I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie wspierania zaufania w społeczeństwie informacyjnym poprzez działanie na rzecz ochrony danych i prywatności

(2010/C 280/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16,

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 7 i 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 ([3]), w szczególności jego art. 41,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. **WPROWADZENIE**

1. Technologie informacyjno-komunikacyjne (TIK) dają ogromne możliwości w praktycznie każdym aspekcie naszego życia – pracy, rozrywce, życiu towarzyskim i edukacji. Są one niezbędne w dzisiejszej gospodarce informacyjnej i ogólnie w społeczeństwie.

2. Unia Europejska jest światową potęgą w zaawansowanych TIK i jest zdecydowana utrzymać taki stan rzeczy. Oczekuje się, że aby sprostać temu wyzwaniu, Komisja Europejska niedługo przyjmie nową europejską agendę cyfrową, której priorytetowe znaczenie potwierdziła komisarz Kroes ([4]).

3. EIOD uznaje korzyści wynikające ze stosowania TIK i zgadza się, że UE powinna dołożyć wszelkich starań, aby promować rozwój tych technologii i ich powszechne przyjmowanie. EIOD w pełni popiera także poglądy komisarzy Kroes i Reding, zgodnie z którymi podstawą tego nowego środowiska powinny być osoby fizyczne ([5]). Osoby fizyczne powinny mieć możliwość polegania na zdolności TIK do zapewnienia bezpieczeństwa informacji i kontrolowania ich wykorzystania, a także powinny mieć pewność, że ich prawa do prywatności i ochrony danych będą respektowane w przestrzeni cyfrowej. Poszanowanie tych praw jest niezbędne do zwiększania zaufania konsumentów. Zaufanie to jest z kolei istotne, aby obywatele korzystali z nowych usług ([6]).

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 201 z 31.7.2002, s. 37.
([3]) Dz.U. L 8 z 12.1.2001, s. 1.

([4]) Odpowiedzi na kwestionariusz Parlamentu Europejskiego dla komisarz Neelie Kroes w kontekście przesłuchania w Parlamencie Europejskim, które poprzedzało mianowanie komisarza.
([5]) Odpowiedzi na kwestionariusz Parlamentu Europejskiego dla komisarz Neelie Kroes w kontekście przesłuchania w Parlamencie Europejskim, które poprzedzało mianowanie komisarza; przemówienie komisarz Viviane Reding na temat europejskiej agendy cyfrowej dla nowych konsumentów cyfrowych, wygłoszone na wielostronnym forum Europejskiej Organizacji Konsumentów pt. „Prywatność konsumentów i marketing internetowy: tendencje rynkowe i perspektywy w zakresie polityki" (Consumer Privacy and Online Marketing: Market Trends and Policy Perspectives), Bruksela, dnia 12 listopada 2009 r.
([6]) Zob. np. sprawozdanie RISEPTIS pt. „Trust in the Information Society", Sprawozdanie Rady Doradczej RISEPTIS (badania i innowacje na rzecz bezpieczeństwa, prywatności i wiarygodności w społeczeństwie informacyjnym). Dostępne pod adresem http://www.think-trust.eu/general/news-events/riseptis-report.html Zob. także: J. B Horrigan, „Broadband Adoption and Use in America", Inicjatywa Szerokopasmowa Omnibus (Omnibus Broadband Initiative) Federalnej Komisji Łączności (Federal Communications Commission), OBI Working Paper Series No 1.

4. UE ma silne ramy prawne w zakresie ochrony danych i prywatności, których zasady pozostają całkowicie uzasadnione w erze cyfrowej. Nie można jednak popadać w samozadowolenie. W wielu przypadkach TIK dają podstawy do nowych obaw, które nie są uwzględnione w istniejących ramach. Konieczne są zatem pewne działania, aby dopilnować, że poszczególne prawa przewidziane w prawodawstwie UE w dalszym ciągu zapewniają skuteczną ochronę w tym nowym środowisku.

5. W niniejszej opinii omówiono środki, które Unia Europejska może promować lub podejmować w celu zagwarantowania ochrony prywatności osób fizycznych i danych w zglobalizowanym świecie, którego siłą napędową nadal będą technologie. Przedstawiono tu instrumenty ustawodawcze i o charakterze nieustawodawczym.

6. Po przedstawieniu w ogólnym zarysie TIK jako nowych osiągnięć, które dają możliwości, ale i stwarzają zagrożenie, w opinii omówiono potrzebę zintegrowania – na poziomie praktycznym – ochrony danych i prywatności od samego powstania nowych technologii informacyjno-komunikacyjnych (co jest nazywane zasadą poszanowania prywatności od samego początku). Aby zapewnić zgodność z tą zasadą, w opinii omówiono potrzebę uwzględnienia – na co najmniej dwa różne sposoby – zasady poszanowania prywatności od samego początku w ramach prawnych dotyczących ochrony danych. Po pierwsze, poprzez włączenie jej jako ogólnej obowiązującej zasady, a po drugie – poprzez włączenie jej w konkretne obszary TIK stanowiące określone zagrożenia dla ochrony danych/prywatności, które to zagrożenia można zmniejszyć dzięki odpowiedniej architekturze technicznej i projektowi. Obszary te to identyfikacja radiowa (ang. radio frequency identification, RFID), aplikacje portali społecznościowych i aplikacje przeglądarek. Ponadto w opinii zawarto zalecenia dotyczące innych narzędzi i zasad mających na celu ochronę prywatności osób fizycznych i danych w sektorze TIK.

7. W odniesieniu do powyższych kwestii w niniejszej opinii omówiono niektóre uwagi grupy roboczej art. 29 poczynione w ramach wkładu do konsultacji publicznych na temat przyszłości prywatności ([1]). Niniejsza opinia jest ponadto oparta na wcześniejszych opiniach EIOD, takich jak: opinia z dnia 25 lipca 2007 r. w sprawie dyrektywy o ochronie danych, opinia z dnia 20 grudnia 2007 r. w sprawie RFID i dwie opinie w sprawie dyrektywy o prywatności i łączności elektronicznej ([2]).

II. TIK DAJĄ NOWE MOŻLIWOŚCI, ALE STANOWIĄ TAKŻE NOWE ZAGROŻENIA

8. TIK są porównywane z innymi ważnymi wynalazkami z przeszłości, takimi jak elektryczność. Chociaż może być zbyt wcześnie na ocenę ich rzeczywistego wpływu historycznego, związek pomiędzy TIK a rozwojem gospodarczym w krajach rozwiniętych jest wyraźny. TIK tworzą miejsca pracy, dają korzyści gospodarcze i przyczyniają się do wzrostu ogólnego dobrobytu. Wpływ TIK wykracza poza kwestie czysto gospodarcze, ponieważ technologie te odgrywają ważną rolę w stymulowaniu innowacyjności i kreatywności.

9. Ponadto TIK zmieniły sposób, w jaki ludzie pracują, prowadzą życie towarzyskie i nawiązują wzajemne kontakty. Na przykład ludzie w coraz większym stopniu polegają na TIK w relacjach społecznych i gospodarczych. Osoby fizyczne mogą korzystać z szeregu nowych zastosowań TIK, np. w dziedzinie e-zdrowia, e-transportu i e-administracji, a także z innowacyjnych interaktywnych systemów w zakresie rozrywki i nauki.

10. W świetle tych korzyści wszystkie instytucje Unii Europejskiej wyraziły zobowiązanie do wspierania TIK jako narzędzia niezbędnego do zwiększenia konkurencyjności przemysłu europejskiego i przyspieszenia tempa naprawy gospodarczej w Europie. W sierpniu 2009 r. Komisja przyjęła sprawozdanie w sprawie konkurencyjności Europy w dziedzinie technologii cyfrowych ([3]) i rozpoczęła konsultacje społeczne na temat odpowiednich przyszłych strategii promujących TIK. W dniu 7 grudnia 2009 r. Rada przyjęła konkluzje stanowiące wkład do tych konsultacji pt. „Po strategii i2010 – ku otwartemu, zielonemu i konkurencyjnemu społeczeństwu wiedzy" ([4]). Niedawno Parlament Europejski przyjął

([1]) Opinia grupy roboczej art. 29 WP 168 „Przyszłość prywatności. Wspólny wkład w konsultacje Komisji Europejskiej w sprawie ram prawnych dotyczących podstawowego prawa do ochrony danych osobowych" (The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data), przyjęta w dniu 1 grudnia 2009 r.

([2]) Opinia EIOD 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, s. 1; opinia EIOD 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), Dz.U. C 101 z 23.4.2008, s. 1; opinia EIOD z dnia 10 kwietnia 2008 r. 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), Dz.U. C 181 z 18.7.2008, s. 1; druga opinia EIOD z dnia 9 stycznia 2009 r. w sprawie przeglądu dyrektywy 2002/58/WE dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej).

([3]) Sprawozdanie w sprawie konkurencyjności Europy w dziedzinie technologii cyfrowych – Najważniejsze osiągnięcia strategii i2010 w latach 2005–2009, (SEC(2009) 1060).

([4]) Konkluzje Rady „Po strategii i2010 – ku otwartemu, zielonemu i konkurencyjnemu społeczeństwu wiedzy" (17107/09), przyjęte w dniu 18.12.2009 r.

sprawozdanie mające na celu dostarczenie Komisji wskazówek w zakresie określenia agendy cyfrowej [1].

11. Wraz z możliwościami i korzyściami towarzyszącymi rozwojowi TIK pojawiają się nowe zagrożenia, szczególnie dla prywatności i ochrony danych osobowych dotyczących osób fizycznych. TIK na ogół prowadzą do szybkiego wzrostu (dość często w sposób niewidoczny dla osób fizycznych) liczby informacji gromadzonych, przechowywanych, filtrowanych, przekazywanych lub w inny sposób zatrzymywanych, i dlatego mnożą się zagrożenia dla tych danych.

12. Na przykład procesory RFID zastępują kody kreskowe na (niektórych) produktach konsumenckich. Poprzez poprawę przepływu informacji w łańcuchu dostaw (a zatem zmniejszenie potrzeby utrzymywania bezpiecznego poziomu zapasów, zapewniania dokładniejszych prognoz itp.) nowy system ma przynosić korzyści zarówno przedsiębiorstwom, jak i konsumentom. Jednakże jednocześnie zwiększa się niepokojąca możliwość bycia śledzonym, dla różnych celów i przez różne podmioty, za pośrednictwem dóbr osobistych opatrzonych etykietami.

13. Innym przykładem jest tzw. „przetwarzanie w chmurze" (ang. cloud computing), które polega na świadczeniu za pośrednictwem Internetu usług konsumenckich i niekonsumenckich dostarczanych przez organizacje zewnętrzne. Zakres tych usług jest bardzo szeroki – od bibliotek fotografii, kalendarzy, poczty elektronicznej i baz danych konsumentów po bardziej złożone usługi okołobiznesowe. Korzyści zarówno dla przedsiębiorstw, jak i osób fizycznych są oczywiste – obniżenie kosztów (koszty są przyrostowe), mniejsze uzależnienie od lokalizacji (łatwy dostęp do informacji w dowolnym miejscu świata), automatyzacja (brak konieczności posiadania dedykowanych zasobów informatycznych i aktualizowania oprogramowania) itp. Jednocześnie istnieje bardzo realne zagrożenie zakłóceniami bezpieczeństwa i hakerstwem. Istnieje także obawa o utratę dostępu do własnych danych i kontroli nad nimi.

14. Wykazano, że korzyści i zagrożenia współistnieją w innych obszarach wykorzystujących TIK. Przykładem jest dziedzina e-zdrowia, która może zwiększać efektywność, obniżać koszty, zwiększać dostępność i ogólnie poprawiać jakość usług opieki zdrowotnej. Jednakże z e-zdrowiem często wiąże się kwestia legalności wtórnego wykorzystywania informacji dotyczących e-zdrowia, wymagająca dokładnej analizy celów każdego potencjalnego wtórnego wykorzystania [2]. Ponadto wraz z powszechniejszym stosowaniem elektronicznych kart zdrowia systemy takich kart stają się przedmiotem skandalów ujawniających wiele przypadków nieupoważnionego dostępu.

15. Podsumowując, prawdopodobnie pozostanie pewien poziom szczątkowego ryzyka nawet po dokonaniu odpowiednich ocen i zastosowaniu koniecznych środków. Całkowity brak zagrożenia byłby nierealny. Jednakże, jak omówiono poniżej, można i trzeba wdrożyć środki ograniczające takie zagrożenia do stosownego poziomu.

III. POSZANOWANIE PRYWATNOŚCI OD SAMEGO POCZĄTKU JAKO NAJWAŻNIEJSZE NARZĘDZIE ZWIĘKSZANIA INDYWIDUALNEGO POZIOMU ZAUFANIA DO TIK

16. Z potencjalnych korzyści wynikających z TIK można w praktyce korzystać tylko wtedy, gdy technologie te są w stanie zwiększać poziom zaufania – innymi słowy, gdy ze względu na swoje właściwości i korzyści mogą zapewnić gotowość użytkowników do polegania na TIK. Zaufanie będzie rosło jedynie wtedy, gdy TIK będą niezawodne, bezpieczne, pozostające pod kontrolą osób fizycznych i gdy gwarantowana będzie ochrona danych osobowych i prywatności użytkowników.

17. Powszechne zagrożenia i niepowodzenia, takie jak przedstawione poniżej, mogą szkodzić zaufaniu użytkownika do społeczeństwa informacyjnego, szczególnie gdy wiążą się z wykorzystaniem danych osobowych niezgodnie z przeznaczeniem lub ich naruszeniem ze szkodą dla prywatności osób fizycznych. Może to poważnie zagrażać rozwojowi TIK i korzyściom, które mogą przynosić.

18. Jednakże rozwiązanie problemu tych zagrożeń dla prywatności i ochrony danych nie może polegać na wyeliminowaniu, wykluczeniu ani odmowie wykorzystywania lub promowania TIK. Byłoby to niewykonalne i nierealne; uniemożliwiłoby osobom fizycznym korzystanie z pożytków płynących z TIK i poważnie ograniczyłoby ogólne korzyści, jakie można uzyskać dzięki tym technologiom.

19. EIOD uważa, że bardziej pozytywnym rozwiązaniem jest projektowanie i rozwijanie TIK z poszanowaniem prywatności i ochrony danych. Jest zatem niezwykle istotne, aby uwzględnić prywatność i ochronę danych w całym cyklu życia technologii, od najwcześniejszego etapu projektowania po jej ostateczne wprowadzenie, użytkowanie i ostateczne usunięcie. Rozwiązanie to jest zwykle nazywane „poszanowaniem prywatności od samego początku". Poniżej omówiono je bardziej szczegółowo.

20. Poszanowanie prywatności od samego początku może wiązać się z różnymi działaniami w zależności od konkretnego przypadku lub zastosowania. W niektórych przypadkach może ono np. wymagać wyeliminowania/ograniczenia danych osobowych bądź zapobiegania zbędnemu lub niepożądanemu przetwarzaniu. W innych przypadkach może ono wiązać się z oferowaniem narzędzi zwiększających kontrolę użytkowników nad ich własnymi danymi osobowymi. Takie środki należy rozważać przy określaniu norm lub najlepszych praktyk. Mogą one także

[1] Sprawozdanie w sprawie określenia nowej agendy cyfrowej dla Europy – od i2010 do digital.eu (2009/2225 (INI)), przyjęte w dniu 18.3.2010 r.

[2] Na przykład sprzedaż lub wykorzystywanie informacji na temat stanu zdrowia gromadzonych na potrzeby prowadzenia leczenia nie mogą mieć na celu wybierania lokalizacji dla przychodni satelickich, tworzenia ośrodków leczenia ambulatoryjnego oraz innych rodzajów planowania przyszłych działań o skutkach finansowych, które wymagałyby dokładnego zbadania.

być wprowadzone w architekturze systemów informacyjno-komunikacyjnych lub w strukturalnej organizacji podmiotów przetwarzających dane osobowe.

III.1. **Zasada poszanowania prywatności od samego początku stosowana w różnych środowiskach TIK i ich wpływ**

21. Potrzeba zasady poszanowania prywatności od samego początku występuje w wielu różnych środowiskach TIK. Na przykład sektor opieki zdrowotnej jest w coraz większym stopniu uzależniony od infrastruktury TIK, która często wiąże się ze scentralizowanym przechowywaniem informacji dotyczących stanu zdrowia pacjentów. Zastosowanie zasady poszanowania prywatności od samego początku w sektorze opieki zdrowotnej wymagałoby oceny stosowności różnych środków, takich jak: możliwość ograniczenia do minimum ilości danych przechowywanych centralnie lub ograniczenia ich do indeksu, stosowanie narzędzi szyfrujących, przyznawanie prawa dostępu na zasadzie ograniczonego dostępu, anonimizacja danych, gdy nie są już potrzebne itp.

22. Podobnie systemy transportowe są coraz częściej oferowane domyślnie z zaawansowanymi zastosowaniami TIK, które komunikują się z pojazdem i jego otoczeniem dla różnych celów i na potrzeby różnych funkcji. Na przykład samochody są coraz częściej wyposażane w nowe funkcje TIK (GPS, GSM, sieć czujników itd.), które rejestrują nie tylko ich lokalizację, ale także warunki techniczne w czasie rzeczywistym. Informacje te można wykorzystać na przykład w celu zastąpienia istniejącego systemu podatku drogowego opłatami drogowymi zależnymi od użytkowania. Zastosowanie zasady poszanowania prywatności od samego początku w projekcie architektury tych systemów powinno wspierać przetwarzanie i dalsze przekazywanie jak najmniejszej ilości danych osobowych ([1]). Zgodnie z tą zasadą zdecentralizowana lub połowicznie zdecentralizowana architektura ograniczająca ujawnianie danych dotyczących lokalizacji do punktu centralnego byłaby bardziej pożądana niż architektura scentralizowana.

23. Powyższe przykłady pokazują, że tworzenie technologii informacyjno-komunikacyjnych zgodnie z zasadą poszanowania prywatności od samego początku może znacznie ograniczyć zagrożenia dla prywatności i ochrony danych.

III.2. **Niewystarczające wprowadzenie TIK stosujących zasadę poszanowania prywatności od samego początku**

24. Ważną kwestią jest to, czy podmioty gospodarcze, producenci/dostawcy TIK i administratorzy danych są zainteresowani marketingiem i wdrażaniem zasady poszanowania prywatności od samego początku w TIK. W tym kontekście ważne jest również ocenienie zapotrzebowania użytkowników na tę zasadę.

25. W 2007 r. Komisja wydała komunikat wzywający przedsiębiorstwa do wykorzystywania swojej siły innowacji do tworzenia i wdrażania technologii na rzecz ochrony prywatności w celu poprawienia ochrony prywatności i danych osobowych od samego początku cyklu rozwoju ([2]).

26. Dostępne dowody wykazują jednak, że dotychczas ani producenci TIK, ani administratorzy danych (zarówno w sektorze prywatnym, jak i publicznym) nie byli w stanie spójnie wdrożyć zasady poszanowania prywatności od samego początku ani wprowadzić tej zasady na rynek. Wskazuje się różne przyczyny takiej sytuacji, w tym brak zachęt gospodarczych lub wsparcia instytucjonalnego, niewystarczające zapotrzebowanie itp. ([3]).

27. Jednocześnie zapotrzebowanie użytkowników na poszanowanie prywatności od samego początku jest dość małe. Użytkownicy produktów i usług TIK mogą słusznie zakładać, że ich prywatność i dane osobowe są faktycznie chronione, chociaż w wielu przypadkach tak nie jest. W niektórych przypadkach zwykle nie są oni w stanie przyjąć środków bezpieczeństwa niezbędnych do ochrony własnych danych osobowych lub danych innych osób. Sytuacja ta często wynika z braku pełnej czy nawet częściowej wiedzy użytkowników na temat tych zagrożeń. Na przykład, ogólnie rzecz biorąc, młodzież lekceważy zagrożenia dla prywatności związane z udostępnianiem danych osobowych na portalach społecznościowych i często ignoruje ustawienia dotyczące prywatności. Inni użytkownicy zdają sobie sprawę z zagrożeń, ale mogą nie mieć wiedzy technicznej koniecznej do wdrożenia technologii ochronnych, np. zabezpieczających połączenie z Internetem, lub do zmiany ustawień wyszukiwarki w celu zminimalizowania możliwości tworzenia profilu w oparciu o monitorowanie czynności związanych z surfowaniem po Internecie.

28. Zagrożenia dla ochrony prywatności i danych są jednak bardzo realne. Jeżeli prywatność i ochrona danych nie są uwzględniane od samego początku, często jest za późno na naprawę systemów i jest ona zbyt droga; za późno też jest na naprawienie już spowodowanych szkód. Rosnąca liczba przypadków naruszenia danych osobowych

([1]) Zob. opinia Europejskiego Inspektora Ochrony Danych z dnia 22 lipca 2009 r. w sprawie komunikatu Komisji dotyczącego planu działania na rzecz wdrażania inteligentnych systemów transportowych w Europie i towarzyszącego mu wniosku w sprawie dyrektywy Parlamentu Europejskiego i Rady ustanawiającej ramy wdrażania inteligentnych systemów transportowych w dziedzinie transportu drogowego oraz ich interfejsów z innymi rodzajami transportu, dostępna pod adresem: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_PL.pdf

([2]) Komunikat Komisji dla Parlamentu Europejskiego i Rady w sprawie lepszej ochrony danych z wykorzystaniem technologii na rzecz ochrony prywatności, 2.5.2007 r., (COM(2007) 228 wersja ostateczna).

([3]) Badanie dotyczące korzyści gospodarczych wynikających z technologii na rzecz ochrony prywatności (privacy enhancing technology — PETs), jls/2008/D4/036.

w ostatnich latach doskonale odzwierciedla ten problem i zwiększa potrzebę poszanowania prywatności od samego początku.

29. Powyższe stwierdzenia wyraźnie wskazują na to, że producenci i dostawcy TIK mających na celu przetwarzanie danych osobowych powinni być odpowiedzialni – wraz z administratorami danych – za projektowanie ich z uwzględnieniem ochrony danych i zabezpieczeń prywatności. W wielu przypadkach oznaczałoby to, że technologie te powinny być projektowane z domyślnymi ustawieniami prywatności.

30. W tym kontekście trzeba rozważyć, jakie kroki powinny podjąć osoby odpowiedzialne za wyznaczanie kierunków polityki w tej dziedzinie, aby wspierać poszanowanie prywatności od samego początku w rozwoju TIK. Pierwsze pytanie dotyczy tego, czy istniejące ramy prawne w dziedzinie ochrony danych zawierają odpowiednie przepisy mające na celu zapewnienie wdrożenia zasady poszanowania prywatności od samego początku przez zarówno administratorów danych, jak i producentów/twórców. Drugie pytanie odnosi się do tego, co należy zrobić w kontekście europejskiej agendy cyfrowej, aby zagwarantować, że sektor TIK zwiększy zaufanie konsumentów.

IV. **WPROWADZENIE ZASADY POSZANOWANIA PRYWATNOŚCI OD SAMEGO POCZĄTKU DO PRAWA I POLITYKI UE**

IV.1. **Obecne ramy prawne dotyczące ochrony danych i prywatności**

31. UE posiada szeroko zakrojone ramy dotyczące ochrony danych i prywatności, które zapisane są w dyrektywie 95/46/WE ([1]), dyrektywie 2002/59/WE ([2]) oraz w praktyce sądowej Europejskiego Trybunału Praw Człowieka ([3]) i Trybunału Sprawiedliwości.

32. Dyrektywa o ochronie danych stosuje się do „każdej operacji lub zestawu operacji dokonywanych na danych osobowych" (gromadzenia, przechowywania, ujawniania itd.). Nakłada na podmioty, które przetwarzają dane osobowe („administratorów danych") wymóg zgodności z określonymi zasadami oraz obowiązki. Określono w niej prawa osób fizycznych, takie jak prawo dostępu do danych osobowych. Dyrektywa o prywatności i łączności elektronicznej dotyczy w szczególności ochrony prywatności w sektorze łączności elektronicznej ([4]).

33. Obecna dyrektywa o ochronie danych nie zawiera jednoznacznego wymogu poszanowania prywatności od samego początku. Obejmuje jednak przepisy, które pośrednio, w różnych sytuacjach, mogą wymagać wprowadzenia zasady poszanowania prywatności od samego początku. W szczególności art. 17 wymaga od administratorów danych wprowadzenia odpowiednich środków technicznych i organizacyjnych w celu zapobiegania nielegalnemu przetwarzaniu danych ([5]). Poszanowanie prywatności od samego początku jest zatem ujęte w bardzo ogólny sposób. Ponadto przepisy dyrektywy dotyczą głównie administratorów danych oraz przetwarzania przez nich danych osobowych. Przepisy te nie zawierają wyraźnego wymogu, aby technologie informacyjno-komunikacyjne były zgodne z zasadami ochrony danych i prywatności, co wymaga również uwzględnienia w przepisach projektantów i wytwórców TIK, w tym działań prowadzonych na etapie normalizacji.

34. Dyrektywa o prywatności i łączności elektronicznej jest bardziej jednoznaczna. Jej art. 14 ust. 3 stanowi, że „w miarę potrzeb, możliwe jest przyjęcie środków w celu zapewnienia, że terminal jest skonstruowany w sposób zgodny z prawem użytkowników do ochrony i kontroli używania ich danych osobowych, zgodnie z dyrektywą 1999/5/WE i decyzją Rady 87/95/EWG z dnia 22 grudnia 1986 r. w sprawie normalizacji w dziedzinie technologii informatycznych i telekomunikacji". Przepis ten jednak nie został nigdy wykorzystany ([6]).

35. Podczas gdy powyższe przepisy obu dyrektyw są pomocne w *promowaniu* poszanowania prywatności od samego początku, w praktyce nie są wystarczające do *zapewnienia* uwzględnienia prywatności w TIK.

36. W wyniku powyższej sytuacji w prawodawstwie nie wymaga się w wystarczająco precyzyjny sposób projektowania TIK zgodnie z zasadą poszanowania prywatności od samego początku. Również organy ochrony danych nie posiadają wystarczających kompetencji do zapewnienia wprowadzenia zasady poszanowania prywatności od samego początku. Powoduje to nieskuteczność. Na przykład organy ochrony danych mogą mieć uprawnienia do nakładania sankcji za brak odpowiedzi na wnioski osób fizycznych o udzielenie dostępu do danych i będą posiadały kompetencje do żądania wdrożenia określonych środków w celu zapobieżenia nielegalnemu przetwarzaniu

([1]) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady (zwana dalej „dyrektywą o ochronie danych").

([2]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady (zwana dalej „dyrektywą o prywatności i łączności elektronicznej").

([3]) Zawierającej wykładnię głównych pojęć i warunków zawartych w art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (EKPC), przyjętej w Rzymie w dniu 4 listopada 1950 r., z zastosowaniem ich do różnych dziedzin.

([4]) Traktat lizboński zwiększył tę ochronę poprzez uznanie poszanowania życia prywatnego i ochrony danych osobowych za odrębne prawa podstawowe w art. 7 i 8 Karta praw podstawowych Unii Europejskiej. Karta praw podstawowych Unii Europejskiej stała się obowiązująca z chwilą wejścia w życie traktatu lizbońskiego.

([5]) Artykuł 17 brzmi następująco: „Państwa członkowskie zapewniają, aby administrator danych wprowadził odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem, szczególnie wówczas gdy przetwarzanie danych obejmuje transmisję danych w sieci, jak również przed wszelkimi innymi nielegalnymi formami przetwarzania". Motyw 46 uzupełnia go stwierdzeniem: „Ochrona praw i wolności osób, których dotyczą przetwarzane dane osobowe wymaga przyjęcia odpowiednich rozwiązań technicznych i organizacyjnych, zarówno przy opracowywaniu systemu przetwarzania danych, jak i podczas samego ich przetwarzania, szczególnie w celu utrzymania bezpieczeństwa i niedopuszczenia do niedozwolonego przetwarzania danych".

([6]) Komisja ogłosiła, że planuje zaktualizować dyrektywę 1999/5/WE pod koniec 2010 r.

danych. Jednak nie zawsze jest w wystarczającym stopniu jasne, czy ich kompetencje rozciągają się także na żądanie zaprojektowania systemu w sposób ułatwiający osobom fizycznym korzystanie z ich praw do ochrony danych ([1]). Na przykład na podstawie istniejących przepisów prawnych nie jest oczywiste, czy można wymagać, aby architektura systemu informacyjnego była zaprojektowana w sposób, który ułatwi przedsiębiorstwom reagowanie na wnioski o udzielenie dostępu do danych wystosowane przez osoby fizyczne, tak aby takie wnioski były przetwarzane automatycznie i szybciej. Ponadto późniejsze próby zmiany technologii już po jej opracowaniu lub wprowadzeniu mogą skutkować niespójnymi rozwiązaniami, które nie będą w pełni działały, a poza tym będą uciążliwe gospodarczo.

37. Z punktu widzenia EIOD, który to punkty widzenia podziela także grupa robocza art. 29 ([2]), obecne ramy prawne pozostawiają możliwość wyraźniejszego zatwierdzenia zasady poszanowania prywatności od samego początku.

IV.2. **Wprowadzenie poszanowania prywatności od samego początku na różnych poziomach**

38. W świetle powyższego EIOD zaleca Komisji cztery następujące kierunki działania:

a) zaproponowanie włączenia ogólnego przepisu o poszanowaniu prywatności od samego początku do ram prawnych dotyczących ochrony danych;

b) rozwinięcie tego ogólnego przepisu w przepisach szczegółowych, gdy w różnych sektorach zaproponowane zostaną szczegółowe instrumenty prawne. Te przepisy szczegółowe już mogłyby zostać włączone do instrumentów prawnych; na podstawie art. 17 dyrektywy o ochronie danych (oraz innych istniejących przepisów);

c) uwzględnienie poszanowania prywatności od samego początku jako naczelnej zasady europejskiej agendy cyfrowej;

d) wprowadzenie poszanowania prywatności od samego początku jako zasady w innych inicjatywach UE (głównie o charakterze nieustawodawczym).

Ogólny przepis o poszanowaniu prywatności od samego początku

39. EIOD proponuje jednoznacznie i wyraźnie włączyć zasadę poszanowania prywatności od samego początku do istniejących ram regulacyjnych w zakresie ochrony danych. Mogłoby to wzmocnić i sprecyzować poszanowanie prywatności od samego początku, a także przyczynić się do jej efektywnego wprowadzenia, dodatkowo dając więcej uprawnień organom egzekucyjnym w zakresie wymagania jej faktycznego stosowania w praktyce. Jest to szczególnie konieczne w świetle faktów przedstawionych powyżej, nie tylko ze względu na znaczenie samej zasady jako narzędzia promującego zaufanie, ale również jako zachęty dla zainteresowanych stron do wprowadzenia poszanowania prywatności od samego początku i rozszerzenia gwarancji przewidzianych w istniejących ramach prawnych.

40. Wniosek ten opiera się na zaleceniu grupy roboczej art. 29 dotyczącym wprowadzenia zasady „poszanowania prywatności od samego początku" jako ogólnej zasady w zakresie ram prawnych dotyczących ochrony danych, w szczególności dyrektywy o ochronie danych. Według grupy roboczej art. 29: „Zasada ta powinna być wiążąca dla projektantów i producentów technologii, jak również dla administratorów danych, którzy muszą podejmować decyzje odnośnie do nabywania i wykorzystywania TIK. Powinni być zobowiązani do uwzględnienia technicznej ochrony danych już na etapie planowania informacyjno-technologicznych procedur i systemów. Dostawcy takich systemów lub usług, a także administratorzy powinni wykazać, że podjęli wszelkie środki konieczne do spełnienia tych wymogów".

41. EIOD z zadowoleniem przyjmuje także poparcie komisarz Viviane Reding dla zasady poszanowania prywatności od samego początku, wyrażone w kontekście zapowiedzi przeglądu dyrektywy o ochronie danych ([3]).

42. Kolejną kwestią jest treść takiego uregulowania. Przede wszystkim ogólna zasada poszanowania prywatności od samego początku powinna być neutralna technologicznie. Celem tej zasady nie powinno być regulowanie technologii, tj. nie powinna zalecać określonych rozwiązań technicznych. Powinna natomiast przewidywać wprowadzenie istniejących zasad prywatności i ochrony danych do systemów i rozwiązań informacyjno-komunikacyjnych. Umożliwi to zainteresowanym stronom, producentom, administratorom danych oraz organom ochrony danych

([1]) Zob. sprawozdanie biura brytyjskiego komisarza ds. informacji pt. „Poszanowanie prywatności od samego początku" (Privacy by Design), opublikowane w listopadzie 2008 r.

([2]) Zob. opinia grupy roboczej art. 29 WP 168 „Przyszłość prywatności. Wspólny wkład w konsultacje Komisji Europejskiej w sprawie ram prawnych dotyczących podstawowego prawa do ochrony danych osobowych" (The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data), przyjęta w dniu 1 grudnia 2009 r.

([3]) „Poszanowanie prywatności od samego początku to zasada leżąca w interesie zarówno obywateli, jak i przedsiębiorstw. Poszanowanie prywatności od samego początku doprowadzi do lepszej ochrony osób fizycznych, a także do zwiększenia zaufania do nowych usług i produktów, co z kolei będzie miało pozytywny wpływ na gospodarkę. Istnieją pewne zachęcające przykłady, lecz bardzo wiele pozostaje do zrobienia". Przemówienie programowe w Dniu Ochrony Danych, dnia 28 stycznia 2010 r., Parlament Europejski, Bruksela.

interpretowanie zasady w każdym poszczególnym przypadku. Po drugie, zgodność z tą zasadą powinna być obowiązkowa na różnych etapach, od tworzenia norm i projektowania architektury, po ich wdrażanie przez administratora danych.

Przepisy w konkretnych instrumentach prawnych

43. Obecne i przyszłe instrumenty ustawodawcze muszą zawierać zasadę poszanowania prywatności od samego początku w oparciu o istniejące ramy prawne oraz – po przyjęciu ogólnego przepisu zaproponowanego powyżej – w oparciu o ten ostatni. Na przykład zgodnie z aktualnymi inicjatywami związanymi z inteligentnymi systemami transportu Komisja będzie ponosiła w pierwszym etapie szczególną odpowiedzialność za zdefiniowanie środków, inicjatyw standaryzacyjnych, procedur i najlepszych praktyk. W trakcie wykonywania tych zadań poszanowanie prywatności od samego początku powinno być zasadą naczelną.

44. EIOD zwraca także uwagę, że zasada poszanowania prywatności od samego początku jest również szczególnie ważna w obszarze wolności, bezpieczeństwa i sprawiedliwości, zwłaszcza w odniesieniu do celów strategii zarządzania informacjami przewidzianej w programie sztokholmskim ([1]). W swojej opinii w sprawie programu sztokholmskiego EIOD podkreślił, że architektura wymiany informacji powinna być oparta na „poszanowaniu prywatności od samego początku" ([2]): „Oznacza to konkretnie, że systemy informatyczne służące zapewnieniu bezpieczeństwa publicznego powinny być zawsze tworzone zgodnie z zasadą poszanowania prywatności od samego początku".

45. W swojej opinii dotyczącej przyszłości prywatności ([3]) grupa robocza art. 29 jeszcze bardziej stanowczo nalega, aby w obszarze wolności, bezpieczeństwa i sprawiedliwości – gdzie organy publiczne odgrywają główną rolę i gdzie środki nadzoru bezpośrednio wpływają na podstawowe prawa do poszanowania prywatności i ochrony danych – wymogi poszanowania prywatności od samego początku były obowiązkowe. Poprzez wprowadzenie tych wymogów do systemów informacyjnych rządy mogłyby wspierać poszanowanie prywatności od samego początku w ramach swoich zdolności jako „klientów pilotażowych".

Poszanowanie prywatności od samego początku jako naczelna zasada europejskiej agendy cyfrowej

46. Technologie informacyjno-komunikacyjne są coraz bardziej złożone i wiążą się z większymi zagrożeniami dla prywatności i ochrony danych. Na ogół informacje w formie cyfrowej, które łatwiej jest uzyskać, powielić i przesłać, narażone są na znacznie większe zagrożenie niż informacje w formie papierowej. Wraz z rozwojem sieci połączonych obiektów zagrożenia te będą się nasilać. Im większe będzie zagrożenie dla prywatności/ochrony danych, tym większe będzie zapotrzebowanie na silniejsze środki ochrony danych/prywatności. Z tego względu argument za koniecznością wprowadzenia w sektorze TIK zasady poszanowania prywatności od samego początku jest nie do odparcia. Ponadto, jak stwierdzono powyżej, zaufanie osób fizycznych do TIK ma zasadnicze znaczenie, jeśli mają one korzystać z tych nowych usług, a prywatność i ochrona danych są niezbędnymi elementami tego zaufania.

47. Powyżej podkreślono, że w ramach strategii rozwoju TIK trzeba potwierdzić potrzebę projektowania tych technologii z nieodłącznym elementem prywatności i ochrony danych, tj. z uwzględnieniem zasady poszanowania prywatności od samego początku.

48. W europejskiej agendzie cyfrowej należy zatem jednoznacznie poprzeć zasadę poszanowania prywatności od samego początku jako element niezbędny do zapewnienia zaufania obywateli do TIK i usług online. W agendzie tej należy stwierdzić, że prywatność i zaufanie idą w parze i że poszanowanie prywatności od samego początku powinno być nadrzędnym czynnikiem w rozwijaniu wiarygodnego sektora TIK.

Poszanowanie prywatności od samego początku jako zasada w innych inicjatywach UE

49. Poszanowanie prywatności od samego początku powinno być dla Komisji zasadą naczelną we wdrażaniu polityki, działań i inicjatyw w określonych sektorach TIK, w tym w dziedzinie e-zdrowia, e-zamówień, e-zabezpieczenia społecznego, e-nauczania itp. Wiele z tych inicjatyw będzie punktami działania w ramach europejskiej agendy cyfrowej.

50. Oznacza to na przykład, że inicjatywy mające na celu zapewnienie większej skuteczności i nowoczesności usług administracyjnych, tak aby osoby fizyczne mogły kontaktować się z administracją, powinny uwzględniać potrzebę zaprojektowania i działania tych usług zgodnie z zasadą poszanowania prywatności od samego początku. Dotyczy to również polityki i działań Komisji na rzecz szybszego Internetu, treści cyfrowych lub ogólnego promowania stałej, bezprzewodowej komunikacji i transmisji danych.

([1]) Program sztokholmski – Otwarta i bezpieczna Europa dla dobra i ochrony obywateli, zatwierdzony przez Radę Europejską w grudniu 2009 r.

([2]) Opinia Europejskiego Inspektora Ochrony Danych z dnia 10 lipca 2009 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady dotyczącego przestrzeni wolności, bezpieczeństwa i sprawiedliwości w służbie obywateli, Dz.U. C 276 z 17.11.2009, s. 8, pkt 60.

([3]) Opinia grupy roboczej art. 29 WP 168 „Przyszłość prywatności. Wspólny wkład w konsultacje Komisji Europejskiej w sprawie ram prawnych dotyczących podstawowego prawa do ochrony danych osobowych" (The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data), przyjęta w dniu 1 grudnia 2009 r.

51. Powyższe stwierdzenia odnoszą się także do obszarów, w których Komisja jest odpowiedzialna za zakrojone na szeroką skalę systemy informatyczne, takie jak SIS i VIS, a także do przypadków, w których odpowiedzialność Komisji ogranicza się do utworzenia i utrzymywania wspólnej infrastruktury takiego systemu, na przykład europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS).

52. Szczegółowy sposób rozwinięcia zasady poszanowania prywatności od samego początku będzie zależał od danego sektora i sytuacji. Na przykład gdy inicjatywom Komisji towarzyszą wnioski ustawodawcze dotyczące określonego sektora TIK, w wielu przypadkach stosowne będzie zawarcie w nich jednoznacznego odniesienia do pojęcia poszanowania prywatności od samego początku, które ma zastosowanie do projektu konkretnej aplikacji/systemu TIK. W przypadku opracowywania planów działania dla określonego obszaru powinny one systematycznie zapewniać stosowanie ram prawnych, a dokładniej gwarantować tworzenie danych TIK z uwzględnieniem poszanowania prywatności od samego początku.

53. Jeżeli chodzi o badania, to siódmy program ramowy i kolejne programy powinny być wykorzystywane w charakterze narzędzi wspierających projekty, które mają na celu analizowanie norm, TIK i architektury przyczyniających się do wzmocnienia prywatności, a zwłaszcza zasady poszanowania prywatności od samego początku. Ponadto poszanowanie prywatności od samego początku powinno również stanowić niezbędny element, który należy uwzględnić w szerzej zakrojonych projektach z dziedziny TIK mających na celu przetwarzanie danych osobowych osób fizycznych.

Obszary będące przedmiotem szczególnego zainteresowania

54. W niektórych przypadkach, ze względu na określone zagrożenia dla prywatności i ochrony danych osób fizycznych lub z powodu innych czynników (opór sektora przed oferowaniem produktów uwzględniających poszanowanie prywatności od samego początku, zapotrzebowanie konsumentów itp.), konieczne może być określenie – w instrumentach ustawodawczych lub nie – bardziej jednoznacznych i szczegółowych środków w zakresie poszanowania prywatności od samego początku, które muszą być zawarte w określonym rodzaju produktu/technologii TIK.

55. EIOD zidentyfikował różne obszary (RFID, portale społecznościowe i aplikacje przeglądarek), które jego zdaniem wymagają na tym etapie dokładnego rozważenia przez Komisję i podjęcia praktycznych działań interwencyjnych, o których mowa powyżej. Te trzy obszary omówiono bardziej szczegółowo poniżej.

V. **IDENTYFIKACJA RADIOWA – RFID**

56. Etykiety RFID mogą być zintegrowane z przedmiotami, zwierzętami i ludźmi. Mogą być wykorzystane do gromadzenia i przechowywania danych osobowych takich jak ewidencja medyczna, do śledzenia przemieszczania się ludzi lub do tworzenia profilu ich zachowań w różnych celach. Może się to odbywać bez wiedzy osoby fizycznej [1].

57. Efektywne gwarancje dotyczące ochrony danych, prywatności oraz wszystkich powiązanych wymiarów etycznych mają zasadnicze znaczenie dla zaufania publicznego do RFID oraz przyszłego Internetu przedmiotów. Jedynie wówczas technologia dostarczy wielu korzyści gospodarczych i społecznych.

V.1. **Luki w obowiązujących ramach prawnych dotyczących ochrony danych**

58. Dyrektywa o ochronie danych oraz dyrektywa o prywatności i łączności elektronicznej stosują się do gromadzenia danych przy pomocy zastosowań RFID [2]. Wymagają m.in. wprowadzenia odpowiednich środków ochrony prywatności na potrzeby zastosowań RFID [3].

59. Jednakże te ramy prawne nie uwzględniają w pełni wszystkich kwestii ochrony danych i prywatności wiążących się z tą technologią. Wynika to z faktu, że dyrektywy

[1] Skrót RFID oznacza identyfikację radiową (ang. *radio frequency identification*). Główne elementy technologii *lub* infrastruktury identyfikacji radiowej to *etykieta* (np. mikroprocesor), czytnik oraz aplikacja połączona z etykietami i czytnikami za pośrednictwem oprogramowania pośredniczącego i przetwarzająca wytworzone dane. Etykieta składa się z obwodu elektronicznego, w którym przechowywane są dane, oraz z anteny, dzięki której dane są przekazywane drogą radiową. Czytnik posiada antenę i demodulator, który przetwarza informacje analogowe otrzymywane z łącza radiowego na dane cyfrowe. Informacje te można następnie wysyłać za pośrednictwem sieci do baz danych i serwerów w celu przetworzenia przy pomocy komputera.

[2] W dyrektywie o prywatności i łączności elektronicznej odniesienie do RFID znajduje się w art. 3: „Niniejsza dyrektywa ma zastosowanie do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności we Wspólnocie włącznie z publicznymi sieciami łączności służącymi do zbierania danych i obsługi urządzeń identyfikacyjnych". Uzupełnia to motyw 56 dyrektywy 2009/136/WE: „Postęp technologiczny pozwala na rozwój nowych aplikacji opartych na urządzeniach do gromadzenia danych i identyfikacji, którymi mogłyby być urządzenia bezkontaktowe wykorzystujące częstotliwości radiowe. Na przykład urządzenia do identyfikacji radiowej (»RFID«) wykorzystują częstotliwości radiowe do odczytu danych z etykiet towarowych z unikatowym kodem, które to dane następnie mogą być przekazywane do istniejących sieci łączności. Zastosowanie tego rodzaju technologii na szeroką skalę może przynieść istotne korzyści gospodarcze i społeczne, a tym samym w znaczący sposób przyczynić się do urzeczywistnienia rynku wewnętrznego, jeżeli ich stosowanie zostanie zaakceptowane przez obywateli. Aby osiągnąć ten cel, należy zapewnić ochronę wszystkich podstawowych praw jednostek, w tym prawa do prywatności i ochrony danych. W przypadku gdy takie urządzenia są przyłączone do publicznie dostępnych sieci łączności elektronicznej lub korzystają z usług łączności elektronicznej jako podstawowej infrastruktury, zastosowanie mają odpowiednie przepisy dyrektywy 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej), wraz z przepisami dotyczącymi bezpieczeństwa, ruchu i danych dotyczących lokalizacji oraz przepisami dotyczącymi poufności".

[3] Na przykład art. 17 dyrektywy o ochronie danych nakłada obowiązek wprowadzenia odpowiednich środków technicznych i organizacyjnych w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub niedozwolonym ujawnieniem.

nie są wystarczająco szczegółowe pod względem rodzajów zabezpieczeń, jakie powinny być wdrożone w zastosowaniach RFID. Istniejące zasady muszą być uzupełnione dodatkowymi, przewidującymi konkretne zabezpieczenia, w szczególności zobowiązującymi do wprowadzenia rozwiązań technicznych (poszanowanie prywatności od samego początku) do technologii RFID. Dotyczy to etykiet przechowujących dane osobowe, które powinny posiadać polecenie zakończenia procesu (ang. *kill command*), oraz zastosowania kryptografii w etykietach przechowujących określone rodzaje danych osobowych.

V.2. **Samoregulacja jako pierwszy krok**

60. W marcu 2007 r. Komisja przyjęła komunikat ([1]), w którym uznano m.in. potrzebę opracowania szczegółowych wytycznych dotyczących praktycznego wdrażania RFID, a także zalety przyjęcia kryteriów projektowania w celu uniknięcia zagrożeń dla prywatności i bezpieczeństwa.

61. Aby osiągnąć te cele, w maju 2009 r. Komisja przyjęła zalecenie w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową ([2]). W zastosowaniach RFID w sprzedaży detalicznej wymagane jest dezaktywowanie etykiet w punkcie sprzedaży, chyba że osoba fizyczna wyrazi zgodę na aktywność etykiety. Zasada ta ma zastosowanie, chyba że ocena skutków w zakresie ochrony danych i prywatności wykaże, że etykiety prawdopodobnie nie stanowią zagrożenia dla prywatności lub ochrony danych osobowych, w którym to przypadku mogą pozostać aktywne po opuszczeniu punktu sprzedaży, jeżeli osoba fizyczna nie zrezygnuje z tej możliwości bez ponoszenia kosztów.

62. EIOD zgadza się z podejściem Komisji zakładającym wykorzystanie instrumentów samoregulacyjnych. Jednakże, jak opisano poniżej, nie można wykluczyć, że samoregulacja nie dostarczy oczekiwanych wyników; dlatego apeluje do Komisji, aby była gotowa do przyjęcia innych środków.

V.3. **Problematyczne obszary i możliwe dodatkowe środki na wypadek, gdyby zawiodła samoregulacja**

63. EIOD obawia się, że organizacje obsługujące zastosowania RFID w sektorze sprzedaży detalicznej mogą pominąć możliwość monitorowania etykiet RFID przez niepożądane osoby trzecie. Takie monitorowanie może ujawniać dane osobowe przechowywane na etykiecie (jeżeli jakiekolwiek istnieją), ale może również umożliwić osobom trzecim śledzenie lub rozpoznanie osoby w czasie po prostu poprzez wykorzystanie niepowtarzalnych identyfikatorów znajdujących się na jednej etykiecie lub większej liczbie etykiet noszonych przez osobę fizyczną w środowisku, które może nawet znajdować się poza granicą działania zastosowania RFID. EIOD obawia się także, że operatorzy zastosowań RFID mogą odczuwać pokusę nadmiernego korzystania z wyjątku i tym samym pozostawiać etykiety aktywne po opuszczeniu punktu sprzedaży.

64. Jeżeli taka sytuacja nastąpi, może być za późno na zmniejszenie zagrożeń dla ochrony danych i prywatności osób fizycznych, na które już mogły zostać narażone. Ponadto biorąc pod uwagę charakter samoregulacji, krajowe organy egzekwowania prawa mogą znajdować się w trudniejszej sytuacji, gdy wymagają od organizacji obsługujących zastosowania RFID przyjęcia określonych środków poszanowania prywatności od samego początku.

65. W świetle powyższego EIOD apeluje do Komisji, aby była gotowa do zaproponowania instrumentów ustawodawczych regulujących podstawowe kwestie wykorzystywania RFID w przypadku gdyby nie powiodło się skuteczne wdrożenie istniejących ram prawnych. Ocena Komisji nie powinna być zbytnio opóźniona; opóźnienie naraziłoby osoby fizyczne na zagrożenie i również wobec przemysłu przyniosłoby skutek odwrotny do zamierzonego, ponieważ niepewność prawna jest zbyt duża i rozwiązanie trwałych problemów będzie prawdopodobnie trudniejsze i bardziej kosztowne.

66. W ramach środków, które być może trzeba będzie zaproponować, EIOD zaleca zapewnienie zasady wyrażania zgody w punkcie sprzedaży, zgodnie z którą wszystkie etykiety RFID dołączone do produktów konsumenckich byłyby dezaktywowane domyślnie w punkcie sprzedaży. Określenie przez Komisję konkretnej technologii, która ma zostać wykorzystana, może nie być konieczne ani właściwe. Natomiast w prawie UE należy ustanowić obowiązek prawny uzyskania zgody co do aktywowania etykiet, pozostawiając operatorom możliwość decydowania, w jaki sposób mają spełnić ten wymóg.

V.4. **Dalsze kwestie do rozważenia: zarządzanie Internetem przedmiotów**

67. Informacje wytworzone przez etykiety RFID – na przykład informacje o produkcie – mogą być połączone w globalną sieć infrastruktury komunikacyjnej. Jest ona zwykle nazywana „Internetem przedmiotów". Kwestie dotyczące ochrony danych/prywatności powstają, ponieważ przedmioty świata rzeczywistego mogą być identyfikowane poprzez etykiety RFID, które oprócz informacji o produkcie mogą zawierać dane osobowe.

68. Istnieje wiele otwartych pytań co do tego, kto będzie zarządzał przechowywaniem informacji związanych z obiektami opatrzonymi etykietami. Jak będzie to zorganizowane? Kto będzie miał dostęp do tych informacji? W czerwcu 2009 r. Komisja przyjęła komunikat w sprawie Internetu przedmiotów ([3]), w którym jednoznacznie określono potencjalne problemy tego zjawiska związane z ochroną danych i prywatności.

([1]) Komunikat Komisji z dnia 15.3.2007 r. 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 wersja ostateczna).

([2]) Zalecenie Komisji z dnia 12.5.2009 r. w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową (C(2009) 3200 wersja ostateczna).

([3]) Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie Internetu przedmiotów – plan działań dla Europy, 18.6.2009 r., (COM(2009) 278 wersja ostateczna).

69. EIOD pragnie podkreślić niektóre z tych kwestii podniesionych przez Komisję, które – jego zdaniem – zasługują na bliższą uwagę w miarę rozwoju Internetu przedmiotów. Po pierwsze, potrzeba zdecentralizowanej architektury może ułatwiać wykonalność i odpowiedzialność w zakresie ram prawnych UE. Po drugie, w możliwie szerokim zakresie powinno być chronione prawo osób fizycznych do niepodlegania śledzeniu. Innymi słowy, przypadki, w których osoby fizyczne są śledzone przy pomocy etykiet RFID bez wyrażenia na to zgody, powinny być bardzo ograniczone. Taka zgoda powinna być jednoznaczna. Zazwyczaj nazywa się to „milczeniem czipów" i prawem do pozostawienia w spokoju. Ponadto przy projektowaniu Internetu przedmiotów zasada poszanowania prywatności od samego początku powinna być zasadą naczelną. Na przykład wymagałoby to projektowania konkretnych zastosowań RFID, które posiadają wbudowane mechanizmy przekazujące użytkownikom kontrolę, z domyślnymi ustawieniami prywatności.

70. EIOD oczekuje, że będzie proszony o opinię, gdy Komisja będzie wprowadzać działania przewidziane w komunikacie, szczególnie w odniesieniu do projektu komunikatu w sprawie poszanowania prywatności i zaufania we wszechobecnym społeczeństwie informacyjnym.

VI. **PORTALE SPOŁECZNOŚCIOWE I POTRZEBA DOMYŚLNYCH USTAWIEŃ PRYWATNOŚCI**

71. Portale społecznościowe są „hitem miesiąca". Wydaje się, że pod względem popularności przewyższają wiadomości e-mail. Łączą one ludzi z innymi osobami o podobnych zainteresowaniach lub aktywności. Ludzie mogą posiadać własne profile internetowe i wymieniać pliki multimedialne, takie jak: filmy wideo, zdjęcia, muzykę, a także profile kariery zawodowej.

72. Młodzież szybko przyjęła portale społecznościowe i tendencja ta utrzymuje się. W ciągu ostatnich kilku lat spadła średnia wieku użytkowników Internetu w Europie: 9–10-latkowie obecnie łączą się z Internetem kilka razy w tygodniu; 12–14-latkowie codziennie, często spędzają w sieci od jednej do trzech godzin.

VI.1. **Portale społecznościowe a obowiązujące ramy prawne dotyczące ochrony danych i prywatności**

73. Rozwój portali społecznościowych umożliwił użytkownikom przesyłanie do Internetu informacji o sobie i o osobach trzecich. Czyniąc to, zdaniem grupy roboczej art. 29 ([1]), użytkownicy Internetu działają jako administratorzy danych, zgodnie z art. 2 lit. d) dyrektywy o ochronie danych, w odniesieniu do danych, które przesyłają ([2]). Jednakże w większości przypadków takie przetwarzanie objęte jest wyjątkiem dotyczącym domowego charakteru przetwarzania danych wynikającym z art. 3 ust. 2 dyrektywy. Jednocześnie portale społecznościowe uznawane są za administratorów danych o tyle, o ile zapewniają środki do przetwarzania danych użytkownika i wszystkie podstawowe usługi związane z zarządzaniem przez użytkownika (np. rejestracja i usuwanie kont).

74. W kategoriach prawnych oznacza to, że użytkownicy Internetu i portale społecznościowe wspólnie ponoszą odpowiedzialność za przetwarzanie danych osobowych jako „administratorzy danych" w rozumieniu art. 2 lit. d) dyrektywy, aczkolwiek w różnym stopniu i przy zastosowaniu różnych obowiązków.

75. Zatem użytkownicy powinni wiedzieć i rozumieć, że poprzez przetwarzanie danych osobowych własnych oraz innych osób podlegają przepisom prawodawstwa UE dotyczącego ochrony danych, które wymaga m.in. uzyskania świadomej zgody osób, których informacje są przesyłane, oraz zapewnienia tym osobom prawa do sprostowania, sprzeciwu itd. Podobnie portale społecznościowe muszą m.in. wdrożyć odpowiednie techniczne i organizacyjne środki zapobiegające nieuprawnionemu przetwarzaniu, biorąc pod uwagę zagrożenia związane z przetwarzaniem danych i ich charakterem. To z kolei oznacza, że portale społecznościowe powinny zapewnić przyjazne dla użytkownika ustawienia domyślne, w tym ustawienia ograniczające dostęp do profilu użytkownika do jego własnych, samodzielnie wybranych kontaktów. Ustawienia powinny również wymagać wyrażenia zgody przez użytkownika zanim jakikolwiek profil zostanie udostępniony osobom trzecim, a profile o ograniczonym dostępie nie powinny być znajdowane przez wyszukiwarki wewnętrzne.

76. Niestety istnieje różnica pomiędzy wymogami prawnymi a faktyczną zgodnością. Podczas gdy, w sensie prawnym, użytkownicy Internetu są uważani za administratorów danych i są związani ramami prawnymi UE w zakresie ochrony danych i prywatności, w rzeczywistości często nie są świadomi tej roli. Ogólnie mówiąc, mają bardzo małą wiedzę o tym, że przetwarzają dane osobowe oraz że z publikowaniem takich informacji wiążą się zagrożenia dla prywatności i ochrony danych. Szczególnie młodzież umieszcza w Internecie treści, lekceważąc konsekwencje dla siebie i innych osób, np. w kontekście późniejszych zapisów do instytucji edukacyjnych lub starania się o pracę.

([1]) Zob. opinia grupy roboczej art. 29 WP 168 w sprawie portali społecznościowych, przyjęta w dniu 12 czerwca 2009 r.

([2]) „Administrator danych" oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych; jeżeli cele i sposoby przetwarzania danych są określane w przepisach ustawowych i wykonawczych lub przepisach wspólnotowych, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub wspólnotowe.

77. Jednoczenie operatorzy portali społecznościowych często wybierają wstępnie ustawienia domyślne w oparciu o opcję rezygnowania, ułatwiając w ten sposób ujawnianie danych osobowych. Niektórzy umożliwiają domyślne udostępnianie profilów wyszukiwarkom. W związku z tym powstaje pytanie, czy osoby fizyczne rzeczywiście wyraziły zgodę na ujawnienie danych, jak również czy portale społecznościowe działają zgodnie z art. 17 dyrektywy (opisanym powyżej), wymagającym od nich wdrożenia odpowiednich technicznych i organizacyjnych środków zapobiegających nieuprawnionemu przetwarzaniu.

VI.2. **Zagrożenia powodowane przez portale społecznościowe i sugerowane przeciwdziałanie tym zagrożeniom**

78. Wynikiem powyżej opisanych zagadnień jest wzrost zagrożenia dla prywatności i ochrony danych osób fizycznych. Naraża to użytkowników Internetu i osoby, których dane przesłano, na jawne naruszenie ich prywatności i ochrony danych.

79. W tym kontekście kwestią, którą Komisja powinna się zająć, jest co należy i można zrobić, aby rozwiązać ten problem. Niniejsza opinia nie zawiera wyczerpującej odpowiedzi na to pytanie, ale przedstawia kilka sugestii do dalszego rozważenia.

Inwestowanie w edukację użytkowników Internetu

80. Pierwszą sugestią jest inwestowanie w edukację użytkowników. Pod tym względem instytucje UE i organy krajowe powinny zainwestować w edukowanie i poszerzanie wiedzy w zakresie zagrożeń, jakie stanowią strony internetowe portali społecznościowych. Na przykład DG ds. Społeczeństwa Informacyjnego i Mediów uruchomiła program Bezpieczniejszy Internet, który ma na celu zwiększenie roli dzieci i młodzieży oraz ich ochronę poprzez na przykład działania poszerzające wiedzę ([1]). Niedawno instytucje UE rozpoczęły kampanię „Pomyśl, zanim napiszesz", aby poszerzyć wiedzę na temat zagrożeń wynikających z udostępniania nieznajomymi danych osobowych.

81. EIOD zachęca Komisję do dalszego wspierania tego typu działań. Jednakże sami operatorzy portali społecznościowych również powinni odgrywać aktywną rolę, ponieważ mają prawny i społeczny obowiązek edukowania użytkowników w zakresie korzystania z ich usług w sposób bezpieczny i przyjazny dla prywatności.

82. Jak opisano powyżej, publikując informacje na portalach społecznościowych, można je domyślnie udostępnić na kilka różnych sposobów. Na przykład informacje mogą zostać ogólnie udostępnione, w tym wyszukiwarkom internetowym, które mogą je indeksować, zapewniając w ten sposób bezpośredni odnośnik do tych informacji. Z drugiej strony udostępnianie informacji może być ograniczone do „wybranych przyjaciół" lub mogą być one zupełnie prywatne. Oczywiście zezwolenia dotyczące profilu i stosowana terminologia różnią się w zależności od portalu.

83. Jednakże, jak w skrócie przedstawiono powyżej, bardzo niewielu użytkowników serwisów społecznościowych wie, jak kontrolować dostęp do publikowanych informacji, a co dopiero jak zmienić domyślne ustawienia prywatności. Ustawienia prywatności zwykle pozostają niezmienione, ponieważ użytkownicy nie zdają sobie sprawy ze skutków niezmieniania tych ustawień lub nie wiedzą, jak to zrobić. Dlatego też najczęściej brak zmiany ustawień prywatności nie oznacza, że osoby fizyczne podjęły świadomą decyzję o zezwoleniu na udostępnianie informacji. W tym kontekście jest szczególnie ważne, aby osoby trzecie, takie jak wyszukiwarki, nie przekazywały odnośników do poszczególnych profilów zgodnie z założeniem, że użytkownicy domyślnie zezwolili (bez zmiany ustawień prywatności) na udostępnianie informacji bez ograniczeń.

84. Chociaż edukacja użytkowników może pomóc w rozwiązaniu tego problemu, sama w sobie nie wystarczy. Według zaleceń grupy roboczej art. 29 zawartych w jej opinii w sprawie portali społecznościowych dostawcy usług portali społecznościowych powinni oferować przyjazne dla prywatności, bezpłatne domyślne ustawienia prywatności. Dzięki temu użytkownicy byliby bardziej świadomi swoich działań i mieli możliwość podejmowania lepszych decyzji co do tego, czy chcą udostępniać informacje i komu.

Rola samoregulacji

85. Komisja zawarła porozumienie z dwudziestoma dostawcami usług portali społecznościowych, które znane jest jako „Zasady bezpieczniejszego korzystania z portali społecznościowych dla UE" ([2]). Celem porozumienia jest poprawienie bezpieczeństwa nieletnich w czasie korzystania ze stron portali społecznościowych w Europie. Zasady te obejmują wiele wymogów wywodzących się ze stosowania wyżej opisanych ram prawnych dotyczących ochrony danych. Obejmują one na przykład wymóg zwiększenie roli użytkowników poprzez narzędzia i technologie w celu zagwarantowania, że mogą oni kontrolować wykorzystywanie i rozpowszechnianie swoich danych osobowych. Obejmuje to również potrzebę zapewnienia domyślnych ustawień prywatności.

86. Na początku stycznia 2010 r. Komisja udostępniła wnioski ze sprawozdania oceniającego wdrażanie tych zasad ([3]). Zaniepokojenie EIOD budzi fakt, że sprawozdanie wykazuje, iż podjęto pewne kroki, natomiast wielu innych nie zrealizowano. Na przykład sprawozdanie ujawniło problemy w zakresie przekazywania informacji o środkach i narzędziach bezpieczeństwa dostępnych na

([1]) Informacje na temat tego programu dostępne są pod adresem: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Zasady te dostępne są pod adresem: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Sprawozdanie na temat oceny wdrożenia zasad bezpieczniejszych portali społecznościowych w UE, dostępne pod adresem: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

stronach internetowych. Wykazano w nim również, że mniej niż połowa sygnatariuszy porozumienia ogranicza dostęp do profilów nieletnich wyłącznie do ich przyjaciół.

Potrzeba obowiązkowego domyślnego ustawienia prywatności

87. W tym kontekście najważniejszą kwestią jest to, czy dodatkowe środki o charakterze politycznym są konieczne do zagwarantowania, że portale społecznościowe skonfigurują swoje usługi z zastosowaniem domyślnego ustawienia prywatności. Kwestię tę poruszyła była komisarz ds. społeczeństwa informacyjnego i mediów Viviane Reding, która zwróciła uwagę, że prawodawstwo może być niezbędne ([1]). Podobnie Europejski Komitet Ekonomiczno-Społeczny stwierdził, że oprócz samoregulacji należy prawnie narzucić minimalne normy ochrony ([2]).

88. Jak zauważono powyżej, obowiązek nałożony na dostawców usług portali społecznościowych co do wprowadzenia domyślnych ustawień prywatności można pośrednio wywieść z art. 17 dyrektywy o ochronie danych ([3]), który zobowiązuje administratorów danych do wdrożenia odpowiednich środków technicznych i organizacyjnych („zarówno przy opracowywaniu systemu przetwarzania danych, jak i podczas samego ich przetwarzania"), aby utrzymać bezpieczeństwo i zapobiec nieuprawnionemu przetwarzaniu, biorąc pod uwagę zagrożenia wynikające z przetwarzania danych oraz charakter danych.

89. Jednakże artykuł ten jest zbyt ogólny i pozbawiony szczegółowości, również w tym kontekście. Nie stwierdza się w nim wyraźnie, co rozumie się przez odpowiednie środki techniczne i organizacyjne w kontekście portali społecznościowych. Obecna sytuacja wiąże się zatem z niepewnością prawną, które powoduje problemy, zarówno dla organów regulacyjnych, jak i osób fizycznych, których prywatność i dane osobowe nie są w pełni chronione.

90. W świetle powyższego EIOD zaleca Komisji przygotowanie prawodawstwa, które obejmowałoby, jako minimum, nadrzędny wymóg dotyczący obowiązkowych ustawień prywatności, połączony z bardziej szczegółowymi wymogami w zakresie:

a) zapewnienia ustawień ograniczających dostęp do profilu użytkownika do jego własnych, samodzielnie wybranych kontaktów. Ustawienia powinny również wymagać wyrażenia zgody przez użytkownika zanim jakikolwiek profil zostanie udostępniony osobom trzecim;

b) zagwarantowania, że profile o ograniczonym dostępie nie mogą być znajdowane przez wyszukiwarki wewnętrzne/zewnętrzne.

91. Oprócz zapewnienia obowiązkowych domyślnych ustawień prywatności pozostaje pytanie, czy dodatkowe, szczególne środki ochrony danych i inne środki (na przykład dotyczące ochrony nieletnich) również byłyby odpowiednie. Wiąże się z nim ogólniejsza kwestia, czy właściwe byłoby utworzenie szczegółowych ram prawnych dla tych rodzajów usług, które oprócz przewidywania obowiązkowych ustawień prywatności regulowałyby inne aspekty. EIOD prosi Komisję o wzięcie tej kwestii pod rozwagę.

VII. **DOMYŚLNE USTAWIENIA PRYWATNOŚCI W PRZEGLĄDARKACH W CELU ZAGWARANTOWANIA ŚWIADOMEJ ZGODY NA OTRZYMYWANIE REKLAM**

92. Dostawcy reklamy internetowej wykorzystują pliki cookie oraz inne narzędzia do monitorowania zachowania indywidualnych użytkowników w czasie ich surfowania po Internecie w celu katalogowania ich zainteresowań i tworzenia profilów. Informacje te są następnie wykorzystywane do wysyłania im ukierunkowanych reklam ([4]).

VII.1. **Pozostałe wyzwania i zagrożenia w obecnych ramach prawnych dotyczących ochrony danych/prywatności**

93. Przetwarzanie to jest objęte dyrektywą o ochronie danych (gdy dotyczy danych osobowych) oraz art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Artykuł ten wyraźnie wymaga informowania użytkownika o gromadzeniu na jego komputerze lub innym urządzeniu takich narzędzi jak pliki cookie itd. i zapewnieniu mu możliwości zareagowania na to poprzez wyrażenie zgody lub odmowę ([5]).

94. Do chwili obecnej dostawcy reklamy internetowej polegali na ustawieniach wyszukiwarki i polityce prywatności, żeby informować użytkowników oraz umożliwić im wyrażenie zgody na otrzymywanie plików cookie lub odmowę tej zgody. Wyjaśniali w polityce prywatności

([1]) Viviane Reding, członek Komisji Europejskiej odpowiedzialna za społeczeństwo informacyjne i media, „Pomyśl, zanim napiszesz! Jak sprawić, aby portale społecznościowe były bezpieczniejsze dla dzieci i nastolatków?" (Think before you post! How to make social networking sites safer for children and teenagers?), Dzień Bezpiecznego Internetu, Strasburg, dnia 9 lutego 2010 r.

([2]) Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie wpływu portali społecznościowych na obywateli/konsumentów, dnia 4 listopada 2009 r.

([3]) Omówiony również w pkt 33 niniejszego dokumentu.

([4]) Śledzące pliki cookie (tzw. ciasteczka) to małe pliki tekstowe zawierające niepowtarzalny identyfikator. Zwykle reklamodawcy internetowi (a także operatorzy lub wydawcy stron internetowych) umieszczają pliki cookie na dyskach twardych odwiedzających, w szczególności w przeglądarkach użytkowników Internetu, gdy odwiedzający po raz pierwszy wejdą na stronę internetową zawierającą reklamy będące częścią ich sieci. Plik cookie umożliwia reklamodawcy internetowemu rozpoznanie odwiedzającego, który ponownie odwiedzi daną stronę internetową lub każdą inną stronę w ramach sieci reklamowej. Takie powtarzające się odwiedziny umożliwią reklamodawcy internetowemu opracowanie profilu odwiedzającego.

([5]) Artykuł 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej niedawno zmieniono w celu zwiększenia ochrony przed przechwyceniem komunikacji użytkowników za pośrednictwem np. oprogramowania szpiegującego i plików cookie przechowywanych na komputerze użytkownika lub innym urządzeniu. Na mocy nowej dyrektywy użytkownicy powinni mieć zapewnione lepsze informacje i łatwiejsze sposoby kontrolowania tego, czy chcą, aby pliki cookie były przechowywane na ich terminalach.

wydawców, w jaki sposób można zrezygnować z otrzymywania wszystkich plików cookie lub przyjmować je w poszczególnych przypadkach. W ten sposób zamierzali spełniać obowiązek oferowania użytkownikom prawa od odrzucenia plików cookie.

95. Podczas gdy metoda ta (poprzez przeglądarkę internetową) rzeczywiście może skutecznie zapewnić wyrażanie świadomej zgody, rzeczywistość jest zupełnie inna. Na ogół użytkownicy nie maja podstawowej wiedzy na temat gromadzenia danych, a tym bardziej od osób trzecich, wartości takich danych, ich wykorzystania, sposobu działania tej technologii, a szczególnie jak i gdzie można z plików cookie zrezygnować. Kroki, jakie użytkownik musi wykonać, aby zrezygnować z otrzymywania plików cookie, wydają się nie tylko skomplikowane, ale również nadmierne (najpierw musi ustawić przeglądarkę, aby akceptowała pliki cookie, a następnie skorzystać z opcji rezygnowania).

96. Wskutek tego w praktyce bardzo niewiele osób korzysta z opcji rezygnowania, nie dlatego, że podjęły świadomą decyzję o akceptowaniu reklamy behawioralnej, ale raczej dlatego, że nie zdają sobie sprawy z tego, iż poprzez niekorzystanie z tej opcji w rzeczywistości akceptują otrzymywanie plików cookie.

97. Dlatego też chociaż w sensie prawnym art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej zapewnia skuteczną ochronę prawną, w praktyce uznaje się, że użytkownicy Internetu wyrażają zgodę na objęcie monitorowaniem dla celów wysyłania reklamy behawioralnej, podczas gdy w rzeczywistości w wielu, jeżeli nie w większości przypadku, są całkowicie nieświadomi, że takie monitorowanie ma miejsce.

98. Grupa robocza art. 29 przygotowuje przydatną opinię mającą na celu wyjaśnienie wymogów prawnych dotyczących prezentowania reklamy behawioralnej. Jednakże interpretacja może nie być sama w sobie wystarczająca do rozwiązania tego problemu i być może Unia Europejska będzie musiała podjąć dodatkowe działania.

VII.2. **Potrzeba dalszych działań, w szczególności przewidujących obowiązkowe domyślne ustawienia prywatności**

99. Jak opisano powyżej, przeglądarki internetowe zwykle pozwalają na pewien poziom kontroli nad pewnymi rodzajami plików cookie. Obecnie ustawienia domyślne większości przeglądarek internetowych akceptują wszystkie pliki cookie. Innymi słowy, domyślnie przeglądarki internetowe są ustawione na akceptowanie wszystkich plików cookie, niezależnie od ich celu. Jedynie gdy użytkownik zmieni ustawienia swojej przeglądarki internetowej, żeby odrzucała pliki cookie, co – jak opisano powyżej – robi bardzo niewiele osób, nie będzie otrzymywać plików cookie. Ponadto w trakcie pierwszej instalacji lub aktualizacji programu przeglądarki nie istnieje żaden kreator ustawień prywatności.

100. Sposobem zaradzenia powyższemu problemowi byłoby wyposażenie przeglądarek w domyślne ustawienia prywatności. Innymi słowy, przeglądarki posiadałyby ustawienie „nie akceptuj plików cookie osób trzecich". Aby uzupełnić to rozwiązanie i zwiększyć jego skuteczność, wyszukiwarka powinna żądać od użytkownika przejścia przez kreator ustawień prywatności przy pierwszej instalacji lub aktualizacji przeglądarki. Potrzebne są bardziej szczegółowe i przejrzyste informacje na temat rodzajów plików cookie oraz przydatności niektórych z nich. Użytkownicy chcący być monitorowani w celu otrzymywania reklamy będą należycie informowani i będą musieli zmienić ustawienia przeglądarki. Zapewniłoby im to większą kontrolę nad swoimi danymi osobowymi i prywatnością. Zdaniem EIOD byłby to efektywny sposób poszanowania i zapewnienia zgody użytkownika [1].

101. Biorąc pod uwagę z jednej strony powszechny charakter problemu, czyli liczbę użytkowników Internetu, którzy są obecnie monitorowani w oparciu o iluzoryczną zgodę, a z drugiej skalę interesu, potrzeba dodatkowych zabezpieczeń staje się poważniejsza. Wdrożenie zasady poszanowania prywatności od samego początku w aplikacjach przeglądarek internetowych mogłoby spowodować zasadniczą zmianę, dając osobom fizycznym kontrolę nad praktykami gromadzenia danych wykorzystywanymi w celach reklamowych.

102. Z tych powodów EIOD nalega, aby Komisja rozważyła środki ustawodawcze wymagające obowiązkowego domyślnego ustawienia prywatności w przeglądarkach oraz udzielania istotnych informacji.

VIII. **INNE ZASADY MAJĄCE NA CELU OCHRONĘ PRYWATNOŚCI OSÓB FIZYCZNYCH/OCHRONĘ DANYCH**

103. Chociaż zasada poszanowania prywatności od samego początku ma duże możliwości poprawienia ochrony danych osobowych osób fizycznych i ich prywatności, konieczne jest opracowanie i wdrożenia do prawodawstwa zasad uzupełniających w celu zapewnienia zaufania konsumentów do TIK. W tym kontekście EIOD zwraca uwagę na zasadę odpowiedzialności i ukończenie procesu tworzenia obowiązkowych ram dotyczących naruszenia bezpieczeństwa, które mają zastosowanie we wszystkich sektorach.

VIII.1. **Zasada odpowiedzialności w celu zapewnienia zgodności z zasadą poszanowania prywatności od samego początku**

104. W dokumencie grupy roboczej art. 29 pt. „Przyszłość prywatności" [2] zaleca się włączenie zasady odpowiedzialności do dyrektywy o ochronie danych. Zasada ta jest

[1] Jednocześnie EIOD zdaje sobie sprawę, że nie rozwiązałoby to całkowicie problemu, ponieważ istnieją pliki cookie, które nie mogą być kontrolowane za pośrednictwem przeglądarki, np. pliki Flash cookie. Z tego względu twórcy przeglądarek musieliby domyślnie włączyć opcje kontroli Flash do opcji kontroli plików cookie przy udostępnianiu nowych przeglądarek.

[2] Opinia grupy roboczej art. 29 WP 168 „Przyszłość prywatności. Wspólny wkład w konsultacje Komisji Europejskiej w sprawie ram prawnych dotyczących podstawowego prawa do ochrony danych osobowych" (The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data), przyjęta w dniu 1 grudnia 2009 r.

obecna w niektórych międzynarodowych instrumentach dotyczących ochrony danych ([1]). Wymaga od organizacji wdrożenia procedur dostosowujących ją do istniejącego prawodawstwa, a także ustalenia metod oceniania i wykazywania zgodności z prawem i innymi obowiązującymi instrumentami.

105. EIOD w pełni popiera zalecenie grupy roboczej art. 29. Uważa, że zasada te będzie miała duże znaczenie dla ułatwienia skutecznego stosowania zasad i zobowiązań dotyczących ochrony danych. Zasada odpowiedzialności będzie wymagała od administratorów danych wykazania, że wprowadzili mechanizm niezbędny do zapewnienia zgodności z obowiązującymi przepisami w zakresie ochrony danych. Prawdopodobnie przyczyni się to do skutecznego wdrożenia zasady poszanowania prywatności od samego początku w TIK, ponieważ jest to szczególnie stosowny element pod względem wykazywania odpowiedzialności.

106. Do pomiaru i wykazania odpowiedzialności administratorzy danych mogliby wykorzystać wewnętrzne procedury i osoby trzecie, które mogą przeprowadzić audyt lub inne rodzaje kontroli i weryfikacji, co może skutkować przyznaniem odznaczeń lub nagród. W tym kontekście EIOD zaleca Komisji rozważenie, czy – oprócz ogólnej zasady odpowiedzialności – przydatny może być wymóg prawny dotyczący określonych środków związanych z odpowiedzialnością, takich jak konieczność dokonywania oceny skutków w zakresie ochrony danych i prywatności oraz okoliczności takiej oceny.

VIII.2. **Naruszenie bezpieczeństwa: ukończenie procesu tworzenia ram prawnych**

107. Zeszłoroczne poprawki do dyrektywy o prywatności i łączności elektronicznej wprowadziły wymóg zgłaszania przypadków naruszenia danych osobom, których te dane dotyczą, oraz właściwym organom. Naruszenie danych jest ogólnie definiowane jako każde naruszenie prowadzące do zniszczenia, utraty, ujawnienia itd. danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych w związku z usługą. Powiadomienie osób fizycznych będzie konieczne, jeżeli naruszenie danych może wywrzeć niekorzystny wpływ na ich dane osobowe lub prywatność. Może to mieć miejsce w przypadku gdy naruszenie może doprowadzić do kradzieży tożsamości lub poważnego upokorzenia lub szkody dla reputacji. Powiadomienie właściwych organów będzie wymagane w przypadku każdego naruszenia danych, niezależnie od tego, czy istnieje zagrożenie dla osób fizycznych.

Stosowanie obowiązków związanych z naruszeniem bezpieczeństwa we wszystkich sektorach

108. Niestety obowiązek ten stosuje się wyłącznie do dostawców publicznie dostępnych usług łączności elektronicznej, takich jak: spółki telekomunikacyjne, dostawcy usług dostępu do Internetu, dostawców usług poczty elektronicznej itd. EIOD zaleca Komisji przedstawienie wniosków w sprawie naruszenia bezpieczeństwa mających zastosowanie do wszystkich sektorów. Jeśli chodzi o treść takich ram, EIOD uważa, że ramy prawne dotyczące naruszenia bezpieczeństwa przyjęte w dyrektywie o prywatności i łączności elektronicznej stanowią złoty środek między ochroną praw osób fizycznych, w tym praw do ochrony danych i do prywatności, a obowiązkami nałożonych na podmioty objęte dyrektywą. Jednocześnie są to ramy posiadające prawdziwą siłę, ponieważ są wspierane konstruktywnymi przepisami wykonawczymi, które zapewniają organom wystarczające uprawnienia do prowadzenia dochodzeń i nakładania kar w przypadku niezgodności.

109. EIOD zaleca zatem Komisji przyjęcie wniosku ustawodawczego stosującego te ramy do wszystkich sektorów, z właściwymi poprawkami, jeśli to konieczne. Ponadto zapewniłoby to stosowanie takich samych norm i procedur we wszystkich sektorach.

Ukończenie procesu tworzenia ram prawnych przewidzianych w dyrektywie o prywatności i łączności elektronicznej poprzez procedurę komitetową

110. Zmieniona dyrektywa o prywatności i łączności elektronicznej upoważnia Komisję do przyjęcia technicznych środków wykonawczych, tj. szczegółowych środków dotyczących powiadamiania o naruszeniach bezpieczeństwa, w drodze procedury komitetowej ([2]). To upoważnienie jest uzasadnione koniecznością zapewnienia spójnego wdrożenia i stosowania ram prawnych dotyczących naruszenia bezpieczeństwa. Spójne wdrożenie ma na celu zagwarantowanie, że osoby fizyczne w całej Wspólnocie korzystają z równie wysokiego poziomu ochrony i że właściwe podmioty nie są obciążone różnymi wymogami co do powiadamiania.

111. Dyrektywę o prywatności i łączności elektronicznej przyjęto w listopadzie 2009 r. Wydaje się, że nie istnieje żaden powód uzasadniający opóźnianie rozpoczęcia prac nad przyjęciem technicznych środków wykonawczych. EIOD zorganizował dwa seminaria, które miały na celu wymianę i zbieranie doświadczeń w zakresie powiadamiania o naruszeniu danych. Z przyjemnością podzieli się wynikami tych działań i oczekuje współpracy z Komisją oraz innymi zainteresowanymi stronami nad dostosowaniem ogólnych ram prawnych w zakresie naruszenia danych.

112. EIOD zaleca Komisji szybkie podjęcie koniecznych kroków. Przed przyjęciem technicznych środków wykonawczych Komisja musi przeprowadzić szeroko zakrojone konsultacje, w tym z udziałem Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji, EIOD i grupy roboczej art. 29. Ponadto konsultacjami muszą zostać objęte także inne właściwe zainteresowane strony, szczególnie w celu poinformowania ich o najlepszych technicznych i gospodarczych środkach wykonawczych.

([1]) Wytyczne OECD z 1980 r. w sprawie ochrony prywatności i transgranicznego przepływu danych osobowych; deklaracja madrycka o prywatności w sprawie globalnych norm w zakresie prywatności na całym świecie, dnia 3 listopada 2009 r.

([2]) Procedura komitetowa polega na przyjęciu technicznych środków wykonawczych za pośrednictwem komitetu przedstawicieli państw członkowskich, któremu przewodniczy Komisja. W przypadku dyrektywy o prywatności i łączności elektronicznej ma zastosowanie tzw. procedura regulacyjna połączona z kontrolą, co oznacza, że Parlament Europejski i Rada mogą wyrazić sprzeciw wobec środków zaproponowanych przez Komisję. Zob. http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **WNIOSKI**

113. Ustalono, że zaufanie, a raczej jego brak, jest podstawowym zagadnieniem w powstawaniu i skutecznym wprowadzaniu technologii informacyjno-komunikacyjnych. Jeżeli ludzie nie ufają TIK, technologie te prawdopodobnie nie odniosą sukcesu. Zaufanie do TIK zależy od różnych czynników – najważniejszym jest zagwarantowanie, że te technologie nie ograniczają podstawowych praw osób fizycznych do prywatności i ochrony danych osobowych.

114. W celu dalszego wzmocnienia ram prawnych dotyczących ochrony danych/prywatności, które to zasady pozostają całkowicie uzasadnione w społeczeństwie informacyjnym, EIOD proponuje, aby Komisja wprowadziła poszanowanie prywatności od samego początku na różnych szczeblach prawa i formułowania zasad polityki.

115. Zaleca Komisji cztery następujące kierunki działania:

a) zaproponowanie włączenia ogólnego przepisu o poszanowaniu prywatności od samego początku do ram prawnych dotyczących ochrony danych. Przepis ten powinien być neutralny technologicznie, a zgodność z nim powinna być obowiązkowa na różnych etapach;

b) rozwinięcie tego ogólnego przepisu w przepisach szczegółowych, gdy w różnych sektorach zaproponowane będą szczegółowe instrumenty prawne. Te przepisy szczegółowe już mogłyby zostać włączone do instrumentów prawnych; na podstawie art. 17 dyrektywy o ochronie danych (oraz innych istniejących przepisów);

c) uwzględnienie poszanowania prywatności od samego początku jako naczelnej zasady europejskiej agendy cyfrowej;

d) wprowadzenie poszanowania prywatności od samego początku jako zasady w innych inicjatywach UE (głównie o charakterze nieustawodawczym).

116. W trzech wyznaczonych obszarach TIK EIOD zaleca Komisji dokonanie oceny potrzeby przedstawienia wniosków w sprawie wdrożenia zasady poszanowania prywatności od samego początku w określony sposób:

a) w odniesieniu do RFID – zaproponowanie środków ustawodawczych regulujących podstawowe kwestie wykorzystywania RFID na wypadek gdyby nie powiodło się skuteczne wdrożenie istniejących ram prawnych poprzez samoregulację. W szczególności należy uwzględnić zasadę wyrażania zgody w punkcie sprzedaży, zgodnie z którą wszystkie etykiety RFID dołączone do produktów konsumenckich byłyby domyślnie dezaktywowane w punkcie sprzedaży;

b) w odniesieniu do portali społecznościowych – przygotowanie prawodawstwa, które obejmowałoby, jako minimum, nadrzędny wymóg dotyczący obowiązkowych ustawień prywatności, połączony z bardziej szczegółowymi wymogami w zakresie ograniczenia dostępu do profilów użytkowników do własnych, samodzielnie wybranych kontaktów użytkownika, a także zagwarantowania, że profile o ograniczonym dostępie nie mogą być znajdowane przez wyszukiwarki wewnętrzne/zewnętrzne;

c) w odniesieniu do reklamy ukierunkowanej – rozważenie przepisów przewidujących w ustawieniach przeglądarek domyślne odrzucanie plików cookie osób trzecich i wymaganie od użytkownika skorzystania z kreatora ustawień prywatności przy pierwszej instalacji lub aktualizacji przeglądarki.

117. Ponadto EIOD zaleca Komisji:

a) rozważenie wdrożenia zasady odpowiedzialności w istniejącej dyrektywie o ochronie danych; oraz

b) opracowanie ram zasad i procedur wdrażania przepisów dyrektywy o ochronie prywatności i łączności elektronicznej dotyczących powiadamiania o naruszeniu bezpieczeństwa, a także rozszerzenia ich zakresu stosowania na wszystkich administratorów danych.

Sporządzono w Brukseli dnia 18 marca 2010 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych