I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych 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

(2008/C 101/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

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

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 8,

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych,

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. **WSTĘP**

1. W dniu 15 marca 2007 r. Komisja opublikowała komunikat zatytułowany „Identyfikacja radiowa (RFID) w Europie: w stronę ram polityki" ([1]) (zwany dalej: „komunikatem"). Na mocy art. 41 rozporządzenia (WE) nr 45/2001 EIOD odpowiada za doradzanie instytucjom i organom wspólnotowym we wszystkich kwestiach związanych z przetwarzaniem danych osobowych. Zgodnie z tym artykułem EIOD przedstawia niniejszą opinię.

2. Niniejszą opinię należy traktować jako odpowiedź EIOD na ten komunikat, jak również reakcję na inne działania w obszarze RFID, które miały miejsce od przyjęcia komunikatu. Wśród innych działań w tej dziedzinie, które uwzględniono w niniejszej opinii, należy wymienić:

— decyzję Komisji z dnia 28 czerwca 2007 r. powołującą grupę ekspertów do spraw identyfikacji radiowej ([2]), bezpośredni skutek komunikatu. Grupa ta znana jest również jako „grupa ds. RFID skupiająca strony zainteresowane" (ang. *RFID-Stakeholders Group*). Zgodnie z art. 4 ust. 4 lit. b) tej decyzji EIOD uczestniczy w działaniach grupy w charakterze obserwatora,

— rezolucję Rady z dnia 22 marca 2007 r. w sprawie strategii na rzecz bezpiecznego społeczeństwa informacyjnego w Europie ([3]),

— projekt „RFID i zarządzanie tożsamością" zainicjowany przez Parlament Europejski ([4]),

([1]) COM(2007) 96 wersja ostateczna.
([2]) Decyzja 467/2007/WE (Dz.U. L 176 z 6.7.2007, str. 25).
([3]) Dz.U. C 68 z 24.3.2007, str. 1.
([4]) Projekt „RFID i zarządzanie tożsamością — studium przypadku z pierwszej linii działań na rzecz otoczenia inteligentnego" zamówiony przez Zespół ds. Oceny Rozwiązań Naukowych i Technologicznych Parlamentu Europejskiego (STOA) a wykonany przez ETAG (Europejską Grupę ds. Oceny Technologii), http://www.europarl.europa.eu/stoa/default_en.htm

— wydanie przez Grupę Roboczą ds. Ochrony Danych powołaną na mocy art. 29 opinii nr 4/2007 w sprawie pojęcia danych osobowych ([1]),

— Komunikat Komisji dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych ([2]) oraz opinię EIOD na temat tego komunikatu z dnia 25 lipca 2007 r. ([3]),

— przyjęcie przez Komisję wniosku w sprawie dyrektywy zmieniającej (między innymi) dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej ([4]).

3. EIOD z zadowoleniem przyjmuje komunikat Komisji w sprawie RFID, ponieważ zajęto się w nim głównymi zagadnieniami wyłaniającymi się w kontekście rozpowszechniania technologii RFID, nie zaniedbując głównych kwestii związanych z ochroną danych i prywatności. Komunikat ten poprzedziły spójne i skrupulatne prace przygotowawcze. Przed przygotowaniem komunikatu przeprowadzono pięć warsztatów tematycznych oraz internetowe konsultacje publiczne ([5]), które zamówiła Komisja.

4. EIOD zgadza się z poglądem, że systemy RFID mogą odegrać kluczową rolę w rozwoju społeczeństwa informacyjnego określaną zwykle mianem „internetu rzeczy" (ang. *Internet of things*), i w pełni podziela obawy, o których mowa w art. 3.2 komunikatu, że systemy RFID mogą stanowić zagrożenie dla prawa do prywatności osób i ochrony danych. W sprawozdaniu za 2005 rok EIOD uznał RFID — wraz z biometrią, otoczeniem inteligentnym oraz systemami zarządzania tożsamością — za rozwiązania technologiczne, które będą miały istotny wpływ na ochronę danych.

5. Zdaniem EIOD oswojenie technologii RFID i ich powszechne przyjęcie nie tylko będzie możliwe ze względu na ich atrakcyjność, wygodę lub oferowane przez nie nowe usługi, ale i zostanie ułatwione dzięki korzyściom płynącym z należycie dostosowanych i spójnych zabezpieczeń danych.

([1]) Dokument WP 136 opublikowany na stronie internetowej grupy roboczej.

([2]) Komunikat Komisji z dnia 7 marca 2007 r. dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych, COM(2007) 87 wersja ostateczna.

([3]) Dz.U. C 255 z 27.10.2007, str. 1. Zwana dalej: „Opinią na temat komunikatu w sprawie dyrektywy o ochronie danych".

([4]) Wniosek z dnia 13 listopada 2007 r. w sprawie 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 Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. 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 wersja ostateczna. Dyrektywa 2002/58/WE będzie dalej zwana „dyrektywą o prywatności i łączności elektronicznej".

([5]) http://www.rfidconsultation.eu/

6. Krótko mówiąc: EIOD uznaje RFID za podstawowe nowe rozwiązanie technologiczne, które w komunikacie Komisji słusznie nazwano początkiem nowego etapu rozwoju społeczeństwa informacyjnego.

7. Rozwiązanie to prowokuje ważne pytania w różnych dziedzinach; jedną z nich jest obszar ochrony danych i prywatności. Niniejsza opinia EIOD ogranicza się do tego obszaru.

II. **ZAKRES OPINII**

8. Opinia skupia się w szczególności na skutkach, jakie wspomniane rozwiązania mogą mieć dla ochrony danych i prywatności. Skutki te w chwili obecnej są niepewne, również ze względu na fakt, że rozwój systemów RFID i proces ich upowszechniania właśnie trwają i nie wiadomo, dokąd te zjawiska zaprowadzą.

9. W tym świetle EIOD przyjmuje następujące podejście:

— po pierwsze należy wyjaśnić, jakie praktyczne skutki dla ochrony danych i prywatności będzie miało rozpowszechnienie systemów RFID,

— po drugie, należy określić te skutki w kontekście obowiązujących ram prawnych dotyczących ochrony danych i prywatności,

— po trzecie, EIOD rozważa, czy skutki te wymagają wprowadzenia bardziej szczegółowych zasad rozwiązywania kwestii związanych z ochroną danych, które wynikają ze stosowania technologii RFID. Kwestia ta została już podniesiona przez EIOD w jego opinii na temat komunikatu w sprawie dyrektywy o ochronie danych i zostanie rozwinięta w niniejszej opinii.

10. Przyjmując to podejście, EIOD zamierza przyczynić się do tego, by podczas opracowywania systemów RFID i ich rozpowszechniania uwzględniano uzasadnione obawy dotyczące ochrony danych i prywatności.

III. **WYJAŚNIENIE SKUTKÓW**

Systemy i tagi RFID

11. Pomimo faktu, że — jak wspomniano — rozwój systemów RFID i ich upowszechnianie właśnie trwają, a ich wynik jest niepewny, można opisać główne cechy tych zjawisk pod kątem skutków, jakie te zjawiska mają dla ochrony danych.

12. W ocenie potencjalnych skutków technologii RFID dla ochrony dany danych i prywatności bardzo istotne jest nie tylko rozważenie samych tagów RFID, ale całej infrastruktury RFID: tag, czytnik, sieć, referencyjna baza danych i baza danych, w których przechowywane są dane wytworzone przez skojarzenie taga z czytnikiem. Jak podkreślono krótko we wprowadzeniu do komunikatu, RFID nie są jedynie „elektronicznymi etykietkami", a zatem kwestie związane z ochroną danych nie ograniczają się do tagów, ale obejmują wszystkie elementy całej infrastruktury RFID. W istocie każdy z tych elementów ma do odegrania pewną rolę we wdrażaniu europejskich ram prawnych dotyczących ochrony danych, kiedy jest to konieczne. Na elementy te wpływają główne czynniki rozwoju społeczeństwa informacyjnego, takie jak niemal nieograniczona szerokość pasma, wszechobecne połączenia sieciowe i nieskończona pojemność pamięci.

Wpływ systemów i tagów RFID

13. Niezależnie od konieczności zastosowania szerszego podejścia, o czym wspomniano w poprzednim akapicie, z kilku powodów w pierwszej kolejności skupiono się w niniejszej opinii na wykorzystaniu RFID do wyposażania w tagi produktów użytkowych w sektorze handlu detalicznego. Oczywistą przyczyną jest coraz szersze używanie tagów, które wydaje się zmierzać do ich powszechnego stosowania. W przeciwieństwie do innych zastosowań RFID, mających wąski lub ograniczony zakres, wyposażanie w tagi produktów potencjalnie może zostać wprowadzone na rynek na masową skalę. Już w tej chwili wiele produktów użytkowych jest wyposażonych w tag RFID. Wiąże się z tym fakt, że takie użycie będzie miało swój wpływ na olbrzymią liczbę osób, których dane osobowe potencjalnie mogą być przetwarzane za każdym razem, kiedy osoby te nabędą produkt wyposażony w tag RFID.

14. Należy zwrócić szczególną uwagę na konsekwencje, jakie dla posiadaczy produktów będzie miało wyposażenie tychże w tagi RFID. Systemy RFID mogą zwiększać zależność między przedmiotem a jego posiadaczem. Po zwiększeniu tego typu zależności posiadacza takiego przedmiotu można zlokalizować i sklasyfikować jako „osobę dysponującą niskim budżetem" lub osobę będącą „atrakcyjnym celem" przyszłych transakcji; nadmiernie zindywidualizowane przyporządkowanie [1] może prowadzić do automatycznego „karania" za pewne zachowania (obowiązek recyklingu, odpady, itp.). Jednostki nie powinny podlegać procesowi automatycznego podejmowania niekorzystnych decyzji. Ta właściwość RFID powoduje wzrost ryzyka, że społeczeństwo informacyjne przybliży się do sytuacji, w której decyzje będą podejmowane automatycznie i w której technologia będzie nadużywana, aby kontrolować ludzkie zachowania.

15. Dane przechowywane lub wytwarzane przez tag RFID mogą być danymi osobowymi, o których mowa w art. 2 dyrektywy o ochronie danych. Na przykład karty elektroniczne stosowane przy przejazdach mogą zawierać informacje o tożsamości, jak również o niedawnych przejazdach posiadacza. Gdyby ktoś pozbawiony skrupułów chciał śledzić dane osoby, wystarczyłoby, aby strategicznie rozmieścił czytniki, które dostarczałyby informacji o przemieszczaniu się posiadaczy kart, co stanowiłoby pogwałcenie ich prywatności i naruszenie ochrony danych osobowych.

16. Podobne zagrożenia dla prywatności mogłyby zaistnieć, nawet gdyby informacje, które przechowuje tag RFID, nie zawierały nazwisk jednostek. Tagi RFID zawierają niepowtarzalne identyfikatory dołączane do produktów użytkowych: w przypadku gdy każdy tag ma niepowtarzalny identyfikator, identyfikacji takiej można używać do celów nadzoru. Jeśli na przykład ktoś nosi zegarek, który ma tag RFID zawierający numer identyfikacyjny, może to stanowić również niepowtarzalny identyfikator osoby noszącej ten zegarek, nawet jeśli nie jest znana jej tożsamość. W zależności od tego, w jaki sposób informacja ta jest wykorzystywana — i umieszczana w odniesieniu do samego zegarka lub danej osoby — przedmiotowa dyrektywa będzie miała zastosowanie lub nie. Przykładowo miałaby ona zastosowanie w przypadku generowania informacji na temat miejsca przebywania osób, które to informacje mogłyby zostać wykorzystane do monitorowania zachowania tych osób lub na przykład do różnicowania cen, zabraniania dostępu lub do nadania niepożądanego rozgłosu.

17. W tym kontekście konieczne jest zadbanie o to, by aplikacje RFID były stosowane przy zachowaniu koniecznych środków technicznych, które zminimalizują ryzyko niepożądanego ujawnienia informacji. Środki takie mogą obejmować wymaganie, żeby infrastruktura RFID — zwłaszcza tagi RFID — została zaprojektowana sposób pozwalający uniknąć tego typu sytuacji. Na przykład można rozmieszczać karty RFID wyposażone w funkcję, która pozwoli je dezaktywować (ang. *kill command*). Opcja ta zostanie szerzej omówiona w rozdziale IV niniejszej opinii.

18. Dając możliwość śledzenia produktów po opuszczeniu przez nie punktu sprzedaży, systemy RFID powodują, że w debacie o prywatności pojawiają się nowe zagadnienia. W istocie przy analizie ich wpływu pod uwagę należy wziąć dwa elementy: stopień, w jakim dany przedmiot stanowi własność osobistą oraz jego mobilność [2].

19. Cykl życia danego produktu także może uzupełniać wymaganą analizę ryzyka i przyczyniać się do ilościowej oceny poszczególnych zagrożeń dotyczących prywatności. Zważywszy na fakt, że taga nie można dezaktywować, produkt o długim cyklu życia należący do użytkownika końcowego będzie mógł dostarczyć więcej odnośnych danych na temat posiadacza produktu i pozwoli stworzyć jego dokładniejszy profil. Z drugiej strony, produkt o krótkim cyklu życia, jak np. puszka z napojem, od etapu produkcji aż do momentu recyklingu może stanowić mniejsze zagrożenie, a co za tym idzie mogą go dotyczyć mniej restrykcyjne zasady niż te stosowane wobec produktu o dłuższym cyklu życia.

[1] Dr Sarah Spiekermann, dyrektor Berlińskiego Centrum Badań nad Ekonomią Internetu (Berlin Research Centre on Internet Economics), warsztaty poświęcone RFID i wszechobecnej komputeryzacji zorganizowane przez organizację Trans Atlantic Consumer Dialogue, 13 marca 2007 r.

[2] Dara J. Glasser, Kenneth W. Goodman and Norman G. Einspruch, Chips, tags and scanners: Ethical challenges for radio frequency identification, Ethics and Information Technology, Volume 9, No. 2/2007.

Zagadnienia związane z ochroną danych i prywatności w związku z wprowadzaniem systemu RFID

20. Aby lepiej zrozumieć skutki, jakie stosowanie systemów RFID będzie miało dla ochrony danych i prywatności, należy wymienić pięć podstawowych kwestii związanych z prywatnością i bezpieczeństwem.

21. Pierwszym zagadnieniem jest identyfikacja podmiotu danych. Ponad sześćdziesiąt lat temu tag RFID miał określać, czy „zbliża się przyjaciel czy wróg". Dzisiejsze systemy RFID są w stanie nie tylko określić ogólne cechy przedmiotu, ale mogą w sposób jednoznaczny pomóc w identyfikacji osoby; konieczne jest zatem przeprowadzanie tego w sposób uwzględniający ochronę danych.

22. Drugim zagadnieniem jest identyfikacja administratora danych. W przypadku systemów RFID identyfikacja administratora danych określonego w art. 2 lit. d) dyrektywy o ochronie danych może być trudniejsza, a zatem wymaga głębszej analizy. Zidentyfikowanie administratora danych pozostaje jednak kluczowym krokiem w ustalaniu odpowiedzialności poszczególnych podmiotów, które będą musiały pozostawać w zgodzie z ramami prawnymi dotyczącymi ochrony danych. W trakcie cyklu życia danego taga administrator danych, który je przetwarza, może zmieniać się kilka razy, w zależności od usług dodatkowych, które mogą być dostarczane w związku z oznaczonym przedmiotem.

23. Trzecim zagadnieniem jest malejące znaczenie tradycyjnego rozróżnienia między sferą osobistą a sferą publiczną. Chociaż rozróżnienie między przestrzenią prywatną a publiczną również w przeszłości nie było jednoznaczne, większość ludzi jest świadoma istnienia między nimi granic (oraz szarych stref) i rozmyślnie lub intuicyjnie podejmuje decyzje, w jaki sposób się zachować. Jak twierdzi Hall ([1]) przestrzeń osobista przekłada się zwykle na odległość fizyczną dzielącą od innych. Zarządzanie prywatnością można uznać również za dynamiczny proces regulowania granic ([2]). Nie zaskakuje zatem, że bezprzewodowy charakter komunikacji za pomocą tagów, jak również możliwość ich odczytywania „poza linią wzroku" wywołują zaniepokojenie dotyczące prywatności, gdyż rozmywają te tradycyjne granice i możliwości zarządzania nimi. Pojawiają się bowiem obawy, że jednostka może utracić częściowo lub całkowicie posiadaną dotąd kontrolę nad utrzymywaniem odległości. W związku z tym zarówno zwolennicy, jak i przeciwnicy pierwszych zastosowań systemów RFID skupiali się na ich możliwościach odczytu.

24. Czwarte zagadnienie dotyczy rozmiarów i fizycznych właściwości tagów RFID. Ponieważ tag zasadniczo musi być mały i tani, środki bezpieczeństwa, które można by zastosować w tej części systemu RFID, będą z definicji ograniczone. Jednak fakt, że komunikacja jest bezprzewodowa wprowadza nowy element ryzyka w porównaniu z komunikacją przewodową, a co za tym idzie potrzebne są dodatkowe wymagania w zakresie bezpieczeństwa.

25. Zagadnienie piąte dotyczy braku przejrzystości w przetwarzaniu (danych). Stosowanie systemów RFID może prowadzić do niezauważalnego gromadzenia i przetwarzania informacji, które mogłyby zostać wykorzystane do stworzenia profilu danej jednostki. Skutek ten można bardzo dobrze zilustrować, używając porównania systemów RFID do telefonu komórkowego — jak to zresztą robi się dość często. Z jednej strony technologia telefonii komórkowej zdobyła bardzo wysoki poziom akceptacji niezależnie od potencjalnego ryzyka ingerencji w sferę prywatności. Można dojść do wniosku, że systemy RFID zostaną przyjęte w taki sam sposób. Z drugiej strony należy podkreślić, że telefon komórkowy jest obiektem widzialnym, który pozostaje pod kontrolą użytkownika i można go wyłączyć. Tak nie jest w przypadku RFID.

26. Chociaż wspomniane wyżej niezauważalne gromadzenie i przetwarzanie informacji może być legalne, jest możliwe — a w różnych okolicznościach całkiem prawdopodobne — że będzie się ono odbywało również w sposób nielegalny.

27. Wyjaśnienia umieszczone w tym rozdziale prowadzą do następującego wniosku. Powszechne stosowanie technologii RFID jest zasadniczo nową kwestią i może mieć fundamentalny wpływ na nasze społeczeństwo oraz na ochronę praw podstawowych w tym społeczeństwie, takich jak ochrona danych i prywatności. Technologia RFID może przynieść zmianę jakościową.

IV. **OKREŚLENIE SKUTKÓW**

Wprowadzenie

28. Obecny rozdział zostanie poświęcony głównie wpływowi technologii RFID na ochronę praw podstawowych — takich jak ochrona danych i prywatności — w naszym społeczeństwie. Składa się on dwóch części; pierwsza z nich to krótki opis sposobu, w jaki te prawa podstawowe chronione są przez obecne ramy prawne. W drugiej części EIOD omówi możliwości pełnego wykorzystania tych ram. Zamiar ten przedstawiono w opinii na temat komunikatu w sprawie dyrektywy o ochronie danych, określając go jako „pełne wdrożenie obecnych przepisów dyrektywy".

29. Punkt wyjścia przedstawia się następująco: nowe rozwiązania technologiczne, takie jak systemy RFID mają wyraźny wpływ na konieczność stworzenia skutecznych ram prawnych w zakresie ochrony danych. Ponadto potrzeba skutecznej ochrony danych osobowych poszczególnych osób może ograniczać wykorzystywanie tych nowych technologii. Interakcja jest więc obustronna: technologia wpływa na prawodawstwo, a prawodawstwo wpływa na technologię ([3]).

([1]) Hall, E.T. 1966. The Hidden Dimension. (1st ed.). Garden City, N.Y: Doubleday. (Ukryty wymiar, Warszawa: Warszawskie Wydawnictwo Literackie Muza, 2003).

([2]) Altman, I. 1975 The Environment and Social Behaviour, Brooks/Cole Monterrey.

([3]) Zob. uwagi EIOD z marca 2006 roku do komunikatu Komisji w sprawie interoperacyjności między europejskimi bazami danych opublikowane na stronie internetowej EIOD.

Ochrona praw podstawowych

30. Ochrona podstawowych praw do ochrony danych i prywatności w Unii Europejskiej jest w pierwszym rzędzie zagwarantowana w ramach prawnych, które są potrzebne, gdyż mamy do czynienia z prawami, o których mowa w art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności oraz w art. 7 i 8 Karty praw podstawowych Unii Europejskiej. Odpowiednie ramy prawne dotyczące ochrony danych i RFID to zasadniczo: dyrektywa o ochronie danych 95/46/WE oraz dyrektywa o prywatności i łączności elektronicznej 2002/58/WE ([1]).

31. Ogólne ramy prawne mające zastosowanie do ochrony danych określone w dyrektywie 95/46/WE dotyczą RFID w stopniu, w jakim dane przetwarzane przez systemy RFID pokrywają się z definicją danych osobowych. O ile w niektórych przypadkach aplikacje RFID wyraźnie przetwarzają dane osobowe i niewątpliwie wchodzą w zakres stosowania dyrektywy o ochronie danych, istnieją również zastosowania, w przypadku których stosowanie dyrektywy o ochronie danych może nie być takie oczywiste. Opinia nr 4/2007 Grupy Roboczej ds. Ochrony Danych powołanej na mocy art. 29 w sprawie pojęcia danych osobowych ma być przyczynkiem do wypracowania jaśniejszej i powszechnie uznawanej koncepcji danych osobowych, a przez to ma rozwiać tę niepewność ([2]).

32. W przypadku dyrektywy o prywatności i łączności elektronicznej sytuacja przedstawia się następująco. Do chwili obecnej nie jest jasne, czy dyrektywa ta dotyczy zastosowań RFID. Z tego powodu wniosek Komisji z dnia 13 listopada 2007 r. w sprawie zmian do tej dyrektywy zawiera przepis, który ma sprecyzować, że dyrektywa w rzeczywistości dotyczy niektórych zastosowań RFID. Jednak inne zastosowania RFID mogą nie zostać objęte ze względu na ograniczenie tej dyrektywy do przetwarzania danych osobowych w związku ze świadczeniem dostępnych publicznie usług łączności elektronicznej w publicznych sieciach telekomunikacyjnych.

33. Ochrona danych osobowych może zostać uzupełniona szeregiem instrumentów samoregulacyjnych (ramy pozaprawne). Stosowanie tych instrumentów jest aktywnie propagowane w obu dyrektywach, zwłaszcza w art. 27 dyrektywy o ochronie danych, który stanowi, że państwa członkowskie i Komisja zachęcają do opracowywania kodeksów postępowania, których celem będzie usprawnienie procesu prawidłowego wdrażania niniejszej dyrektywy. Ponadto instrumenty samoregulacyjne mogłyby skutecznie przyczyniać się do wdrażania środków bezpieczeństwa, o których mowa w art. 17 dyrektywy o ochronie danych oraz w art. 14 dyrektywy o prywatności i łączności elektronicznej.

([1]) W pkt 59 niniejszej opinii zostanie omówione znaczenie trzeciej dyrektywy, tj. dyrektywy Parlamentu Europejskiego i Rady 1999/5/WE z dnia 9 marca 1999 r. w sprawie urządzeń radiowych i końcowych urządzeń telekomunikacyjnych oraz wzajemnego uznawania ich zgodności (Dz.U. L 91 z 7.4.1999, str. 10).

([2]) Zob. m.in. s. 10 opinii przywołanej w przypisie 5.

Pełne wdrożenie istniejących ram

34. W opinii na temat komunikatu w sprawie dyrektywy o ochronie danych wymieniono szereg narzędzi, które umożliwiają lepsze wdrożenie tej dyrektywy. Większość narzędzi niewiążących, o których mowa w tej opinii, dotyczy również RFID — są wśród nich komunikaty wyjaśniające lub inne, propagowanie wzorców postępowania, stosowanie etykiet dotyczących ochrony prywatności lub przeprowadzanych przez strony trzecie kontroli zachowywania prywatności. Możliwość przyjęcia szczegółowych zasad dotyczących RFID zostanie omówiona w rozdziale V. Wprowadzenie poprawek jest jednak możliwe również przy obecnych ramach.

Instrumenty samoregulacyjne

35. EIOD zgadza się z Komisją, że w pierwszej fazie lepiej jest zostawić miejsce dla samoregulacji, pozwalając stronom zainteresowanym szybko stworzyć warunki zgodne z prawem, a w ten sposób przyczynić się do stworzenia bezpieczniejszego otoczenia prawnego.

36. Oczekuje się, że Komisja w porozumieniu z grupą ds. RFID skupiającą strony zainteresowane będzie stymulowała proces samoregulacji i sterowała nim. W tym kontekście EIOD z zadowoleniem przyjmuje zapowiedziane w komunikacie wydanie zalecenia, które określi „zasady wykorzystania identyfikacji radiowej, którymi powinny kierować się organy publiczne i pozostałe zainteresowane podmioty".

37. W komunikacie przewiduje się, że samoregulacja przyjmie formę kodeksu postępowania lub kodeksu dobrych praktyk. Zdaniem EIOD, niezależnie od tego, jaką formę przyjmie samoregulacja, powinna ona:

— dawać konkretne i praktyczne wskazówki na temat poszczególnych rodzajów zastosowań RFID, a co za tym idzie przyczyniać się do zgodności z ramami prawnymi w zakresie ochrony danych,

— rozwiązywać szczegółowe kwestie i problemy, które pojawiają się w kontekście ogólnych zastosowań RFID,

— przyczyniać się do jednolitego i harmonijnego stosowania dyrektywy o ochronie danych w całej UE, a dokładniej w tej branży, która najprawdopodobniej będzie stosowała ten sam rodzaj aplikacji RFID w całej UE,

— być stosowana przez wszystkie zainteresowane strony. Niespełnianie jej wymogów powinno mieć negatywne (najlepiej finansowe) skutki.

38. EIOD zwraca uwagę na jedno zagadnienie, w którym samoregulacja będzie szczególnie przydatna. W przypadku zastosowań RFID, które zakładają przetwarzanie danych osobowych, dyrektywa o ochronie danych nakłada na administratorów danych różne zobowiązania, wynikające w szczególności z art. 17 (bezpieczeństwo przetwarzania) i z art. 7 (konieczność przetwarzania danych jedynie wówczas, gdy istnieją odpowiednie podstawy prawne). Zgodnie z tymi przepisami administratorzy danych muszą z jednej strony ustanowić środki zapobiegające nieuprawnionemu ujawnianiu danych. Z drugiej strony administratorzy danych muszą zadbać o to, by przetwarzanie, takie jak ujawnienie informacji dzięki czytnikom — w odpowiednich przypadkach — odbywało się jedynie po uzyskaniu świadomej zgody osoby, której te dane dotyczą.

39. Można interpretować, że te przepisy dyrektywy o ochronie danych wymagają, aby aplikacje RFID były stosowane przy zapewnieniu koniecznych rozwiązań technicznych, które będą zapobiegały lub minimalizowały ryzyko niechcianego ujawnienia danych i w odpowiednich przypadkach gwarantowały przetwarzanie danych lub dokonywanie ich transferu jedynie po uzyskaniu świadomej zgody. Zdaniem EIOD takie zobowiązanie (tj. stosowanie koniecznych rozwiązań technicznych, które będą zapobiegały lub minimalizowały ryzyko niechcianego ujawnienia danych) i jego wiążącego charakteru dla stosujących RFID będą jeszcze bardziej zdecydowane i jasne, jeśli wymóg ten zostanie zawarty w kodeksie postępowania lub kodeksie dobrych praktyk wspomnianych powyżej. Z tych powodów EIOD zdecydowanie radzi, aby zalecenie Komisji zawierało taką interpretację dyrektywy o ochronie danych, podkreślając istnienie obowiązku rozmieszczania aplikacji RFID z zastosowaniem koniecznych rozwiązań technicznych, które będą zapobiegały niechcianemu gromadzeniu lub ujawnianiu informacji.

Potrzeba wskazówek

40. EIOD zaleca, aby Komisja w ścisłej współpracy z grupą ekspertów ds. RFID przygotowała jeden lub kilka dokumentów zawierających jasne wskazówki na temat stosowania obecnych ram prawnych do otoczenia RFID. We wskazówkach tych należy uwzględnić praktyczne sposoby przestrzegania zasad określonych w dyrektywie o ochronie danych i w dyrektywie o prywatności i łączności elektronicznej. Jeśli chodzi o ogólne podejście do tych wskazówek i ich konkretną treść, EIOD ma następujące sugestie.

41. Wskazówki ustalające zasady, które będą obowiązywały w odniesieniu do stosowania RFID powinny być wystarczająco zwięzłe i koncentrować się na konkretnych sektorach. Podejście uniwersalne nie spełni stawianego celu, który polega na zapewnieniu jasnych i spójnych ram. Zamiast tego zakres tych wskazówek musi się ograniczać do dobrze zdefiniowanych zastosowań RFID w określonych dziedzinach.

42. Ponadto w wytycznych tych należy zaproponować praktyczne i skuteczne metody opracowywania „technik i standardów", które mogłyby się przyczynić do zapewnienia zgodności systemów RFID z ramami prawnymi dotyczącymi ochrony danych i które będą wiązały się z wykorzystaniem technologii zakładającej poszanowanie prywatności od samego początku.

43. Stosując obecne ramy prawne do otoczenia RFID, należy zwrócić szczególną uwagę na przestrzeganie zasad ochrony danych i związanych z nimi obowiązków, które dotyczą administratorów danych aplikacji RFID. Najbardziej istotne są następujące obowiązki i zasady:

— zasada prawa do informacji, w tym prawa do informacji o tym, kiedy dane są gromadzone przez czytniki, a także — w odpowiednich przypadkach — że produkty są wyposażone w tagi,

— zasada udzielenia zgody, jako jedna z podstaw prawnych do przetwarzania danych. Zasada ta polega na obowiązku dezaktywacji tagów RFID w punkcie sprzedaży, chyba że podmiot danych wyraził swoją zgodę ([1]). Prawo do dezaktywacji tagów RFID służy również zapewnieniu bezpieczeństwa informacji, tj. dopilnowaniu, by dane przetwarzane dzięki tagom RFID nie zostały ujawnione niepożądanym stronom trzecim,

— prawo jednostek do tego, by nie podlegać niekorzystnym decyzjom opartym wyłącznie na automatycznym przetwarzaniu określonego profilu osoby.

44. Jeśli chodzi o prawo do informacji, we wskazówkach powinno się określić, że jednostkom należy udzielać informacji dotyczących przetwarzania ich danych osobowych. W szczególności należy zwrócić uwagę jednostek na (i) obecność czytników, a na produktach lub ich opakowaniu obecność aktywnych tagów RFID; (ii) skutki ich obecności w kontekście gromadzenia informacji oraz (iii) cele, do jakich gromadzone informacje mają zostać wykorzystane.

45. Odpowiednim sposobem dostarczania informacji może być logo. Logo można wykorzystać do zwrócenia uwagi na obecność czytników i tagów RFID, które mają pozostać aktywne. Jednak wykorzystanie samego logo nie wystarczy do zagwarantowania sprawiedliwego przetwarzania informacji wymagającego, by informacje przekazywane podmiotom danych były jasne i podane w zrozumiały sposób. Wykorzystanie logo należy uznać za sposób uzupełniający udzielanie bardziej szczegółowych informacji.

([1]) Zob. szczegółowe omówienie pkt 46–50 niniejszej opinii.

Podstawa: zasada wyrażenia zgody (ang. opt-in)

46. W przypadku wszystkich istotnych zastosowań RFID rozwiązania powinny przestrzegać zasady wyrażenia zgody w punkcie sprzedaży i realizować ją jako warunek konieczny. Zezwolenie na to, by tagi RFID dalej transmitowały informacje po opuszczeniu przez nie punktu sprzedaży byłoby niezgodne z prawem, o ile administrator danych nie miałby odpowiednich podstaw prawnych. Odpowiednimi podstawami prawnymi zwykle byłyby jedynie a) zgoda podmiotu danych lub b) jeśli takie ujawnienie jest konieczne do wykonania usługi — specjalna i dobrowolna prośba danej jednostki ([1]). Oba rodzaje podstaw prawnych byłyby wtedy formą wyrażenia zgody.

47. Zgodnie z zasadą wyrażenia zgody tagi powinny ulec dezaktywacji w punkcie sprzedaży, chyba że osoba, która kupiła produkt wyposażony w tag, będzie chciała, aby pozostał on aktywny. Korzystając z prawa do pozostawienia aktywnego taga, osoba ta zgadzałaby się na dalsze przetwarzanie swoich danych, na przykład na przesłanie danych do czytnika przy następnej wizycie u administratora danych.

48. Aby uporać się z rosnącą różnorodnością zastosowań RFID i ułatwić rozwój nowych innowacyjnych modeli biznesowych, EIOD podkreśla wagę, jaką ma elastyczne podejście. Elastyczność należy zastosować również w odniesieniu do wprowadzenia zasady wyrażenia zgody.

49. Jest bardzo dużo opcji wprowadzenia zasady wyrażenia zgody. Alternatywą dla usunięcia taga mogłoby być jego zablokowanie, czasowe wyłączenie lub — zgodnie z modelem zabezpieczeń zainspirowanym biologicznym mechanizmem wdrukowania (ang. *resurrecting duckling model*) ([2]) — przypisanie go tylko do jednego użytkownika. W przypadku taga o krótkim cyklu życia adres taga, który łączy go z informacjami przechowywanymi w bazie danych, mógłby zostać wykasowany z referencyjnej bazy danych, dzięki czemu można byłoby uniknąć przetwarzania przez ten tag dodatkowych danych.

50. Podsumowując, chociaż EIOD uważa, że zasada wyrażenia zgody w punkcie sprzedaży jest zobowiązaniem prawnym, które w większości przypadków wynika z dyrektywy o ochronie danych, istnieją powody, aby wyszczególnić to zobowiązanie w instrumentach samoregulacyjnych, również w celu zapewnienia stosowania tej zasady w najodpowiedniejszy sposób. W każdym razie specjalne wdrożenie jest potrzebne dla tych zastosowań RFID, które nie mieszczą się w zakresie stosowania dyrektywy o ochronie danych.

([1]) W niektórych zastosowaniach RFID można będzie się oprzeć na innych podstawach, takich jak art. 7 lit. f) (uzasadnione interesy administratora danych, przy zachowaniu odpowiednich środków bezpieczeństwa).

([2]) Nazwa tego modelu, który został opracowany przez Franka Stajano i Rossa Andersona z Uniwersytetu w Cambridge, została zainspirowana obserwacją „jak pisklę zakłada, że pierwszy poruszający się obiekt, który zobaczyło po wykluciu, musi być jego matką".

Potrzeba „poszanowania prywatności od samego początku"

51. Aby zminimalizować zagrożenia dla ochrony danych i prywatności, komunikat Komisji wprowadza w części 3.2, str. 6, pomysł wyszczególnienia i przyjęcia kryteriów na wczesnym etapie projektu. EIOD z zadowoleniem przyjmuje to podejście. W istocie przyjęcie kryteriów specyfikacji i projektu, zwanych inaczej najlepszą dostępną technologią (ang. *Best Available Technique* — BAT), skutecznie przyczyni się do uregulowania ochrony danych i wymagań związanych z bezpieczeństwem. Takie wyznaczenie kryteriów technologicznych i organizacyjnych — jeśli będzie często weryfikowane — wzmocni model symbiozy wymagań dotyczących prywatności i bezpieczeństwa, które opracowuje Unia Europejska.

52. Właściwe zdefiniowanie najlepszych dostępnych technologii w zakresie prywatności i bezpieczeństwa systemów RFID będzie również kluczowe dla budowania wiarygodnego otoczenia, które wzmocni ich powszechną akceptację wśród użytkowników, jak również dla konkurencyjności przemysłu europejskiego.

53. Proces selekcji najlepszych dostępnych technologii dla systemów RFID powinien być napędzany ocenami wpływu z dziedziny prywatności i bezpieczeństwa, których przeprowadzenie nadal wymaga pewnego wysiłku. EIOD uważa, że Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) razem ze wspólnymi ośrodkami badawczymi Komisji Europejskiej w porozumieniu ze stronami zainteresowanymi w danej branży mogą przyczynić się do zidentyfikowania tych najlepszych praktyk i do rozwoju takich metodologii. Rozpoczynając niedawno projekt dotyczący wytycznych technicznych w zakresie RFID niemiecki Urząd Federalny ds. Bezpieczeństwa Informacji (BSI) podał właściwy przykład ([3]) ilustrujący najlepsze dostępne technologie, które teraz powinny zostać rozwinięte na poziomie europejskim.

54. W szybkim przyjęciu zasady poszanowania prywatności od samego początku znaczącą rolę mogą odegrać również normy. Komisja powinna zatem brać udział w przyjęciu środków służących ochronie prywatności i danych przy opracowywaniu międzynarodowych norm dotyczących RFID. Grupa Robocza ds. Ochrony Danych powołana na mocy art. 29 w swoim dokumencie roboczym ([4]) w sprawie RFID jasno zobrazowała, w jaki sposób normy mogą przyczynić się do opracowania systemów RFID, które będą korzystne dla ochrony prywatności.

([3]) http://www.bsi.bund.de/veranst/rfid/index.htm

([4]) Dokument roboczy (WP 105) w sprawie zagadnień dotyczących technologii RFID, 19 stycznia 2005 r.

55. Ponadto EIOD z zadowoleniem przyjmuje stanowisko zajęte przez Komisję wobec badań i rozwoju technologii RFID oraz potrzebę złagodzenia zagrożeń dla prywatności. W istocie zasada poszanowania prywatności od samego początku powinna zostać wprowadzona na najwcześniejszym etapie rozwoju technologii, co w większym stopniu przyczyni się do ich zgodności z ramami prawnymi dotyczącymi ochrony danych. Jak przedstawiono krótko w sprawozdaniu za 2006 rok, EIOD włączy się w te wysiłki, udzielając — w zależności od przypadku — porad i wydając opinie na temat projektów 7. programu ramowego (2007–2013).

V. **CZY SĄ POTRZEBNE SPECJALNE ŚRODKI LEGISLACYJNE?**

56. Samoregulacja może nie być wystarczającym środkiem do pełnego wdrożenia istniejących ram ochrony danych i prywatności. Nawet jeśli samoregulacja spełni wspomniane wcześniej wymagania, jej stosowanie jest dobrowolne, a nałożenie sankcji za jej zaniechanie nie zawsze może być skuteczne. Ponadto, nadal mogą być potrzebne wiążące środki prawne, aby zagwarantować ochronę prawa do ochrony danych i prywatności jednostkom. Jest to potrzebne na wypadek niepowodzenia podejścia przewidującego samoregulację.

57. Kluczowym zagadnieniem jest określenie instrumentów koniecznych do zagwarantowania, że aplikacje RFID są skutecznie stosowane wraz z koniecznymi rozwiązaniami technicznymi, które mają zapobiegać zagrożeniom dla ochrony danych i prywatności lub je minimalizować, i że odpowiedzialni administratorzy danych podejmują odpowiednie działania, aby wypełnić swoje zobowiązania zgodnie z obowiązującymi ramami prawnymi. Stąd wynika kilka dodatkowych pytań:

— czy są niezbędne specjalne zasady?

— jeśli tak, czy można je przyjąć na podstawie istniejących ram prawnych, na przykład korzystając z istniejących procedur komitetowych?

— lub czy konieczny jest nowy instrument prawny, gwarantujący skuteczne stosowanie rozwiązań RFID, które będą miały wbudowaną technologię chroniącą prywatność.

58. W obecnym rozdziale omówione zostaną możliwości wydania na podstawie istniejących ram prawnych wiążących środków legislacyjnych, natomiast w rozdziale VI zostanie omówiona — jako odrębne zagadnienie — konieczność wprowadzenia nowego instrumentu prawnego.

59. Po pierwsze, należy zwrócić szczególną uwagę na przepisy art. 17 dyrektywy 95/46/WE, art. 14 ust. 3 dyrektywy 2002/58/WE oraz art. 3 ust. 3 lit. c) dyrektywy 1999/5/WE. Art. 14 ust. 3 pozwala państwom członkowskim przyjmować środki w celu zadbania, by terminal został skonstruowany w sposób zgodny z prawem użytkowników do ochrony i kontroli wykorzystywania ich danych osobowych, zgodnie z dyrektywą 1999/5/WE ([1]). Art. 3 ust. 3 lit. c) dyrektywy 1999/5/WE stanowi, że Komisja może zdecydować — przy zastosowaniu procedury komitetowej — że aparatura należąca do niektórych klas sprzętu lub aparatura określonego typu ma być tak skonstruowana, aby miała wbudowane systemy zabezpieczające w celu zapewnienia ochrony danych osobowych i prywatności użytkownika lub subskrybenta. Dotychczas nie stosowano art. 3 ust. 3 lit. c) dyrektywy 1999/5/WE.

60. Przepisy te dają prawodawcy — na szczeblu krajowym i wspólnotowym — umocowanie do wprowadzenia wymogu, aby środki służące ochronie danych i prywatności były obowiązkowo uwzględniane przy produkcji systemów RFID; koncepcja ta jest znana jako „poszanowanie prywatności od samego początku" ([2]). Zachęcają również do stosowania najlepszych dostępnych technik.

61. Aby stosowanie koncepcji „poszanowania prywatności od samego początku" stało się obowiązkowe, EIOD zaleca, aby Komisja skorzystała z mechanizmu, o którym mowa w art. 3 ust. 3 lit. c) dyrektywy 1999/5/WE w porozumieniu z Grupą Ekspertów ds. RFID.

62. Po drugie, możliwe jest określenie, że istniejące ramy prawne mają być stosowane również do RFID przez wprowadzenie zmian do samych dyrektyw. Jak stwierdzono, Komisja właśnie przedstawiła wniosek w sprawie zmiany dyrektywy o prywatności i łączności elektronicznej, który zawiera nowy przepis dotyczący tej kwestii. EIOD z zadowoleniem przyjmuje ten pierwszy sygnał potwierdzający, że dyrektywa ta ma zastosowanie również do rozwiązań RFID. EIOD zajmie się szczegółowymi kwestiami wynikającymi ze związku między dyrektywą o prywatności i łączności elektronicznej w swojej opinii na temat wniosku w sprawie zmian, która zostanie wydana na początku roku 2008.

63. Biorąc pod uwagę fakt, że w najbliższym czasie ([3]) Komisja nie przewiduje żadnych zmian w dyrektywie o ochronie danych, możliwości wyjaśnienia, że obecne ramy prawne dotyczą również RFID, są ograniczone.

VI. **CZY POTRZEBNE SĄ SZCZEGÓŁOWE RAMY PRAWNE DOTYCZĄCE RFID?**

Plany Komisji

64. W komunikacie ([4]) podkreśla się znaczenie, jakie ma bezpieczeństwo i poszanowanie prywatności od samego początku. Wymaga się również zaangażowania wszystkich zainteresowanych stron. Głównym wynikiem działań Komisji będzie „zalecenie, w którym określi zasady

([1]) Oraz zgodnie z decyzją Rady 87/95/EWG z dnia 22 grudnia 1986 r. w sprawie normalizacji w dziedzinie technologii informatycznych i telekomunikacji (Dz.U. L 36 z 7.2.1987, str. 31).
([2]) Zob. rozdział IV.
([3]) EIOD popiera to podejście, zob. pkt 64.
([4]) Zob. pkt 4.1 komunikatu.

wykorzystania identyfikacji radiowej, którymi powinny kierować się organy publiczne i pozostałe zainteresowane podmioty". Zalecenie zostanie prawdopodobnie przyjęte wiosną 2008 roku. Plany legislacyjne, o których mowa w komunikacie, składają się z dwóch etapów. Komisja zamierza:

— rozważyć odpowiednie przepisy dotyczące RFID w planowanym wniosku w sprawie zmiany dyrektywy o prywatności i łączności elektronicznej. Jak już wspomniano, Komisja zaproponowała taką zmianę dyrektywy o prywatności i łączności elektronicznej w listopadzie 2007 roku, potwierdzając, że dyrektywa ta ma zastosowanie do rozwiązań RFID ([1]), ale nie proponując rozszerzenia zakresu stosowania dyrektywy o prywatności i łączności elektronicznej na sieci prywatne,

— ocenić potrzebę dalszych kroków legislacyjnych, które mają zagwarantować ochronę danych i prywatności.

65. Zgodnie z tą strategią należy oczekiwać, że Komisja nie planuje — przynajmniej nie w krótkim terminie — przedłożenia nowego szczegółowego prawa, które gwarantowałoby ochronę danych i prywatności w dziedzinie RFID.

Dane dla prawodawcy

66. W opinii na temat komunikatu w sprawie dyrektywy o ochronie danych EIOD wymienił kilka projektów działań legislacyjnych dotyczących przetwarzania danych osobowych, które można podsumować w następujący sposób:

— po pierwsze, należy zachować podstawowe zasady ochrony danych: „Nie ma konieczności ustalania nowych zasad, ale istnieje oczywista potrzeba wprowadzenia innych rozwiązań administracyjnych, z jednej strony skutecznych i właściwych dla społeczeństwa operującego w sieci, a z drugiej strony minimalizujących koszty administracyjne" ([2]),

— po drugie, wnioski legislacyjne należy składać wyłącznie wówczas, gdy dostatecznie dowiedziono konieczności i proporcjonalności nowego uregulowania. Z tego powodu w krótkim terminie nie należy zmieniać ogólnych ram legislacyjnych dotyczących ochrony danych,

— po trzecie, zmiany zachodzące w społeczeństwie mogą doprowadzić do konieczności stworzenia szczegółowych ram prawnych, aby dostosować zasady dyrektywy o ochronie danych do kwestii powstających w związku z określonymi technologiami, takim jak RFID. Jasne jest, że również w tym kontekście spełnione muszą zostać warunki związane z koniecznością i proporcjonalnością.

67. Jako następny krok warto wymienić oczekiwania, przed jakimi staje prawodawca w dziedzinie RFID:

— prawodawstwo musi być elastyczne i zostawiać miejsce na innowacje i postęp technologiczny. Powinno to prowadzić do tworzenia prawodawstwa, które będzie w wystarczającym stopniu neutralne wobec technologii,

— po drugie, prawodawstwo musi dawać pewność prawną. Powinno to prowadzić do tworzenia prawodawstwa, które będzie w wystarczającym stopniu szczegółowe. Strony zainteresowane muszą dokładnie wiedzieć, w jaki sposób jest regulowane ich postępowanie,

— po trzecie, prawodawstwo musi skutecznie chronić wszystkie uzasadnione interesy, których dotyczy. Wymaga to w każdym wypadku egzekwowania prawa i jasnego zdefiniowania odpowiedzialności; za jakie zachowania odpowiedzialne są poszczególne strony? ([3]) wymagania te mają jeszcze większe znaczenie, w przypadkach gdy zagrożona jest ochrona danych i prywatności, prawa podstawowe jednostki wynikające z europejskiej Konwencji praw człowieka i praw podstawowych oraz Karty praw podstawowych Unii Europejskiej.

Stanowisko EIOD

68. W opinii EIOD jest jasne, że nie wszystkie osiągnięcia technologiczne powinny pociągać za sobą reakcję prawodawcy europejskiego. Postęp technologiczny następuje bardzo szybko, natomiast przyjmowanie i wprowadzanie w życie prawodawstwa jest i powinno być procesem długotrwałym. Prawodawstwo powinno być wynikiem uzyskania równowagi wśród wszystkich interesów, których dotyczy. Kiedy wybranym instrumentem jest dyrektywa, potrzeba nawet jeszcze więcej czasu, ponieważ dyrektywy muszą zostać w pełni wprowadzone do systemów prawnych państw członkowskich.

69. Jednak RFID nie jest tylko jeszcze jednym rozwiązaniem technologicznym, jak to już podkreślono kilkukrotnie w niniejszej opinii. Komunikat odnosi się do RFID jako do początku nowego etapu rozwoju społeczeństwa informacyjnego, który często jest zwany „internetem rzeczy" a tagi RFID będą stanowiły kluczowe elementy „otoczenia inteligentnego". Środowiska te są również ważnym etapem rozwoju tzw. „społeczeństwa kontrolowanego" (ang. *Surveillance Society*) ([4]). Na tej podstawie można uzasadnić działania prawodawcze w obszarze RFID. Technologia RFID może przynieść zmianę jakościową.

([1]) Zob. proponowany nowy art. 3 dyrektywy 2002/58/WE.
([2]) Pkt 24 opinii na temat komunikatu w sprawie dyrektywy o ochronie danych.
([3]) Ujmując to słowami z dziedziny ochrony danych zakłada to oznaczenie „administratora danych".
([4]) Przesłanie to zostało powtórzone w oświadczeniu europejskich organów ochrony danych przyjętym w Londynie 2 listopada 2006 r., które jest dostępne na stronie internetowej EIOD: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. Z tej perspektywy EIOD zaleca rozważenie przyjęcia (wniosku w sprawie) prawodawstwa wspólnotowego, które będzie regulowało główne zagadnienia stosowania RFID w odpowiednich sektorach, gdyby okazało się, że zawiedzie właściwe stosowanie istniejących ram prawnych. Taki środek prawodawczy po jego wejściu w życie należy uznać za *lex specialis* w odniesieniu do ogólnych ram ochrony danych.

71. Przyjęcie takiego instrumentu prawodawczego miałoby następujące zalety:

— instrument ten mógłby ustalić istotne parametry mechanizmów samoregulacji,

— perspektywa przyjęcia instrumentu prawodawczego mogłaby okazać się skuteczną zachętą dla zainteresowanych stron do wprowadzania mechanizmów samoregulacyjnych, które gwarantowałyby odpowiednią ochronę.

72. Aby działanie to miało bardziej praktyczny charakter, można poprosić Komisję o przygotowanie dokumentu konsultacyjnego w sprawie wad i zalet szczegółowego prawodawstwa oraz jego głównych elementów. Oczywiście, można poprosić strony zainteresowane o ich wkład w takie konsultacje. Można też włączyć w nie Grupę Roboczą ds. Ochrony Danych powołaną na mocy art. 29.

Możliwe sposoby

73. Interwencja prawodawcy mogłaby przyczynić się do stworzenia skrojonych na miarę ram prawnych, które będą się składały z szeregu narzędzi regulacyjnych, uzupełniających istniejące ramy prawne i nadających im większą szczegółowość. Takie skrojone na miarę ramy prawne powinny opierać się na znanych zasadach ochrony danych i powinny się skupiać na podziale odpowiedzialności oraz na skuteczności mechanizmów kontroli.

74. Szczególny powód, dla którego takie skrojone na miarę prawodawstwo może być potrzebne, jest związany z faktem, że nie wszystkie zastosowania RFID zakładają przetwarzanie danych osobowych. Innymi słowy, jeśli zastosowanie RFID nie zakłada przetwarzania danych osobowych, strony uczestniczące w procesie wytwarzania i sprzedawania produktów wyposażonych w RFID nie są prawnie zobowiązane do wprowadzania żadnych rozwiązań technologicznych, które zapobiegałyby podsłuchowi lub instalowaniu czytników bez odpowiedniego poinformowania jednostek. Jednak — jak dowiedziono — w przypadku takich zastosowań RFID również istnieją zagrożenia dla prywatności wynikające z możliwości nadzorowania jednostek, co wymaga takiego samego rodzaju zapewnienia prywatności. Właśnie tak może być w przypadku wyposażania w tagi produktów użytkowych zanim znajdą się one w punkcie sprzedaży. Podsumowując, zastosowania RFID zakładające przetwarzanie danych osobowych mogą mimo wszystko być zagrożeniem dla prywatności jednostek, przez to że dają możliwość ukrytego nadzoru i wykorzystywania informacji do niedopuszczalnych celów.

75. EIOD jest zdania, że należy unikać tych niekorzystnych skutków. Ponieważ obecne prawodawstwo częściowo — przynajmniej w przypadku zastosowań RFID, które nie zakładają przetwarzania danych osobowych — nie jest w stanie zapobiec takiemu zagrożeniu dla prywatności, a uwzględniając niedociągnięcia miękkich rozwiązań prawnych, wydaje się, że należy zastosować obowiązkowe środki prawodawcze, aby zagwarantować satysfakcjonujące wyniki.

76. Takie środki powinny w każdym przypadku:

— określać zasadę wyrażenia zgody w punkcie sprzedaży jako szczegółowy i bezdyskusyjny obowiązek prawny, również dla tych zastosowań RFID, które nie mieszczą się w zakresie stosowania dyrektywy o ochronie danych ([1]),

— zapewniać obowiązkowe stosowanie rozwiązań RFID, które mają odpowiednie parametry techniczne lub zakładają „poszanowanie prywatności od samego początku".

VII. **KWESTIA ZARZĄDZANIA**

77. Chociaż „transgraniczny z natury" charakter systemów RFID w komunikacie został uwzględniony tylko na rynku wewnętrznym, EIOD uważa, że wymiar ten należy analizować raczej na szczeblu międzynarodowym. W sklepach systemy RFID są już „transgraniczne", ponieważ aktywność taga nie musi skończyć się w punkcie sprzedaży. Jeśli możliwe jest przekazanie danych osobowych do państwa trzeciego technologie te również stają się „transgraniczne" na poziomie całego systemu RFID, ponieważ wytwórca produktu wyposażonego w tag, który jest częścią systemu RFID, ma siedzibę poza Unią Europejską ([2]).

78. W dłuższej perspektywie zarządzanie referencyjnymi bazami danych identyfikacyjnych RFID również ma krytyczne znaczenie dla właściwego egzekwowania europejskich ram prawnych w zakresie ochrony danych. EIOD wzywa do znalezienia rozwiązania, ponieważ nie do przyjęcia jest postępująca degeneracja tych ram.

79. EIOD przewiduje, że kwestia zarządzania RFID będzie stanowić jedno z głównych wyzwań wymagających znacznych inwestycji. Będzie trzeba znaleźć odpowiednie forum negocjacji, jak również najodpowiedniejszą infrastrukturę zarządzania, aby dopilnować, by prawa do ochrony danych były odpowiednio respektowane we wspomnianym wymiarze międzynarodowym.

([1]) W rozdziale IV omówiono, że zasada wyrażenia zgody w punkcie sprzedaży jest obowiązkiem prawnym, który istnieje już na mocy dyrektywy o ochronie danych.

([2]) Zobowiązaniami dotyczącymi przekazywania danych osobowych zajęto się w art. 25 i 26 dyrektywy o ochronie danych.

80. W tej perspektywie EIOD wzywa Komisję, aby zaprezentowała swoje poglądy na kwestię zarządzania, najlepiej w porozumieniu z grupą ds. RFID skupiającą strony zainteresowane.

VIII. **PODSUMOWANIE**

81. EIOD z zadowoleniem przyjmuje komunikat Komisji w sprawie RFID, ponieważ zajęto się w nim głównymi zagadnieniami wyłaniającymi się w kontekście rozpowszechniania technologii RFID, nie zaniedbując głównych kwestii związanych z ochroną danych i prywatności. Zgadza się z poglądem, że systemy RFID mogą odegrać kluczową rolę w rozwoju społeczeństwa informacyjnego określaną zwykle mianem „internetu rzeczy".

Wyjaśnienie skutków

82. Powszechne stosowanie technologii RFID jest zasadniczo nową kwestią i może mieć fundamentalny wpływ na nasze społeczeństwo oraz na ochronę praw podstawowych w tym społeczeństwie, takich jak ochrona danych i prywatności. Technologia RFID może przynieść zmianę jakościową.

83. Należy wymienić pięć podstawowych kwestii związanych z prywatnością i bezpieczeństwem:

— identyfikacja podmiotu danych,

— identyfikacja administratora(-ów) danych,

— malejące znaczenie tradycyjnego rozróżnienia między sferą osobistą a sferą publiczną,

— konsekwencje określonych rozmiarów i fizycznych właściwości tagów RFID,

— brak przejrzystości przetwarzania (danych),

Określenie skutków

84. Ogólne ramy prawne mające zastosowanie do ochrony danych określone w dyrektywie 95/46/WE dotyczą RFID w stopniu, w jakim dane przetwarzane przez systemy RFID pokrywają się z definicją danych osobowych.

85. Jeśli chodzi o dyrektywę o prywatności i łączności elektronicznej: wniosek Komisji z dnia 13 listopada 2007 r. w sprawie zmian do tej dyrektywy zawiera przepis, który ma sprecyzować, że dyrektywa ta w rzeczywistości dotyczy niektórych zastosowań RFID. Jednak niektóre inne zastosowania RFID mogą nie zostać objęte tą dyrektywą ze względu na jej ograniczenie do przetwarzania danych osobowych w związku ze świadczeniem dostępnych publicznie usług łączności elektronicznej w publicznych sieciach telekomunikacyjnych.

86. Ochrona danych osobowych może zostać uzupełniona szeregiem instrumentów samoregulacyjnych. Należy zostawić miejsce dla takiej samoregulacji, pod warunkiem że będzie ona:

— zapewniała konkretne i praktyczne wskazówki na temat poszczególnych rodzajów zastosowań RFID,

— rozwiązywała szczegółowe kwestie i problemy, które pojawiają się w kontekście ogólnych zastosowań RFID,

— przyczyniała się do jednolitego i harmonijnego stosowania dyrektywy o ochronie danych w całej UE,

— stosowana przez wszystkie zainteresowane strony.

87. EIOD zaleca, aby Komisja w ścisłej współpracy z grupą ekspertów ds. RFID przygotowała co najmniej jeden dokument zawierający jasne wskazówki na temat stosowania obecnych ram prawnych do otoczenia RFID.

88. Wskazówki ustalające zasady, które będą obowiązywały w odniesieniu do stosowania RFID powinny być wystarczająco zwięzłe i koncentrować się na konkretnych sektorach. Powinny one proponować praktyczne i skuteczne metody opracowania „technik i standardów", które mogłyby się przyczynić do zapewnienia zgodności systemów RFID z ramami prawnymi w zakresie ochrony danych i które będą obejmowały technologię zakładającą poszanowanie prywatności od samego początku.

89. EIOD z zadowoleniem przyjmuje podejście zastosowane w komunikacie Komisji, zgodnie z którym proponuje się wprowadzenie pomysłu wyszczególnienia i przyjęcia kryteriów na wczesnym etapie projektu.

90. Chociaż EIOD jest zdania, że zasada wyrażenia zgody w punkcie sprzedaży jest zobowiązaniem prawnym, które w większości przypadków wynika z dyrektywy o ochronie danych, zobowiązanie to należy wyszczególnić w instrumentach samoregulacyjnych.

Czy szczegółowe środki są niezbędne?

91. Aby stosowanie koncepcji „poszanowania prywatności od samego początku" stało się obowiązkowe, EIOD zaleca, aby Komisja skorzystała z mechanizmu, o którym mowa w art. 3 ust. 3 lit. c) dyrektywy 1999/5/WE w porozumieniu z grupą ekspertów ds. RFID.

92. EIOD zaleca rozważenie przyjęcia (wniosku w sprawie) prawodawstwa wspólnotowego, które będzie regulowało główne zagadnienia stosowania RFID w odpowiednich sektorach, gdyby okazało się, że zawiedzie właściwe stosowanie istniejących ram prawnych. Taki środek prawodawczy po jego wejściu w życie należy uznać za *lex specialis* w odniesieniu do ogólnych ram ochrony danych. Ten środek prawodawczy powinien rozwiązywać również obawy dotyczące ochrony danych i prywatności, które pojawiają się w związku z niektórymi zastosowaniami RFID, takimi jak na przykład wyposażanie w tagi produktów zanim znajdą się one w punkcie sprzedaży, i które niekoniecznie muszą obejmować przetwarzanie danych osobowych.

93. Komisja powinna przygotować dokument konsultacyjny w sprawie wad i zalet szczegółowego prawodawstwa oraz głównych elementów takiego prawodawstwa.

94. Interwencja prawodawcy mogłaby przyczynić się do stworzenia skrojonych na miarę ram prawnych, które będą się składały z szeregu narzędzi regulacyjnych, uzupełniających istniejące ramy prawne i nadających im większą szczegółowość. Takie środki powinny w każdym przypadku:

— określać zasadę wyrażenia zgody w punkcie sprzedaży jako szczegółowy i bezdyskusyjny obowiązek prawny, również dla tych zastosowań RFID, które nie mieszczą się w zakresie stosowania dyrektywy o ochronie danych ([1]),

— zapewniać obowiązkowe stosowanie rozwiązań RFID, które mają odpowiednie parametry techniczne lub zakładają „poszanowanie prywatności od samego początku".

Kwestia zarządzania

95. EIOD wzywa Komisję, aby zaprezentowała swoje poglądy na kwestię zarządzania, najlepiej w porozumieniu z grupą ds. RFID skupiającą strony zainteresowane.

Sporządzono w Brukseli, 20 grudnia 2007 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych

([1]) W rozdziale IV omówiono, że zasada wyrażenia zgody w punkcie sprzedaży jest obowiązkiem prawnym, który istnieje już na mocy dyrektywy o ochronie danych.