powiadomieniami o naruszeniu bezpieczeństwa i dokonanie koniecznych ocen może im przysporzyć poważnych trudności. Należy pamiętać, że aby przeprowadzić ocenę tego, czy dane naruszenie spełnia kryterium, organy będą musiały dysponować wystarczającymi poufnymi informacjami, często skomplikowanymi technicznie, które będą musiały opracować bardzo szybko. Uwzględniając trudność oceny i fakt, że niektóre organy dysponują ograniczonymi zasobami, EIOD obawia się, że organom bardzo trudno będzie sprostać temu obowiązkowi i że jego realizacja może pochłonąć zasoby przeznaczone na inne ważne priorytety. Taki system może ponadto wywierać na organy nadmierną presję; jeśli bowiem zdecydują, że naruszenie nie jest poważne, a mimo to dane osoby ucierpią, organy mogą potencjalnie zostać obciążone odpowiedzialnością.

49. Trudność ta staje się tym bardziej oczywista, jeśli weźmie się pod uwagę, że kluczowym czynnikiem w ograniczeniu zagrożeń wynikających z naruszeń bezpieczeństwa, jest czas. O ile organy nie będą w stanie przeprowadzić oceny w bardzo krótkim czasie, dodatkowy czas potrzebny im na przeprowadzenie takich ocen może spowodować, że szkody poniesione przez dane osoby będą większe. Dlatego też, ten dodatkowy etap, który w zamyśle ma zapewnić osobom lepszą ochronę, może – jak na ironię – doprowadzić to tego, że ochrona ta będzie mniej skuteczna niż w ramach systemów opartych na bezpośrednim powiadamianiu.

50. Z wyżej podanych powodów EIOD jest zdania, że należałoby raczej ustanowić system, w myśl którego to dane podmioty przeprowadzałyby ocenę tego, czy naruszenie spełnia kryterium – tak, jak przewiduje to Rada w zaproponowanym podejściu.

51. Aby jednak uniknąć ryzyka ewentualnych nadużyć, np. sytuacji, w której podmioty odmawiałyby powiadomienia, choć jasno wymagałyby tego okoliczności, sprawą najwyższej wagi jest, by istniały pewne gwarancje ochrony danych opisane poniżej.

52. Po pierwsze, obowiązkowi spoczywającemu na objętych nim podmiotach i dotyczącemu podjęcia decyzji, czy powinny dokonać powiadomienia, musi rzecz jasna towarzyszyć inny obowiązek, polegający na obowiązkowym powiadamianiu organów o wszelkich naruszeniach, które spełniają wymagane kryterium. Dane podmioty powinny w takich przypadkach być zobowiązane do poinformowania organów o naruszeniu i o przyczynach podjęcia takiej czy innej decyzji dotyczącej powiadomienia, a także o treści dokonanego powiadomienia.

53. Po drugie, organy powinny rzeczywiście mieć możliwość nadzoru. Wypełniając to zadanie, organy powinny mieć możliwość – ale nie obowiązek – badania okoliczności zaistnienia naruszenia i domagania się wszelkich niezbędnych działań naprawczych ([14]). Możliwości te powinny obejmować nie tylko powiadamianie danych osób (o ile nie zostało ono jeszcze dokonane), lecz również nakładanie obowiązku podjęcia działań służących zapobieżeniu kolejnym naruszeniom. Organom należy przyznać faktyczne uprawnienia i zasoby w tym zakresie; powinny one również dysponować niezbędnym polem manewru, jeśli chodzi o decyzję, kiedy reagować na powiadomienie o naruszeniu bezpieczeństwa. Innymi słowy, dałoby to organom możliwość dokonywania wyboru i angażowania się w dochodzenia w sprawie np. rzeczywiście szkodliwych naruszeń bezpieczeństwa na dużą skalę, przez sprawdzanie i egzekwowanie spójności z wymogami prawa.

54. Aby umożliwić organom wykonanie tego założenia, oprócz uprawnień uznanych na mocy dyrektywy o e-prywatności np. w art. 15a ust. 3 i na mocy dyrektywy o ochronie danych, EIOD sugeruje dodanie fragmentu w brzmieniu: „*Jeśli dany abonent lub dana osoba nie zostali jeszcze powiadomieni, to po zbadaniu charakteru naruszenia właściwy organ krajowy może wystąpić do dostawcy PPECS lub ISSP o dokonanie powiadomienia*".

55. Ponadto EIOD zaleca, by PE i Rada potwierdziły – jak zaproponował EP (poprawka 122, art. 4. ust. 1 lit. a)) – że podmioty mają obowiązek przeprowadzić ocenę ryzyka i określić, których systemów mają zamiar użyć do przetwarzania konkretnych danych osobowych. Stosownie do tego obowiązku podmioty opracują zindywidualizowaną i dokładną definicję środków bezpieczeństwa, które będą stosowane w przypadku tych danych i którymi powinny dysponować organy. Jeśli nastąpi naruszenie bezpieczeństwa, istnienie takiego obowiązku pozwoli objętym nim podmiotom – i ostatecznie także podmiotom sprawującym swoje zadania nadzorcze – określić, czy narażenie takich informacji może mieć niekorzystne skutki dla danych osób lub wyrządzić im szkodę.

56. Po trzecie, obowiązkowi spoczywającemu na objętych nim podmiotach polegającemu na podejmowaniu decyzji, czy powinny powiadomić dane osoby, powinien towarzyszyć obowiązek zachowania szczegółowych i kompleksowych, chronologicznie posegregowanych informacji odnoszących się do kontroli wewnętrznej i dotyczących wszelkich naruszeń, które miały miejsce, oraz wszelkich powiadomień, a także wszelkich środków podjętych, by zapobiec naruszeniom w przyszłości. Do tych chronologicznie posegregowanych informacji odnoszących się do kontroli wewnętrznej dostęp muszą mieć organy – do celów przeglądu i ewentualnego dochodzenia. Pozwoli to organom wywiązać się ze swoich zadań nadzorczych. Można by to osiągnąć, dodając fragment w brzmieniu: „*Dostawcy PPECS i dostawcy ISSP prowadzą i zachowują kompleksowe rejestry zawierające szczegółowe informacje na temat wszelkich zaistniałych przypadków naruszenia bezpieczeństwa, stosowne informacje techniczne z tym związane oraz informacje na temat podjętych działań naprawczych. Rejestry te zawierają również informacje o wszelkich powiadomieniach przesłanych abonentom lub danym osobom oraz właściwym organom krajowym, w tym datę przesłania powiadomienia i jego treść. Akta te są przedstawiane na wniosek właściwego organu krajowego*".

57. Oczywiście, aby zapewnić spójność wdrażania tego kryterium, a także innych odpowiednich aspektów ram naruszeń bezpieczeństwa, takich jak format i procedury powiadamiania, Komisja powinna przyjąć techniczne środki wykonawcze, po konsultacji z EIOD-em, Grupą Roboczą Art. 29 i odpowiednimi zainteresowanymi stronami.

([14]) Art. 15a ust. 3 uznaje te uprawnienia nadzorcze, stanowiąc, że „*państwa członkowskie zapewniają, aby właściwe organy krajowe oraz, w stosownych przypadkach, inne podmioty krajowe, dysponowały wszelkimi uprawnieniami i środkami niezbędnymi do prowadzenia dochodzeń, w tym uprawnieniami do uzyskiwania wszelkich istotnych informacji, których mogą potrzebować, aby nadzorować i egzekwować przestrzeganie przepisów krajowych przyjętych zgodnie z niniejszą dyrektywą*".

Adresaci powiadomienia

58. Jeśli chodzi o adresatów powiadomień, EIOD preferuje terminologię stosowaną przez PE i Komisję od terminologii zaproponowanej przez Radę. PE zastąpił bowiem wyraz „abonenci" wyrazem „użytkownicy". Komisja używa terminów: „abonenci" i „osoba indywidualna". Zarówno sformułowania stosowane przez PE, jak i sformułowania stosowane przez Komisję uwzględniają, że adresatami powiadomień są nie tylko obecni abonenci, lecz również dawni abonenci i strony trzecie, takie jak użytkownicy, którzy mają do czynienia z pewnymi podmiotami objętymi obowiązkiem powiadamiania, nie są jednak abonentami ich usług. EIOD cieszy się z takiego podejścia i apeluje do PE i Rady, by je zachowały.

59. EIOD zauważa jednak pewne niespójności, jeśli chodzi o terminologię w tekście będącym wynikiem pierwszego czytania w PE; należy im zaradzić. Na przykład wyraz „abonenci" został zastąpiony w większości miejsc – choć nie we wszystkich – wyrazem „użytkownicy", w niektórych zaś innych miejscach – wyrazem „konsumenci". Terminy te należy uspójnić.

III. ZAKRES ZASTOSOWANIA DYREKTYWY O E-PRYWATNOŚCI: SIECI PUBLICZNE I PRYWATNE

60. Art. 3 ust. 1 obecnej dyrektywy o e-prywatności określa, jakich podmiotów przede wszystkim ona dotyczy; są to mianowicie podmioty przetwarzające dane *„w związku z"* świadczeniem publicznych usług łączności elektronicznej w publicznych sieciach łączności (wyżej zwane PPECS) ([15]). Przykładami usług PPECS są: dostarczanie dostępu do Internetu, przesyłanie informacji poprzez sieci elektroniczne, połączenia telefonii mobilnej i stacjonarnej itp.

61. PE uchwalił poprawkę 121 zmieniającą art. 3 pierwotnego wniosku Komisji, zgodnie z którą zakres zastosowania dyrektywy o e-prywatności rozszerzono na *„przetwarzanie danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych i prywatnych sieciach łączności oraz w publicznie dostępnych sieciach prywatnych we Wspólnocie, […]"* (art. 3 ust. 1 dyrektywy o e-prywatności). Niestety zarówno Radzie, jak i Komisji trudno było zaakceptować tę poprawkę i dlatego takie podejście nie zostało uwzględnione ani w tekście wspólnego stanowiska ani w zmienionym wniosku.

Stosowanie dyrektywy o e-prywatności do publicznie dostępnych sieci prywatnych

62. Z przyczyn wyjaśnionych poniżej i aby pomóc w osiągnięciu konsensusu, EIOD zachęca do zachowania istoty poprawki 121. EIOD sugeruje ponadto, by włączyć poprawkę, która pozwoli jeszcze doprecyzować typy usług, które zostałyby objęte rozszerzonym zakresem zastosowania.

63. Prywatne sieci są często wykorzystywane do świadczenia usług łączności elektronicznej, takich jak dostęp do Internetu dla nieokreślonej liczby osób, która może być spora. Dzieje się tak np. w przypadku dostępu do Internetu w kafejkach internetowych, a także w punktach dostępu do Wi-Fi znajdujących się w hotelach, restauracjach, portach lotniczych, pociągach i innych placówkach dostępnych dla społeczeństwa, gdzie takie usługi są często świadczone jako dodatek do innych usług (np. napojów, zakwaterowania itd.).

64. We wszystkich powyższych przykładach usługa łączności, np. dostęp do Internetu, jest udostępniana społeczeństwu nie za pośrednictwem sieci publicznej, lecz za pośrednictwem sieci, którą można uznać za prywatną, tj. sieci obsługiwanej przez podmiot prywatny. Poza tym, choć w powyższych przykładach usługa łączności jest świadczona społeczeństwu, to ze względu na to, że użyta sieć jest prywatna, a nie publiczna, można twierdzić, że usługi te nie podlegają wszystkim przepisom dyrektywy o e-prywatności lub przynajmniej niektórym z jej artykułów ([16]). W rezultacie w takich przypadkach prawa podstawowe osób zagwarantowane w dyrektywie o e-prywatności nie są chronione, zaś między użytkownikami korzystającymi z usług dostępu do Internetu za pośrednictwem publicznych firm telekomunikacyjnych i tymi, którzy mają dostęp do tych samych usług za pośrednictwem sieci prywatnych, powstaje nierówność względem prawa. Dzieje się tak, choć zagrożenia dla prywatności i danych osobowych osób są we wszystkich tych przypadkach takie same jak w przypadku, gdy do świadczenia danej usługi używane są sieci publiczne. Podsumowując – wydaje się, że nie istnieje powód, dla którego na mocy dyrektywy usługi łączności świadczone poprzez sieć prywatną miałyby być traktowane inaczej niż usługi świadczone przez sieć publiczną.

65. Dlatego też EIOD opowiedziałby się za poprawką, taką jak poprawka 121 PE, zgodnie z którą dyrektywa o e-prywatności miałaby zastosowanie również do przetwarzania danych osobowych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej w *prywatnych* sieciach łączności.

66. EIOD rozumie jednak, że takie sformułowanie mogłoby mieć nieprzewidziane i prawdopodobnie niezamierzone skutki. Proste odniesienie do sieci prywatnych można by bowiem interpretować jako odniesienie również do sytuacji, których nie zamierzano regulować tą dyrektywą. Na przykład można by utrzymywać, że dosłowne lub ścisłe interpretowanie tego sformułowania mogłoby doprowadzić do tego, że zakresem zastosowania dyrektywy zostaliby objęci właściciele domów wyposażonych

([15]) „Niniejszą dyrektywę stosuje się do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności".

([16]) Wychodząc z przeciwnego założenia, można by przekonywać, że skoro usługa łączności jest świadczona społeczeństwu, to nawet jeśli sieć jest prywatna, świadczenie takich usług podlega obowiązującym ramom prawnych, pomimo tego, że sieć jest prywatna. I tak np. we Francji pracodawcy udostępniający Internet swoim pracownikom bywali traktowani na równi z dostawcami dostępu do Internetu, którzy oferują dostęp do Internetu na zasadach komercyjnych. Nie jest to powszechnie akceptowana wykładnia.

w bezprzewodowe sieci Wi-Fi ([17]), którzy umożliwiają podłączenie się wszystkim w zasięgu tych sieci (zwykle w domu); nie taki jednak zamysł przyświecał autorom poprawki 121. Aby uniknąć opisanej sytuacji, EIOD sugeruje, by zmienić brzmienie poprawki 121 i uwzględnić w zakresie zastosowania dyrektywy o e-prywatności „*przetwarzanie danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności lub w publicznie dostępnych prywatnych sieciach łączności we Wspólnocie, ….*"

67. Dzięki takiemu sformułowaniu jasne byłoby, że dyrektywie o e-prywatności podlegają tylko te prywatne sieci, które są publicznie dostępne. Stosowanie przepisów dyrektywy o e-prywatności *tylko* do *publicznie dostępnych sieci prywatnych* (nie zaś do wszystkich sieci prywatnych) wyznacza pewną granicę, przez co dyrektywie podlegać będą tylko usługi łączności świadczone przez prywatne sieci, które są umyślnie *udostępniane* społeczeństwu. Takie sformułowanie pomoże ponadto podkreślić, że fakt *udostępniania* sieci prywatnej *ogółowi społeczeństwa* jest kluczowym czynnikiem przy określaniu, czy sieć ta będzie objęta dyrektywą (obok czynnika, jakim jest świadczenie publicznie dostępnej usługi łączności). Innymi słowy, bez względu na to, czy sieć jest publiczna czy prywatna, jeśli jest umyślnie udostępniana społeczeństwu i świadczy publiczną usługę łączności, taką jak dostęp do Internetu, to nawet jeśli taka usługa jest dodatkiem do innej usługi (np. zakwaterowania w hotelu), taki typ usługi/sieci podlegałby dyrektywie o e-prywatności.

68. EIOD pragnie zauważyć, że poparte przez niego, przedstawione powyżej podejście, w myśl którego przepisy dyrektywy o e-prywatności są stosowane do *publicznie dostępnych sieci prywatnych*, jest spójne z podejściem przyjętym w wielu państwach członkowskich, w których organy już uznały, że takie typy usług, jak i usługi świadczone w sieciach o czysto prywatnym charakterze wchodzą w zakres zastosowania przepisów krajowych służących wykonaniu dyrektywy o e-prywatności ([18]).

69. Aby zapewnić jeszcze większą pewność prawa co do podmiotów objętych nowym zakresem zastosowania, użyteczne może być włączenie do dyrektywy o e-prywatności poprawki z definicją „publicznie dostępnych sieci prywatnych", która mogłaby brzmieć: „*publicznie dostępna sieć prywatna oznacza sieć obsługiwaną przez podmiot prywatny, do której nieograniczony dostęp ma zwykle ogół społeczeństwa – odpłatnie lub nie albo w związku z innymi usługami lub ofertami – pod warunkiem zaakceptowania stosownych warunków użytkowania*".

70. W praktyce powyższe podejście oznaczałoby, że dyrektywie podlegałyby sieci prywatne w hotelach i innych placówkach, które zapewniają dostęp do Internetu ogółowi społeczeństwa poprzez sieć prywatną. Z drugiej strony świadczenie usług łączności przez sieci o czysto prywatnym charakterze, z których to usług korzysta ograniczona liczba określonych osób, nie będzie objęte dyrektywą. A zatem dyrektywą nie byłyby objęte np. wirtualne sieci prywatne i domy konsumentów wyposażone w bezprzewodowe sieci Wi-Fi. Nie byłyby nią objęte również usługi świadczone za pośrednictwem sieci będących faktycznie sieciami wewnętrznymi.

Sieci prywatne objęte zakresem zastosowania dyrektywy o e-prywatności

71. Wyłączenie sieci prywatnych jako takich, jak zasugerowano powyżej, należy uważać jako środek tymczasowy, który trzeba będzie jeszcze omówić. Zważywszy bowiem z jednej strony, że wyłączenie sieci o czysto prywatnym charakterze jako takich może mieć skutki dla prywatności, a z drugiej – że wyłączenie to dotyczy sporej liczby osób, które zwykle uzyskują dostęp do Internetu za pośrednictwem sieci wewnętrznych, być może w przyszłości trzeba będzie ponownie zastanowić się nad tą kwestią. Z tego względu i by wesprzeć debatę na ten temat, EIOD zaleca dodanie do dyrektywy o e-prywatności motywu, zgodnie z którym Komisja przeprowadzi konsultacji publiczne dotyczące stosowania dyrektywy o e-prywatności do wszystkich sieci prywatnych i weźmie również pod uwagę komentarze EIOD-a, organów ochrony danych i innych stosownych zainteresowanych stron. W motywie tym można ponadto wyjaśnić, że zgodnie z wynikiem tych konsultacji publicznych Komisja powinna przedstawić stosowny wniosek w sprawie rozszerzenia lub ograniczenia zakresu typów podmiotów, które powinny podlegać dyrektywie o e-prywatności.

72. Oprócz powyższego działania należy odpowiednio zmienić różne artykuły dyrektywy o e-prywatności, tak by wszystkie przepisy operacyjne w wyraźny sposób odnosiły się nie tylko do sieci publicznych, lecz również publicznie dostępnych sieci prywatnych.

IV. PRZETWARZANIE DANYCH O RUCHU DO CELÓW BEZPIECZEŃSTWA

73. W trakcie procedury legislacyjnej związanej z przeglądem dyrektywy o e-prywatności, firmy świadczące usługi bezpieczeństwa postulowały, by do dyrektywy o e-prywatności włączyć przepis dający prawne podstawy gromadzenia danych o ruchu do celów zagwarantowania rzeczywistego bezpieczeństwa sieci.

([17]) Zwykle bezprzewodowe sieci lokalne (ang. *Local Area Network (LAN)*).

([18]) Zob. przypis 16.

74. W związku z tym PE dodał poprawkę 181, wprowadzającą nowy art. 6 ust. 6a; w artykule tym jednoznacznie zezwala się na przetwarzanie danych o ruchu do celów bezpieczeństwa: „*Bez uszczerbku dla zgodności z postanowieniami innymi niż postanowienia art. 7 dyrektywy 95/46/WE i art. 5 tej dyrektywy, dane o ruchu można przetwarzać w uzasadnionym interesie kontrolera danych w celu wdrożenia technicznych środków zapewniających bezpieczeństwo sieci i informacji – zgodnie z definicją zawartą w art. 4 lit. (c) rozporządzenia (WE) 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiającego Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji – publicznej usługi łączności elektronicznej, publicznej lub prywatnej sieci łączności elektronicznej, usługi społeczeństwa informacyjnego lub związanego z nimi urządzenia końcowego łączności elektronicznej, chyba że ważniejsze okazują się prawa podstawowe i wolności podmiotów, których dane te dotyczą. Przetwarzanie takie musi się ograniczać do zakresu ściśle niezbędnego do celów tego rodzaju działania mającego zapewniać bezpieczeństwo*".

75. Komisja w swoim zmienionym wniosku zaakceptowała tę poprawkę co do zasady, jednak usunęła z jej tekstu kluczowy fragment, który miał zagwarantować, że przestrzegane będą inne przepisy dyrektywy (początkowy fragment od „*Bez uszczerbku*" do „*tej dyrektywy*"). Rada przyjęła przeredagowaną wersję, w której jeszcze osłabiono ważne zabezpieczenia i równowagę interesów wprowadzone poprawką 181 i nadano tekstowi brzmienie: „*Dane o ruchu mogą być przetwarzane wyłącznie w zakresie niezbędnym do zapewnienia bezpieczeństwa sieci i informacji określonego w art. 4 lit. c) rozporządzenia (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiającego Europejską Agencję Bezpieczeństwa Sieci i Informacji*".

76. Jak wyjaśniono poniżej, art. 6 ust. 6a jest niepotrzebny i podatny na ryzyko nadużywania, zwłaszcza jeśli zostanie przyjęty w formie, która nie zawiera ważnych gwarancji, fragmentów dotyczących przestrzegania innych przepisów dyrektywy czy zachowania równowagi interesów. EIOD zaleca zatem usunięcie tego artykułu lub przynajmniej dopilnowanie, by każdy ewentualny artykuł dotyczący tego zagadnienia zawierał tego rodzaju gwarancje, jakie zawarte były w poprawce 181 przyjętej przez PE.

Podstawy prawne przetwarzania danych o ruchu mające zastosowanie do usług łączności elektronicznej i inni administratorzy danych w ramach obecnych przepisów o ochronie danych

77. Zakres, w jakim dostawcy publicznie dostępnych usług łączności elektronicznej mogą zgodnie z prawem przetwarzać dane o ruchu, jest regulowany art. 6 dyrektywy o e-prywatności, który zezwala na przetwarzanie danych o ruchu tylko do pewnych określonych celów, takich jak naliczenie opłat, rozliczenia międzyoperatorskie i marketing. Przetwarzanie takie można prowadzić, o ile spełnione zostaną wyszczególnione warunki, np. w przypadku marketingu – uzyskana zostanie zgoda danych osób. Inni administratorzy danych, tacy jak dostawcy usług społeczeństwa informacyjnego, mogą ponadto przetwarzać dane o ruchu na mocy art. 7 dyrektywy o ochronie danych, zgodnie z którym administratorzy danych mogą przetwarzać dane osobowe, jeśli czynność ta jest prowadzona zgodnie z co najmniej jedną z wymienionych w artykule podstaw prawnych.

78. Przykładem takiej podstawy prawnej jest art. 7 lit. a) dyrektywy o ochronie danych wprowadzający wymóg uzyskania zgody osoby, której dane dotyczą. Na przykład, jeśli sklep internetowy chce przetwarzać dane o ruchu do celów sprzedaży ogłoszeń reklamowych lub materiałów marketingowych, musi uzyskać zgodę danej osoby. Zgodnie z inną podstawą prawną przedstawioną w art. 7 w pewnych okolicznościach możliwe jest przetwarzanie danych o ruchu do celów bezpieczeństwa, np. przez firmy oferujące usługi bezpieczeństwa. Wynika to z art. 7 lit. f), który stanowi, że administratorzy danych mogą przetwarzać dane osobowe, jeśli jest to „*konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą …*". Dyrektywa o ochronie danych nie podaje przykładów sytuacji, w jakich przetwarzanie danych osobowych byłoby zgodne z tym wymogiem. Zamiast tego decyzję podejmują administratorzy danych – indywidualnie dla każdego przypadku – często za zgodą krajowych organów ochrony danych i innych organów.

79. Należy wziąć pod uwagę wzajemną zależność między art. 7 dyrektywy o ochronie danych a proponowanym art. 6 ust. 6a dyrektywy o e-prywatności. Proponowany art. 6 ust. 6a precyzuje, w jakich okolicznościach spełnione zostałyby wymogi art. 7 lit. f) opisane powyżej. Zezwalając bowiem na przetwarzanie danych o ruchu w celu zapewnienia bezpieczeństwa sieci i informacji, art. 6 ust. 6a umożliwia takie przetwarzanie do celów uzasadnionych interesów administratora danych.

80. Jak wyjaśniono poniżej, EIOD uważa, że proponowany art. 6 ust. 6a nie jest potrzebny ani użyteczny. Z punktu widzenia prawa bowiem zasadniczo nie ma potrzeby ustalania, czy szczególny typ czynności przetwarzania danych, w tym przypadku przetwarzanie danych o ruchu do celów bezpieczeństwa, spełnia wymogi art. 7 lit. f) dyrektywy o ochronie danych, w którym to przypadku może być konieczne uzyskanie zgody danej osoby na podstawie art. 7 lit. a). Jak zauważono powyżej, ocenę taką przeprowadzają zwykle na poziomie wykonawczym administratorzy danych, tj. firmy, w porozumieniu z organami ochrony danych, a w razie potrzeby – sądy. Ogólnie rzecz biorąc, EIOD uważa, że w pewnych przypadkach zgodne z prawem przetwarzanie danych o ruchu do celów bezpieczeństwa, prowadzone bez naruszania podstawowych praw i wolności osób, prawdopodobnie

spełnia wymogi art. 7 lit. f) dyrektywy o ochronie danych, a zatem może być prowadzone. Ponadto ani dyrektywa o ochronie danych, ani dyrektywa o e-prywatności nie zawierają precedensu polegającego na wybieraniu lub szczególnym traktowaniu pewnego typu czynności przetwarzania danych, który odpowiadałoby wymogom art. 7 lit. f), i nie istnieją dowody, że taki wyjątek jest konieczny. Natomiast, jak zauważono powyżej, wydaje się, że w wielu okolicznościach tego typu czynność można by swobodnie pogodzić z obecnym tekstem. Dlatego też przepis prawny potwierdzający konieczność tej oceny jest w zasadzie niepotrzebny.

Art. 6 ust. 6a w wersji PE, Rady i Komisji

81. Jak wyjaśniono powyżej, należy podkreślić, że poprawka 181 przyjęta przez PE, choć niepotrzebna, została jednak zredagowana, do pewnego stopnia uwzględniając zasady ochrony prywatności i ochrony danych zawarte w przepisach dotyczących ochrony danych. W swej poprawce 181 PE mógłby ponadto zająć się potrzebą ochrony danych i prywatności, na przykład, dodając wyrazy „w określonych przypadkach", by zadbać o wybiórcze stosowanie tego artykułu, lub określając konkretny okres przechowywania danych.

82. Poprawka 181 zawiera pewne elementy, które należy ocenić pozytywnie. Potwierdza, że przetwarzanie powinno być zgodne z wszelkimi zasadami ochrony danych, które mają zastosowanie do przetwarzania danych osobowych („*Bez uszczerbku dla zgodności z postanowieniami […] dyrektywy 95/46/WE i […] tej dyrektywy*"). Ponadto, choć w myśl poprawki 181 dozwolone jest przetwarzanie danych o ruchu do celów bezpieczeństwa, zachowano w niej równowagę między interesami podmiotu przetwarzającego dane o ruchu a interesami osób, których dane są przetwarzane, tak że takie przetwarzanie danych może być prowadzone, tylko jeśli interesy podmiotu przetwarzającego dane nie są ważniejsze niż interesy podstawowych praw i wolności danych osób („*chyba że ważniejsze okazują się prawa podstawowe i wolności podmiotów, których dane te dotyczą*"). Wymóg ten jest kluczowy, ponieważ dzięki niemu możliwe staje się przetwarzanie danych o ruchu w poszczególnych przypadkach; nie umożliwia on jednak danemu podmiotowi masowego przetwarzania danych o ruchu.

83. Przeredagowana przez Radę wersja poprawki zawiera elementy godne pochwały, takie jak zachowane wyrażenie „*ściśle niezbędny*", które podkreśla ograniczony zakres zastosowania tego artykułu. W wersji Rady zabrakło jednak gwarancji ochrony danych i prywatności, o których mowa powyżej. Choć w zasadzie obowiązują ogólne przepisy dotyczące ochrony danych, bez względu na to, czy są wyraźnie przywoływane w każdym przypadku, art. 6 ust. 6a w wersji zredagowanej przez Radę można jednak interpretować jako dający pełne uprawnienia uznaniowe do przetwarzania danych o ruchu, bez konieczności zapewnienia jakichkolwiek gwarancji ochrony danych i prywatności, które obowiązują za każdym razem, gdy przetwarzane są dane o ruchu. Można by zatem utrzymywać, że dane o ruchu wolno zbierać, przechowywać, a następnie użytkować bez konieczności przestrzegania zasad ochrony danych ani wypełniania konkretnych obowiązków, które tak czy inaczej mają zastosowanie do podmiotów odpowiedzialnych, takich jak zasada jakości czy obowiązek uczciwego i zgodnego z prawem przetwarzania czy dbania o poufność i bezpieczeństwo danych. Poza tym, skoro w samym artykule brak odniesienia do stosownych zasad ochrony danych, które ograniczają czas, przez jaki wolno informacje gromadzić, lub do określonych ram czasowych, wersję zaproponowaną przez Radę można interpretować jako zezwalającą na zbieranie i przetwarzanie danych o ruchu do celów bezpieczeństwa przez czas nieokreślony.

84. Rada osłabiła ponadto gwarancje prywatności w niektórych fragmentach tekstu, używając ogólniejszych sformułowań. Usunięto na przykład odniesienie do „*uzasadnionego interesu kontrolera danych*", co wzbudza wątpliwość co do typów podmiotów, którym wolno byłoby skorzystać z tego wyłączenia. Sprawą niesłychanej wagi jest uniknięcie utorowania jakiemukolwiek użytkownikowi czy podmiotowi prawnemu drogi do niewłaściwego wykorzystania tej poprawki.

85. Ostatnie doświadczenia w ramach PE i Rady pokazują, że trudno jest określić w przepisach prawa zakres i warunki, po spełnieniu których wolno zgodnie z prawem przetwarzać dane do celów bezpieczeństwa. Jest mało prawdopodobne, by jakikolwiek obowiązujący czy przyjęty w przyszłości przepis zapobiegł oczywistym zagrożeniom wynikającym z nadmiernie szerokiego stosowania tego wyłączenia z przyczyn innych niż ściśle związane z bezpieczeństwem lub stosowania przez podmioty, które nie powinny mieć możliwości korzystania z tego wyłączenia. Nie oznacza to, że takie przetwarzanie nie jest dozwolone w żadnych okolicznościach. Jednak bardziej poprawną ocenę tego, czy dozwolone jest przetwarzanie i w jakim zakresie, można przeprowadzić na poziomie wykonawczym. Podmioty, które chciałyby zająć się takim przetwarzaniem, powinny omówić zakres i warunki z organami ochrony danych i ewentualnie z Grupą Roboczą Art. 29. Istnieje też inna możliwość: dyrektywa o e-prywatności mogłaby zawierać artykuł, który zezwala na przetwarzanie danych o ruchu do celów bezpieczeństwa, o ile uzyskana zostanie jednoznaczna zgoda organów ochrony danych.

86. Biorąc pod uwagę z jednej strony zagrożenia, jakie art. 6 ust. 6a stwarza dla podstawowego prawa do ochrony danych i prywatności osób, a z drugiej strony fakt, że – jak wyjaśniono w niniejszej opinii – z punktu widzenia prawa artykuł ten jest niepotrzebny, EIOD doszedł do wniosku, że najlepszym wyjściem byłoby skreślenie proponowanego art. 6 ust. 6a w całości.

87. Jeśli – wbrew zaleceniu EIOD-a – przyjęty zostanie jakikolwiek tekst w rodzaju art. 6 ust. 6a w jego obecnej wersji, powinien on przynajmniej zawierać gwarancje ochrony danych omówione powyżej. Powinien on również zostać odpowiednio zespolony z obecną strukturą art. 6, najlepiej jako nowy ustęp 2a.

V. **UMOŻLIWIE OSOBOM PRAWNYM PODEJMOWANIA DZIAŁAŃ W PRZYPADKU NARUSZEŃ DYREKTYWY O E-PRYWATNOŚCI**

88. PE uchwalił poprawkę 133, która umożliwia dostawcom dostępu do Internetu i innym podmiotom prawnym, takim jak stowarzyszenia konsumenckie, występowanie na drogę sądową w przypadku naruszenia któregokolwiek z przepisów dyrektywy o e-prywatności ([19]). Niestety, ani Komisja ani Rada nie zaakceptowały tej poprawki. EIOD bardzo pozytywnie ocenia tę poprawkę i zaleca jej zachowanie.

89. Aby zrozumieć znaczenie tej poprawki, trzeba zdać sobie sprawę, że w dziedzinie ochrony prywatności i danych szkoda wyrządzona danej osobie rozpatrywana jako pojedynczy przypadek zwykle sama w sobie nie jest wystarczająca, by wszcząć kroki prawne przed sądem. Pojedyncze osoby zwykle same nie występują na drogę sądową, tylko dlatego, że stały się adresatami niezamówionych komunikatów lub że ich imię i nazwisko zostało błędnie zamieszczone w książce telefonicznej. Poprawka ta pozwoliłaby stowarzyszeniom konsumenckim i związkom zawodowym zbiorowo reprezentującym interesy konsumentów występować na drogę sądową w ich imieniu. Większe zróżnicowanie mechanizmów egzekwowania prawdopodobnie będzie sprzyjać także lepszemu przestrzeganiu przepisów dyrektywy o e-prywatności, a co za tym idzie – chęci skutecznego ich stosowania.

90. W prawnych ramach niektórych państw członkowskich istnieją prawne precedensy, które przewidują możliwość zbiorowego zadośćuczynienia, dzięki czemu konsumenci lub grupy interesów mogą występować o odszkodowanie od strony, która spowodowała szkodę.

91. Ponadto ustawy o konkurencji ([20]) obowiązujące w niektórych państwach członkowskich upoważniają konsumentów i grupy interesów (obok poszkodowanego w wyniku nieuczciwej konkurencji) do wytaczania sprawy podmiotowi, który popełnił naruszenie. Uzasadnieniem takiego podejścia jest fakt, że firmy popełniające naruszenia ustawy o konkurencji prawdopodobnie odniosą korzyści, ponieważ konsumenci, którzy ponieśli tylko bardzo niewielkie szkody, zazwyczaj niechętnie wytaczają sprawę. To samo uzasadnienie można – ze stosownymi zmianami – zastosować w dziedzinie ochrony danych i prywatności.

92. Co więcej, jak wspomniano powyżej, upoważnienie podmiotów prawnych, takich jak stowarzyszenia konsumenckie i dostawcy PPECS, do występowania na drogę sądową poprawia sytuację konsumentów i sprzyja ogólnemu lepszemu przestrzeganiu przepisów o ochronie danych. Jeśli firmy popełniające naruszenia będą bardziej narażone na pozwanie do sądu, prawdopodobnie włożą więcej wysiłku w przestrzeganie przepisów dotyczących ochrony danych, co w dłuższej perspektywie przyczyni się do zwiększenia poziomu ochrony prywatności i konsumentów. Z wszystkich tych powodów EIOD apeluje do PE i do Rady, by przyjęły przepis umożliwiający podmiotom prawnym występowanie na drogę sądową w przypadku naruszenia któregokolwiek z przepisów dyrektywy o e-prywatności.

([19]) Art. 13 ust. 6 tekstu będącego wynikiem pierwszego czytania w PE.

([20]) Zob. np. paragraf 8 UWG – niemieckiej ustawy o nieuczciwej konkurencji.

VI. **PODSUMOWANIE**

93. Tekst wspólnego stanowiska Rady, tekst będący wynikiem pierwszego czytania w PE oraz zmieniony wniosek Komisji zawierają, w różnym stopniu, elementy zasługujące na pozytywną ocenę, które przyczyniłyby się do wzmocnienia ochrony prywatności i danych osobowych osób.

94. EIOD sądzi jednak, że teksty te można jeszcze udoskonalić, zwłaszcza jeśli chodzi o wspólne stanowisko Rady, w którym niestety nie uwzględniono pewnych poprawek PE służących dopilnowaniu odpowiedniej ochrony prywatności i danych osobowych osób. EIOD nalega, by PE i Rada przywróciły gwarancje prywatności, które były zawarte w tekście będącym wynikiem pierwszego czytania w PE.

95. Ponadto EIOD uważa, że należy udoskonalić pewne przepisy dyrektywy. Odnosi się to w szczególności do przepisów dotyczących naruszenia bezpieczeństwa, ponieważ EIOD uważa, że pełne korzyści z powiadomień o naruszeniu będzie można wyciągnąć, gdy ramy prawne zostaną prawidłowo określone od samego początku. Na koniec – EIOD jest zdania, że należy poprawić i doprecyzować brzmienie pewnych przepisów dyrektywy.

96. W świetle powyższego, EIOD zwraca się do PE i Rady, by zwiększyły starania na rzecz poprawienia i doprecyzowania pewnych przepisów dyrektywy o e-prywatności, a jednocześnie przywróciły w tekście poprawki przyjęte przez PE w pierwszym czytaniu, które miały na celu zapewnienie właściwego poziomu ochrony prywatności i danych. W tym celu w poniższych punktach 97, 98, 99 i 100 zawarto podsumowanie omawianych kwestii i przedstawiono pewne zalecenia i propozycje redakcyjne. EIOD apeluje do wszystkich zainteresowanych stron, by uwzględniły te zalecenia i propozycje, zanim dyrektywa o e-prywatności zostanie ostatecznie przyjęta.

Naruszenie bezpieczeństwa

97. Parlament Europejski, Komisja i Rada przyjęły różne podejścia do kwestii powiadamiania o przypadkach naruszenia bezpieczeństwa. Różnice między trzema modelami są widoczne m.in., jeśli chodzi o podmioty objęte obowiązkiem powiadamiania, kryterium, którego spełnienie pociąga za sobą konieczność powiadomienia, osoby, których dane dotyczą, upoważnione do otrzymania powiadomienia itd. PE i Rada muszą dołożyć wszelkich starań, by opracować solidne ramy prawne dotyczące naruszeń bezpieczeństwa. W tym celu PE i Rada powinny:

— *Zachować* definicję naruszenia bezpieczeństwa w tekstach PE, Rady i Komisji, ponieważ jest ona na tyle ogólna, by dotyczyć większości stosownych sytuacji, w których uzasadnione może być powiadomienie o naruszeniu bezpieczeństwa.

— Do zakresu podmiotów, które mają być objęte proponowanym wymogiem powiadamiania, należy *włączyć* dostawców usług społeczeństwa informacyjnego. Istnieje takie samo jeśli nie większe prawdopodobieństwo, że celem działań skutkujących naruszeniem bezpieczeństwa staną się – tak jak firmy telekomunikacyjne – sklepy, banki i apteki internetowe. Obywatele mają prawo oczekiwać, że zostaną powiadomieni nie tylko, gdy ofiarą naruszenia bezpieczeństwa padną dostawcy dostępu do Internetu, lecz w szczególności gdy stanie się tak w przypadku internetowych banków i aptek, z których ci obywatele korzystają.

— Jeśli chodzi o kryterium, którego spełnienie pociąga za sobą konieczność powiadomienia, to zaproponowane w zmienionym wniosku istnienie „*uzasadnionego prawdopodobieństwa wystąpienia szkody*" jest kryterium właściwym, które zapewnia mechanizmowi funkcjonalność. Należy jednak dopilnować, by pojęcie „szkody" było wystarczające szerokie, by objąć wszystkie stosowne przypadki negatywnych skutków dla prywatności lub innych uzasadnionych interesów danych osób. W przeciwnym wypadku korzystniej byłoby stworzyć nowe kryterium, zgodnie z którym powiadomienie byłoby obowiązkowe, *„jeśli istnieje uzasadnione prawdopodobieństwo, że naruszenie będzie miało niekorzystne skutki dla danych osób*". Podejście zaproponowane przez Radę, zgodnie z którym naruszenie wiązałoby się z *poważnym* naruszeniem czyjejś prywatności, nie zapewniałoby właściwej ochrony danych osób, ponieważ zawiera ono wymóg, by skutek dla prywatności miał poważny charakter. Daje również pole do subiektywnej oceny.

— Choć włączenie organu w podejmowanie decyzji co do tego, czy dany podmiot musi powiadomić dane osoby, z pewnością ma pozytywne skutki, może okazać się rozwiązaniem niepraktycznym i trudnym w stosowaniu i pochłonąć zasoby przeznaczone na inne ważne priorytety. EIOD obawia się, że jeśli organy nie będą reagować wyjątkowo szybko, to taki system może nawet doprowadzić do osłabienia ochrony osób i wywierać na organy nadmierną presję. A zatem, ogólnie rzecz biorąc, EIOD doradza, by *wprowadzić* system, w ramach którego to dane podmioty oceniają, czy muszą dokonać powiadomienia.

— Aby umożliwić organom sprawowanie nadzoru nad ocenami, które organy objęte obowiązkiem powiadomienia przeprowadzają w celu podjęcia decyzji w tej sprawie, należy *wdrożyć* następujące zabezpieczenia:

  — *Dopilnować*, by takie podmioty miały obowiązek powiadamiania organów o wszelkich naruszeniach, które spełniają wymagane kryterium.

  — *Przydzielić* organom rolę nadzorczą, która umożliwi im działania wybiórcze, a przez to skuteczność. Aby osiągnąć ten cel, należy dodać fragment w brzmieniu: *„Jeśli dany abonent lub dana osoba nie zostali jeszcze powiadomieni, to po zbadaniu charakteru naruszenia właściwy organ krajowy może wystąpić do dostawcy PPECS lub ISSP o dokonanie powiadomienia*".

  — *Przyjąć* nowy przepis, wprowadzający wymóg zachowywania przez podmioty szczegółowych i kompleksowych chronologicznie posegregowanych informacji odnoszących się do kontroli wewnętrznej. Cel ten można osiągnąć, dodając fragment w brzmieniu: *„Dostawcy PPECS i dostawcy ISSP prowadzą i zachowują kompleksowe rejestry zawierające szczegółowe informacje na temat wszelkich zaistniałych przypadków naruszenia bezpieczeństwa, stosowne informacje techniczne z tym związane oraz informacje na temat podjętych działań naprawczych. Rejestry te zawierają również informacje o wszelkich powiadomieniach przesłanych abonentom lub danym osobom oraz właściwym organom krajowym, w tym datę przesłania powiadomienia i jego treść. Akta te są przedstawiane na wniosek właściwego organu krajowego*".

— Aby zapewnić spójność w realizacji ram dotyczących naruszeń bezpieczeństwa, należy wyposażyć Komisję w możliwość przyjmowania technicznych środków wykonawczych, po uprzedniej konsultacji z EIOD-em, Grupą Roboczą Art. 29 i innymi właściwymi zainteresowanymi stronami.

— Jeśli chodzi o osoby, które należy powiadomić, *należy stosować* terminy zaproponowane przez Komisję lub PE, tj. „dane osoby" lub „użytkownicy, których dotyczyło naruszenie", ponieważ obejmują one wszystkie osoby, których dane osobowe zostały narażone.

Publicznie dostępne sieci prywatne

98. Usługi łączności są często udostępniane społeczeństwu nie za pomocą sieci publicznych, a sieci obsługiwanych przez podmioty prywatne (np. punkty dostępu do Wi-Fi znajdujące się w hotelach, portach lotniczych), które raczej nie podlegają dyrektywie. PE przyjął poprawkę 121 (art. 3) rozszerzającą zakres zastosowania dyrektywy, tak by podlegały jej publiczne i prywatne sieci łączności, a także publicznie dostępne sieci prywatne. W odniesieniu do powyższego PE i Rada powinny:

— *Zachować* istotę poprawki 121, ale *zmienić jej brzmienie* i uwzględnić w zakresie zastosowania dyrektywy o e-prywatności wyłącznie *„przetwarzanie danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności lub w publicznie dostępnych prywatnych sieciach łączności we Wspólnocie*". Nie byłoby zapisu jednoznacznie stanowiącego, że w zakres zastosowania wchodzą również sieci o charakterze czysto prywatnym (w odróżnieniu od publicznie dostępnych sieci prywatnych).

— Odpowiednio *zmienić* wszystkie przepisy operacyjne, tak by jednoznacznie odnosiły się zarówno do sieci publicznych, jak i publicznie dostępnych sieci prywatnych.

— *Dodać* poprawkę zawierającą definicję: *„publicznie dostępna sieć prywatna oznacza sieć obsługiwaną przez podmiot prywatny, do której nieograniczony dostęp ma zwykle ogół społeczeństwa odpłatnie lub nie albo w związku z innymi usługami lub ofertami pod warunkiem zaakceptowania stosownych warunków użytkowania"*. Zwiększy się dzięki niej pewność prawa co do tego, jakie podmioty są objęte nowym zakresem zastosowania dyrektywy.

— *Przyjąć* nowy motyw, w myśl którego Komisja przeprowadziłaby konsultacje publiczne na temat stosowania dyrektywy o e-prywatności do wszystkich sieci prywatnych i wzięła również pod uwagę komentarze EIOD-a, Grupy Roboczej Art. 29 i innych stosownych zainteresowanych stron. Wyjaśnić, że zgodnie z wynikiem tych konsultacji publicznych Komisja powinna przedstawić stosowny wniosek w sprawie rozszerzenia lub ograniczenia zakresu typów podmiotów, które powinny podlegać dyrektywie o e-prywatności.

Przetwarzanie danych o ruchu do celów bezpieczeństwa

99. PE przyjął w pierwszym czytaniu poprawkę 181 (art. 6 ust. 6a), w której zezwala się na przetwarzanie danych o ruchu do celów bezpieczeństwa. W tekście wspólnego stanowiska Rady zawarto nową wersję, w której osłabiono niektóre zabezpieczenia prywatności. Z tego względu EIOD zaleca, by PE i Rada:

— *Odrzuciły* ten artykuł w całości, ponieważ jest niepotrzebny, a jego nadużywanie mogłoby stanowić nadmierne zagrożenia dla ochrony danych i prywatności osób.

— Istnieje też inna możliwość: gdyby miał zostać przyjęty jakiś wariant art. 6 ust. 6a w jego obecnej wersji, PE i Rada powinny *zawrzeć* w nim gwarancje ochrony danych omówione w niniejszej opinii (zbliżone do gwarancji zaproponowanych w poprawce PE).

Działania w przypadku naruszeń dyrektywy o e-prywatności

100. Parlament przyjął poprawkę 133 (art. 13 ust. 6), która daje podmiotom prawnym możliwość występowania na drogę sądową w przypadku stwierdzenia naruszenia którekolwiek z przepisów dyrektywy. Niestety, Rada nie zachowała poprawki w swoim tekście. Rada i PE powinny:

— *Przyjąć* przepis dający podmiotom prawnym, takim jak stowarzyszenia konsumenckie lub zawodowe, możliwość występowania na drogę sądową w przypadku stwierdzenia naruszenia któregokolwiek z przepisów dyrektywy – a nie tylko naruszenia przepisów dotyczących niezamówionych komunikatów, jak tego chcą w swoim obecnym brzmieniu wspólne stanowisko i zmieniony wniosek. Większa różnorodność mechanizmów egzekwowania zachęci do lepszego przestrzegania wszystkich przepisów dyrektywy o e-prywatności i ich skutecznego stosowania.

Sprostanie wyzwaniu

101. W odniesieniu do wszystkich powyższych kwestii PE i Rada muszą sprostać wyzwaniu, jakim jest opracowanie właściwych zasad i przepisów, które są wykonalne, funkcjonalne i zgodne z prawem do prywatności i ochrony danych osób. EIOD ma nadzieję, że zaangażowane strony dołożą wszelkich starań, by sprostać temu wyzwaniu, i że niniejsza opinia pomoże im w osiągnięciu tego celu.

Sporządzono w Brukseli, dnia 9 stycznia 2009 r.

Peter HUSTINX
Europejski Inspektor Ochrony Danych