Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie identyfikacji radiowej (RFID)

(2007/C 256/13)

W piśmie z dnia 26 lutego 2007 r. Komisja Europejska, działając na podstawie art. 262 Traktatu ustanawiającego Wspólnotę Europejską, zwróciła się do Europejskiego Komitetu Ekonomiczno-Społecznego o opracowanie opinii w sprawie *identyfikacji radiowej (RFID)*.

Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego, której powierzono przygotowanie prac Komitetu w tej sprawie, przyjęła swoją opinię 19 czerwca 2007 r. Sprawozdawcą był Peter MORGAN.

Na 437. sesji plenarnej w dniach 11 i 12 lipca 2007 r. (posiedzenie z dnia 11 lipca) Europejski Komitet Ekonomiczno-Społeczny stosunkiem głosów 138 do 1 — 6 osób wstrzymało się od głosu — przyjął następującą opinię:

1. **Wnioski i zalecenia**

1.1 Identyfikacja radiowa (RFID) jest istotną technologią, która z czasem zyska bardzo na znaczeniu. Dzięki jej obecnym i przyszłym zastosowaniom możliwe będzie ulepszenie szerokiego wachlarza procesów biznesowych zarówno w sektorze publicznym, jak i prywatnym, oraz osiągnięcie znacznych korzyści przez osoby fizyczne oraz przedsiębiorstwa. Identyfikacja radiowa ma również potencjał stymulowania rozwoju aplikacji internetowych na ogromną skalę, dzięki czemu możliwa będzie realizacja koncepcji określanej przez jedną z agend ONZ jako „internet fizycznych przedmiotów". Jednak bez niezwykle skrupulatnej kontroli, identyfikacja radiowa może również prowadzić do naruszenia prywatności indywidualnych osób, niszczenia swobód obywatelskich oraz zagrożenia bezpieczeństwa osób fizycznych i przedsiębiorstw.

1.2 Pełen tytuł komunikatu Komisji brzmi: „Identyfikacja radiowa (RFID) w Europie: w stronę ram polityki". Komisja przeprowadziła już szerokie konsultacje, których wyniki stanowiły podstawę do opracowania komunikatu. Obecnie zwrócono się do EKES-u z wnioskiem o przygotowanie opinii rozpoznawczej. W oparciu o odpowiedzi na wydany komunikat Komisja przedstawi na koniec roku zalecenie dla państw członkowskich. Wszelkie przepisy prawne, których przygotowanie zajęłoby więcej czasu, zostaną opracowane później. A zatem niniejsza opinia powinna się skupiać na treści wspomnianego zalecenia.

1.3 Pragnąc zapewnić sobie wsparcie w formułowaniu zaleceń, Komisja postanowiła utworzyć grupę ds. RFID z udziałem zainteresowanych stron, z którą będzie się konsultować. Komitet chętnie przedstawiłby niniejszą opinię wspomnianej grupie.

1.4 EKES wyraża poparcie dla działań proponowanych przez Komisję w dziedzinie częstotliwości radiowych, normalizacji, zdrowia, bezpieczeństwa oraz środowiska naturalnego. Pragniemy podkreślić, iż należy pilnie zadbać o to, aby przemysł wniósł rzeczywisty wkład w forum normalizacyjne.

1.5 Ponieważ Komisja ma zamiar wydać zalecenia dla państw członkowskich pod koniec tego roku, należy przypuszczać, że zaakceptuje ona infrastrukturę bezpieczeństwa danych i ochrony prywatności w stanie, w jakim znajduje się ona w chwili obecnej. W szczególności sugeruje to, że organy odpowiedzialne za ochronę danych istniejące już w każdym z państw członkowskich staną się organami właściwymi w stosunku do ochrony prywatności i danych w zakresie identyfikacji radiowej. Zagadnienia te są zasadniczym przedmiotem niniejszej opinii.

1.6 Zagrożenia prywatności i swobód obywatelskich wynikające z identyfikacji radiowej są ogromne:

— Identyfikatory RFID mogą być wbudowane w przedmioty i dokumenty bądź na nie naniesione bez wiedzy osoby, która je nabywa. Z uwagi na fakt, że fale radiowe swobodnie i bezgłośnie przenikają przez tkaniny, plastik i inne materiały, możliwe jest odczytywanie identyfikatorów RFID wszytych w odzież lub przymocowanych do wewnętrznych elementów portmonetek, toreb na zakupy, walizek itp.

— Elektroniczny kod produktu mógłby pozwolić na przypisanie jednoznacznego indywidualnego identyfikatora każdemu przedmiotowi na Ziemi. Zastosowanie indywidualnego numeru identyfikacyjnego może doprowadzić do stworzenia światowego systemu rejestracji przedmiotów, w którym każdy obiekt materialny zostałby zidentyfikowany i przyporządkowany swojemu nabywcy lub właścicielowi w punkcie sprzedaży czy punkcie przejęcia.

— Upowszechnienie identyfikacji radiowej wymaga stworzenia ogromnych baz danych zawierających dane pochodzące z jednoznacznych identyfikatorów. Informacje te mogłyby zostać powiązane z danymi osobowymi, szczególnie w miarę zwiększania się pojemności pamięci komputerowej i zdolności przetwarzania danych.

— Identyfikatory mogą być odczytywane, bez względu na przesłaniające je przedmioty, przez czytniki, które można w sposób niewidoczny zainstalować w niemal każdym środowisku, w jakim gromadzą się ludzie. Czytniki można wbudować w terakotę, wpleść w dywan, ukryć w wejściach do pomieszczeń czy w meblach, przez co osoba nie ma praktycznie możliwości zorientowania się, kiedy jej dane są skanowane.

— Gdy do danych osobowych przypisuje się jednoznaczny numer identyfikatora RFID, możliwe jest śledzenie lub rejestrowanie wzorców zachowań osób bez ich wiedzy i zgody.

— Nietrudno jest wyobrazić sobie świat, w którym czytniki RFID składają się na wszechobecną globalną sieć. Taka sieć nie wymagałaby jednak wszechobecnych czytników. Służby odpowiedzialne za pobieranie opłat za wjazd do Londynu są w stanie wyśledzić wszystkie pojazdy przekraczające granice centrum miasta dzięki stosunkowo małej liczbie strategicznie rozmieszczonych kamer. W ten sam sposób możliwe byłoby zbudowanie sieci strategicznie rozmieszczonych czytników RFID. Nie wolno jednak do tego dopuścić.

1.7 Zagrożenia te niosą ze sobą następujące skutki:

— Użytkownicy technologii identyfikacji radiowej muszą upubliczniać swoje strategie i praktyki; nie powinny istnieć żadne tajne bazy danych osobowych.

— Obywatele mają prawo wiedzieć, kiedy towary w sprzedaży detalicznej zawierają identyfikatory bądź czytniki RFID. O każdym przypadku odczytu identyfikatora, mającym miejsce w handlu detalicznym, powinny wiedzieć wszystkie strony.

— Użytkownicy technologii identyfikacji radiowej muszą powiadamiać o powodach stosowania identyfikatorów i czytników. Zbieranie informacji powinno być ograniczone do zaspokojenia bieżących celów.

— Użytkownicy technologii identyfikacji radiowej są odpowiedzialni za jej wdrożenie oraz działanie w granicach przepisów i wytycznych w zakresie bezpieczeństwa danych. Są oni również odpowiedzialni za bezpieczeństwo i prawidłowe działanie systemu oraz jego bazy danych.

1.8 Nie jest jeszcze pewne, w jaki sposób zasady te miałyby być realizowane w praktyce. Najlepiej byłoby, gdyby każde przedsiębiorstwo zajmujące się transakcjami z udziałem konsumentów, np. handlem detalicznym, etykietowaniem, kontrolą dostępu i usługami transportowymi, dawało klientom jakąś formę gwarancji ich przestrzegania, swego rodzaju kartę klienta. Na płaszczyźnie konceptualnej karta tego typu mogłaby obejmować wszystkie zasady dobrych praktyk dotyczące ochrony danych, o których mowa w pkt. 4.5. Ponadto EKES proponuje następujące wytyczne:

a) Należy zakazać kupcom zmuszania klientów do nabywania produktów zawierających aktywne lub uśpione identyfikatory bądź narzucania im takich produktów. Powinna istnieć między innymi możliwość dołączania identyfikatorów do opakowania, czy stosowania zdejmowanych identyfikatorów, na wzór metek na towarach.

b) Klienci powinni mieć możliwość usunięcia lub dezaktywacji wszelkich identyfikatorów umieszczonych na należących do nich przedmiotach.

c) Identyfikacji radiowej zasadniczo nie powinno się stosować do śledzenia osób. Śledzenie ludzi jest niewłaściwe, bez względu na to, czy ma to miejsce na przykład przy użyciu identyfikatorów umieszczonych na odzieży, towarach, biletach czy jakichkolwiek innych produktach.

d) Identyfikacja radiowa nie powinna być stosowana w sposób, który mógłby wykluczać lub ograniczać anonimowość.

e) Właściwe organy powinny wyraźnie wskazać, że zastosowania, o których mowa w punkcie c) i d), będą dopuszczalne jedynie w wyjątkowych okolicznościach i to po uprzednim formalnym powiadomieniu takiego organu.

1.9 Można rozważać pewne wyjątki od powyższych zasad w przypadku, gdy:

— dana osoba zdecyduje się skorzystać z możliwości utrzymania aktywności identyfikatora dla własnej wygody;

— dana osoba wyrazi swoją zgodę na śledzenie w miejscu o krytycznym znaczeniu, takim jak szczególnie ściśle chronione budynki oraz instytucje publiczne i prywatne;

— dana osoba zdecyduje się na korzystanie z zastosowań, które ją zlokalizują i zidentyfikują w taki sam sposób jak ma to już miejsce w momencie korzystania z telefonów komórkowych, kart bankomatowych, adresów internetowych itp.

Wszelkie tego rodzaju wyjątki powinny być zgłaszane właściwemu organowi.

1.10 Identyfikacja radiowa nie jest technologią dojrzałą, tak więc nie pojmujemy jeszcze jej pełnego potencjału. Z jednej strony może ona przynieść niewyobrażalne korzyści naszej cywilizacji technicznej, z drugiej jednak może być największym zagrożeniem technologicznym prywatności i wolności. Zdaniem EKES-u zastosowania RFID należy rozwijać, przestrzegając ściśle kodeksu etycznego w zakresie poszanowania prywatności, wolności i bezpieczeństwa danych. Niemniej należy kontynuować ów rozwój pod warunkiem zapewnienia niezbędnych zabezpieczeń.

1.11 Podsumowując, można stwierdzić, że w dziedzinach, w których dozwolone są zastosowania identyfikacji radiowej, ich wdrażanie powinno być w pełni przejrzyste dla wszystkich zainteresowanych stron. Zasadniczo dopuszczalne są zastosowania mające na celu poprawę obsługi towarów. Zastosowania umożliwiające identyfikację osób są zasadniczo niedopuszczalne, z wyjątkiem otoczenia, w którym osoby te znajdują się przejściowo. Zastosowania pozwalające na powiązanie osób z towarami mogą być dopuszczalne w celach marketingowych. Zastosowania identyfikujące osoby poprzez towary, które zakupiły, są generalnie niedopuszczalne. Ponadto niektóre zastosowania są nieodpowiednie w wolnym społeczeństwie i nie powinno się na nie zezwalać. Podstawowym zaleceniem ze strony Komisji dla państw członkowskich musi być bezwzględna potrzeba zachowania prywatności i anonimowości.

2. **Czym jest identyfikacja radiowa i dlaczego ma takie znaczenie?**

2.1 Identyfikacja radiowa (RFID) jest technologią umożliwiającą automatyczną identyfikację i odczyt danych dzięki zastosowaniu częstotliwości radiowych. Istotną cechą tej technologii jest fakt, że możliwe jest oznaczenie dowolnego obiektu, zwierzęcia czy nawet człowieka poprzez umieszczenie na nich — za pomocą elektronicznego identyfikatora — jednoznacznych danych identyfikujących lub innych informacji, a następnie odczytywanie ich za pomocą bezprzewodowego urządzenia.

2.2 Identyfikatory składają się z obwodu elektronicznego, w którym przechowywane są dane, oraz z anteny, dzięki której dane są przekazywane drogą radiową. Czytnik RFID komunikuje się z identyfikatorami w celu uzyskania zapisanych informacji. Kiedy czytnik emituje fale radiowe, łączy się ze wszystkimi identyfikatorami w zasięgu. Do kontroli czytnika oraz zbierania i filtrowania informacji wymagane jest odpowiednie oprogramowanie.

2.3 Dostępne są różne rodzaje systemów identyfikacji radiowej. Identyfikatory mogą być aktywne bądź pasywne. Identyfikatory aktywne zawierają wbudowaną baterię zasilającą zespół wewnętrznych obwodów i wytwarzającą fale radiowe, mogą nadawać nawet bez obecności czytnika RFID. Identyfikatory pasywne są zasilane energią fali radiowej przekazywanej przez czytnik, nie mają własnego źródła energii. Identyfikatory mogą mieć możliwość wyłącznie odczytu lub odczytu i zapisu. Identyfikatory służące wyłącznie do odczytu cechują się niższymi kosztami produkcji i wykorzystywane są w większości bieżących zastosowań.

2.4 Zasięg systemu identyfikacji radiowej jest zależny od częstotliwości radiowej, mocy czytnika oraz środowiska pomiędzy identyfikatorem a czytnikiem. W przypadku systemów pasywnych zasięg może wynosić do kilku metrów, natomiast dla systemów aktywnych przekracza 100 metrów.

2.5 W hierarchii technologii bezprzewodowych identyfikacja radiowa znajduje się na najniższym szczeblu. Pod względem odległości, jakie pokonuje sygnał, najwyższą pozycję mają systemy komunikacji satelitarnej, jak np. GPS. Następne miejsca zajmują technologie telefonii komórkowej o szerokim zasięgu, takie jak GSM i GPRS, dalej sygnały o mniejszym zasięgu obejmującym budynki, jak Wi-Fi, kolejno sieci osobiste, takie jak Bluetooth, a na końcu identyfikacja radiowa. Każda z wymienionych technologii jest nieciągła i niezależna, a więc nie występuje na przykład ryzyko, że systemy satelitarne będą odczytywać identyfikatory RFID. Niemniej jednak istnieje możliwość przekazu danych pomiędzy różnymi systemami poprzez urządzenia takie jak telefony komórkowe.

2.6 Poniżej wymieniono szereg przykładów potencjalnych korzyści, jakie niosą ze sobą zastosowania identyfikacji radiowej:

— dla osób indywidualnych może oznaczać bezpieczeństwo (np. żywności, opieki zdrowotnej, ochronę przed fałszerstwami), wygodę (krótsze kolejki przy kasach, ulepszona obsługa bagażu lotniczego, automatyczne płatności) oraz lepszą opiekę nad chorymi, zwłaszcza cierpiącymi na schorzenia przewlekłe, jak np. demencja;

— w transporcie identyfikacja radiowa ma zwiększyć wydajność, bezpieczeństwo i jakość usług, zarówno w odniesieniu do osób, jak i towarów;

— w dziedzinie ochrony zdrowia identyfikacja radiowa może przyczynić się do podniesienia jakości opieki nad pacjentem i jego bezpieczeństwa, a także wpłynąć na poprawę przestrzegania terapii i ulepszyć logistykę. Trwają prace nad sposobami umieszczania identyfikatorów RFID na poszczególnych tabletkach;

— w handlu detalicznym może pomóc w zmniejszeniu braków w zaopatrzeniu oraz ograniczeniu stanów magazynowych i kradzieży;

— w wielu branżach, w których powszechne jest zjawisko podrabiania, zastosowanie identyfikacji radiowej może pozwolić na identyfikację miejsca, gdzie nielegalne towary są wprowadzane do łańcucha dostaw;

— zastosowanie identyfikatorów RFID może również przyczynić się do poprawy skuteczności sortowania i recyklingu materiałów oraz części składowych produktów, przynosząc tym samym pozytywne skutki w dziedzinie gospodarki odpadami i zrównoważonego rozwoju.

2.7 Wiele aspektów związanych z wykorzystaniem identyfikacji radiowej ilustruje jej zastosowanie w cyklu wydawniczym. Już sama liczba drukowanych książek oznacza logistyczny koszmar dla wydawców, dystrybutorów, bibliotek i księgarń. Oprócz logistyki w łańcuchu dostaw, istnieje także potrzeba śledzenia książek już po ich trafieniu na półki, tak aby można je było odnaleźć i wymienić. Ponadto biblioteki muszą kontrolować cykl wypożyczania, podczas gdy nabywcy miewają trudności z odnalezieniem swoich książek. Identyfikatory RFID umieszczone na książkach są rozwiązaniem wszystkich wymienionych problemów. Analogicznie do kontroli wypożyczeń w bibliotekach przedstawiać się będą wszelkie inne zastosowania, w których przedmioty są wielokrotnie wykorzystywane lub wypożyczane.

2.8 Aby zilustrować charakter zagrożeń związanych z tą technologią, poniżej przedstawiono wyciąg z wniosku patentowego złożonego przez firmę IBM (20020615758) z listopada 2002 r. Wniosek dotyczy identyfikacji i śledzenia osób przy użyciu przedmiotów wyposażonych w identyfikatory RFID.

> „Metoda i system identyfikacji i śledzenia osób przy użyciu przedmiotów wyposażonych w identyfikatory RFID, które osoby te mają bezpośrednio przy sobie. Dane dotyczące historii zakupów każdego klienta sklepu detalicznego są zbierane w terminalach punktów sprzedaży i gromadzone w bazie danych transakcji. Gdy osoba mająca na sobie lub przy sobie przedmioty wyposażone w identyfikatory RFID wchodzi do sklepu bądź na inny wyznaczony obszar, zainstalowany na miejscu skaner RFID skanuje identyfikatory umieszczone na tej osobie i odczytuje z nich informacje. Tak uzyskane informacje są porównywane z danymi z transakcji zgromadzonymi w bazie danych transakcji według ustalonych algorytmów korelacji. Na podstawie wyników porównania można ustalić dokładną tożsamość tej osoby lub jej konkretną charakterystykę. Informacje te są wykorzystywane do monitorowania przemieszczania się tej osoby na terenie sklepu lub na innym obszarze".

Wniosek patentowy złożony przez American Express nr 20050038718 zawiera podobną treść.

2.9 Identyfikacja radiowa jest z pewnością czymś więcej niż tylko elektronicznym kodem kreskowym. Główne różnice zawarte w przytoczonym powyżej wyciągu z wniosku patentowego polegają na tym, że:

a) identyfikator zawiera nie tylko opis danego przedmiotu, lecz również jego unikalne dane identyfikujące, które mogą z kolei wskazać jego nabywcę;

b) identyfikator nie musi mieć tradycyjnej postaci mikroprocesora; obwody elektroniczne mogą być bezpośrednio nadrukowane na większość materiałów takich jak odzież;

c) identyfikator może pozostać aktywny po zakupie, a więc nadal możliwe jest wielokrotne odczytywanie zapisanych w nim danych;

d) czytniki identyfikatorów nie są umieszczone jedynie w punktach sprzedaży, lecz można je instalować wszędzie, nie tylko na terenie sklepu detalicznego;

e) porównywanie informacji z bazą danych wprowadza nowy wymiar w dziedzinie zbierania danych, ochrony prywatności i bezpieczeństwa danych.

2.10 Kwestia, czy identyfikator powinien pozostawać aktywny po przejściu przez kasę sklepową, podlega dyskusji. Z jednej strony sytuacja taka stanowi zagrożenie prywatności. Z drugiej natomiast może być z korzyścią dla nabywcy. Na przykład wykorzystanie czytników RFID w domu mogłoby dopomóc w zarządzaniu piwniczką na wino, zawartością lodówek, szaf czy biblioteczek. Jest zatem logiczne, iż wybór ten powinien należeć do danej osoby, jednak technologia i jej zastosowanie muszą oferować konsumentowi takowy wybór.

2.11 Identyfikacja radiowa ma znacznie więcej zastosowań niż tylko identyfikowanie produktów w handlu detalicznym. Technologie tę wykorzystano w kartach identyfikacyjnych używanych w EKES-ie. W londyńskim metrze karty RFID są szeroko stosowane do celów opłaty za przejazd i warunkowania wstępu. Karty kredytowe wkrótce wyposażane będą w obwód RFID umożliwiający dokonywanie drobnych transakcji bez potrzeby posługiwania się kodem PIN. Plakietki działające na zasadzie RFID wykorzystywane są w systemach opłat za autostrady i identyfikacji kierowców. Wstęp na wyciągi narciarskie w niektórych europejskich kurortach narciarskich kontrolowany jest przy pomocy plakietek RFID noszonych w kieszeni kombinezonu narciarskiego. Sprawozdawca niniejszej opinii codziennie korzysta z trzech kart i jednej plakietki RFID. Jego pies ma wszczepiony podskórny mikroprocesor identyfikacyjny w technologii RFID. Podobne mikroprocesory są coraz powszechniej stosowane na całym świecie do celów identyfikacji zwierząt, aby umożliwić identyfikowalność w łańcuchu żywnościowym. Stąd może dzielić nas tylko jeden krok od wszczepiania identyfikatorów — analogicznie jak obecnie w przypadku psów — przestępcom i problemowym pacjentom.

2.12 Identyfikatory w formie, w jakiej używane są w EKES-ie, są niegroźnym zastosowaniem technologii RFID. Identyfikacja tożsamości nabiera o wiele poważniejszego znaczenia w wypadku, gdy identyfikatory RFID stają się elementem odzieży roboczej lub munduru, tak aby można było bezustannie śledzić ruchy noszącej je osoby za pomocą skanerów rozmieszczonych w kluczowych punktach zakładu pracy. Niemniej należy przyznać, że w niektórych wypadkach może to być pożądane, np. dla celów bezpieczeństwa. W każdym razie śledzenie miejsca pobytu osoby, jeśli nie towarzyszą temu odpowiednie zabezpieczenia, stanowiłoby poważne naruszenie jej prywatności, które wymaga należytego uzasadnienia oraz bardzo skrupulatnej kontroli.

2.13 Osobliwą zapowiedź przyszłych zastosowań RFID podaje „The Economist": w klubie Baja Beach w Barcelonie biletem wstępu do sekcji VIP-ów dla stałych gości jest mikroprocesor wszczepiony podskórnie w rękę. Jest on nieco większy niż ziarenko ryżu i pokryty szklaną oraz silikonową otoczką; wykorzystuje się go do identyfikacji osób przy wejściu oraz płaceniu za drinki. Mikroprocesor jest wszczepiany przez pielęgniarkę w znieczuleniu miejscowym. Jest to w istocie identyfikator RFID.

3. **Streszczenie komunikatu**

3.1 Identyfikacja radiowa jest przedmiotem politycznego zainteresowania ze względu na fakt, że może stać się nowym motorem wzrostu i tworzenia miejsc pracy, wnosząc tym samym znaczący wkład do strategii lizbońskiej, o ile uda się pokonać bariery dla innowacji.

3.2 W 2006 r. Komisja przeprowadziła konsultacje publiczne dotyczące identyfikacji radiowej, podczas których wyrażono oczekiwania wobec tej technologii na podstawie doświadczeń użytkowników szybko przyjmujących nowinki techniczne, a także obawy społeczeństwa związane z zastosowaniami identyfikacji radiowej obejmującymi identyfikację i śledzenie przemieszczania się osób.

3.3 Dalszy rozwój i powszechne zastosowanie identyfikacji radiowej może jeszcze bardziej wzmocnić rolę technologii informacyjnych i komunikacyjnych w stymulowaniu innowacyjności i propagowaniu wzrostu gospodarczego.

3.4 Aby ta nowa technologia zyskała akceptację użytkowników, konieczne jest stworzenie jasnych i przewidywalnych ram polityczno-prawnych. Ze względu na transgraniczny z natury charakter technologii identyfikacji radiowej wspomniane ramy powinny zapewniać spójność w obrębie rynku wewnętrznego.

3.5 *Bezpieczeństwo, prywatność i etyka*

3.5.1 Istnieją poważne obawy, że ta wszechobecna i dająca ogromne możliwości technologia może nieść ze sobą zagrożenia prywatności. Technologia RFID może być wykorzystywana do gromadzenia informacji bezpośrednio lub pośrednio związanych ze zidentyfikowaną lub możliwą do zidentyfikowania osobą, a zatem uznawanych za dane osobowe. Identyfikatory RFID mogą przechowywać dane osobowe. Technologia identyfikacji radiowej może być wykorzystywana do śledzenia przemieszczania się osób lub do określania wzorców ich zachowań. Identyfikacja radiowa może sprzyjać powstawaniu nadużyć prowadzących do naruszania prywatności. Wyrażono obawy co do możliwości naruszania podstawowych wartości, prywatności i zwiększenia nadzoru, zwłaszcza w miejscu pracy, gdzie może to prowadzić do dyskryminacji, marginalizacji, prześladowania i ewentualnie utraty pracy.

3.5.2 Oczywiste jest, że identyfikacja radiowa musi być wykorzystywana w sposób akceptowany społecznie i politycznie, dopuszczalny etycznie i dozwolony prawem. Będzie ona mogła przynieść związane z nią liczne korzyści gospodarcze i społeczne pod warunkiem wprowadzenia skutecznych gwarancji ochrony danych i prywatności oraz związanych z tym aspektów etycznych, które stanowią sedno dyskusji na temat społecznej akceptacji technologii RFID.

3.5.3 Wspólnotowe ramy prawne dotyczące ochrony danych i prywatności w Europie zostały skonstruowane w sposób umożliwiający uwzględnianie innowacji. Ochrona danych osobowych jest przedmiotem ogólnej dyrektywy o ochronie danych ([1]), która ma zastosowanie do wszystkich rozwiązań technicznych, w tym do identyfikacji radiowej. Uzupełnienie ogólnej dyrektywy o ochronie danych stanowi dyrektywa o prywatności i łączności elektronicznej ([2]). Zgodnie z tymi dyrektywami władze publiczne w państwach członkowskich będą musiały dopilnować, aby zastosowania identyfikacji radiowej były wprowadzane zgodnie z przepisami o ochronie prywatności i danych osobowych. Może zatem wystąpić konieczność zapewnienia szczegółowych wytycznych dotyczących praktycznego wdrożenia zastosowań identyfikacji radiowej oraz konieczność opracowania odpowiednich kodeksów postępowania.

3.5.4 W kwestii bezpieczeństwa konieczne jest podjęcie przez branżę, państwa członkowskie i Komisję wspólnych starań na rzecz pogłębienia zrozumienia kwestii systemowych i związanych z nimi zagrożeń bezpieczeństwa, które mogą wystąpić w związku z wdrożeniem rozwiązań i systemów identyfikacji radiowej na skalę masową. Istotnym aspektem rozwiązywania powyższych problemów będzie określenie i przyjęcie kryteriów konstrukcyjnych eliminujących zagrożenia prywatności i bezpieczeństwa na poziomie nie tylko technicznym, lecz także organizacyjnym i procesów biznesowych. Przed dokonaniem wyboru systemu RFID i wdrożeniem zastosowania identyfikacji radiowej niezbędne jest zatem przeprowadzenie dokładnej analizy kosztów i korzyści związanych z konkretnymi zagrożeniami bezpieczeństwa i prywatności.

3.5.5 Pojawiają się jednak także obawy co do otwartości i neutralności baz danych, w których rejestrowane mają być jednoznaczne identyfikatory stanowiące centralny element systemu identyfikacji radiowej, a także co do przechowywania i przetwarzania zgromadzonych danych oraz ich wykorzystania przez osoby trzecie. Jest to istotny problem, ponieważ technologia RFID stanowić ma siłę napędową nowej fali rozwoju internetu, której następstwem będzie połączenie miliardów inteligentnych urządzeń i zaawansowanych technicznie czujników w ogólnoświatową sieć telekomunikacyjną. Ten nowy etap rozwoju internetu nazwano „internetem fizycznych przedmiotów".

3.5.6 System rejestracji i nadawania nazw obiektom w przyszłym „internecie fizycznych przedmiotów" powinien być zabezpieczony przed awarią lub niewłaściwym wykorzystaniem, które mogłyby spowodować chaos. Należy wyeliminować możliwość przejęcia go przez partykularne grupy interesu, które mogłyby wykorzystać takie bazy danych i systemy do własnych celów. Konieczne jest także spełnienie wymagań wszystkich zainteresowanych stron w zakresie bezpieczeństwa, etyki i prywatności; dotyczy to zarówno osób fizycznych, jak i podmiotów gospodarczych, których poufne informacje handlowe są przetwarzane w procesach biznesowych wykorzystujących identyfikację radiową.

3.5.7 Podczas projektowania systemu informacyjnego wykorzystującego identyfikację radiową należy uwzględnić wymagania zarówno podmiotów aktywnie uczestniczących w jego tworzeniu (np. przedsiębiorstw, organów publicznych, szpitali), jak i użytkowników, których ma on dotyczyć (obywateli, konsumentów, pacjentów, pracowników). Ponieważ użytkownicy zwykle nie uczestniczą w pracach na etapie projektu, Komisja wspierać będzie opracowanie zbioru wytycznych właściwych dla danego zastosowania (kodeksu postępowania, sprawdzonych rozwiązań) przez grupę ekspertów reprezentujących wszystkie strony. Do końca roku 2007 Komisja wyda zalecenie, w którym określi zasady wykorzystania identyfikacji radiowej, jakimi powinny kierować się organy publiczne i pozostałe zainteresowane podmioty.

3.5.8 Komisja rozważy również uwzględnienie odpowiednich przepisów w planowanym wniosku w sprawie zmiany dyrektywy o prywatności i łączności elektronicznej, a także — równolegle — uwzględni wyniki prac przyszłej grupy ds. RFID, grupy roboczej ds. art. 29 dotyczącego ochrony danych oraz innych inicjatyw, takich jak Europejska Grupa ds. Etyki w Nauce i Nowych Technologiach. Na tej podstawie Komisja oceni potrzebę podjęcia dalszych kroków legislacyjnych w celu zapewnienia ochrony danych i prywatności.

3.5.9 Komisja będzie nadal uważnie śledzić rozwój „internetu fizycznych przedmiotów", którego ważnym elementem ma być identyfikacja radiowa. Pod koniec roku 2008 Komisja opublikuje komunikat zawierający analizę charakteru i skutków tego procesu, ze szczególnym uwzględnieniem kwestii prywatności, zaufania i zarządzania. W komunikacie Komisja dokona oceny istniejących możliwości politycznych, w tym potrzeby podjęcia dalszych kroków legislacyjnych w celu zapewnienia ochrony danych i prywatności oraz realizacji innych celów polityki publicznej.

3.5.10 Uwagi dotyczące kwestii bezpieczeństwa, prywatności i etyki zostały przedstawione w punkcie 4 niniejszej opinii.

3.6 *Inne kwestie dotyczące polityki w zakresie identyfikacji radiowej*

3.6.1 Obok szerokiego obszaru zagadnień dotyczących bezpieczeństwa, prywatności i etyki, do innych kwestii politycznych związanych z identyfikacją radiową należy częstotliwość radiowa, normalizacja oraz kwestie związane ze zdrowiem, bezpieczeństwem i środowiskiem.

3.6.2 Istotne jest ujednolicenie warunków użytkowania częstotliwości, ułatwiające mobilność i pozwalające obniżyć koszty. Komisja przyjęła ostatnio decyzję (2006/804/WE) w sprawie częstotliwości dla urządzeń RFID w zakresie UHF. Uważa się, że przeznaczony zakres będzie wystarczający w perspektywie od trzech do dziesięciu lat, jednak gdyby wystąpiło zapotrzebowanie na przyznanie dodatkowych częstotliwości, Komisja podejmie odpowiednie działania, korzystając z uprawnień przyznanych jej na mocy decyzji o spektrum radiowym (676/2002/WE). EKES podziela to stanowisko.

3.6.3 Sprawne przyjmowanie nowych międzynarodowych norm ISO i harmonizacja norm regionalnych mają zasadnicze znaczenie dla szybkiego upowszechniania się usług. Właściwe europejskie organy normalizacyjne — CEN i ETSI — są w ten proces w pełni zaangażowane. Komisja wzywa te organy, aby we współpracy z przedstawicielami przedmiotowej branży czuwały nad tym, by opracowywane normy odpowiadały europejskim wymaganiom, w szczególności w zakresie ochrony

([1]) Dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych.
([2]) Dyrektywa 2002/58/WE dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej.

prywatności, bezpieczeństwa, praw własności intelektualnej i udzielania licencji. Ponieważ normy branżowe i chronione patenty często idą ze sobą w parze, EKES wzywa Komisję do zastosowania wszelkich dostępnych jej środków w celu skłonienia organów branżowych i normalizacyjnych do przyspieszenia działań, tak aby zapobiec sytuacji, w której europejskie zastosowania RFID staną się nadmiernie uzależnione od drogiej własności intelektualnej w posiadaniu osób zagranicznych.

3.6.4 W odniesieniu do ochrony środowiska naturalnego urządzenia RFID w pełni podlegają dyrektywie w sprawie zużytego sprzętu elektrotechnicznego i elektronicznego oraz dyrektywie w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym. W kwestii zdrowia pojawia się potencjalny problem pola elektromagnetycznego wytwarzanego przez urządzenia w systemach identyfikacji radiowej. Pola elektromagnetyczne związane z zastosowaniami identyfikacji radiowej posiadają generalnie małą moc, a więc narażenie pracowników i społeczeństwa na oddziaływanie takich pól elektromagnetycznych powinno być znacznie poniżej granic przewidzianych w obecnie obowiązujących normach. Jednak w kontekście ogólnego wzrostu zastosowań transmisji bezprzewodowej, Komisja będzie poddawać ramy prawne przeglądowi. EKES podziela to stanowisko.

4. **Uwagi**

4.1 Ponieważ Komisja ma zamiar wydać zalecenia dla państw członkowskich pod koniec tego roku, należy przypuszczać, że zaakceptuje ona infrastrukturę bezpieczeństwa danych i ochrony prywatności w stanie, w jakim znajduje się ona w chwili obecnej. W szczególności sugeruje to, że organy odpowiedzialne za ochronę danych istniejące już w każdym z państw członkowskich staną się organami właściwymi w stosunku do ochrony danych prywatności i danych w zakresie identyfikacji radiowej.

4.2 W swoim komunikacie Komisja stwierdza m.in., że utworzy nową grupę ds. RFID z udziałem zainteresowanych stron, z którą będzie się konsultować. EKES chciałby przedstawić niniejszą opinię wspomnianej grupie.

4.3 Zagrożenia prywatności i swobód obywatelskich wynikające z identyfikacji radiowej są ogromne:

a) Identyfikatory RFID mogą być wbudowane w przedmioty i dokumenty bądź na nie naniesione bez wiedzy osoby, która je nabywa. Z uwagi na fakt, że fale radiowe swobodnie i bezgłośnie przenikają przez tkaniny, plastik i inne materiały, możliwe jest odczytywanie identyfikatorów RFID wszytych w odzież lub przymocowanych do wewnętrznych elementów portmonetek, toreb na zakupy, walizek itp.

b) Elektroniczny kod produktu mógłby pozwolić na przypisanie jednoznacznego indywidualnego identyfikatora każdemu przedmiotowi na Ziemi. Zastosowanie indywidualnego numeru identyfikacyjnego może doprowadzić do stworzenia światowego systemu rejestracji przedmiotów, w którym każdy obiekt materialny zostałby zidentyfikowany i przyporządkowany swojemu nabywcy lub właścicielowi w punkcie sprzedaży czy punkcie przejęcia.

c) Upowszechnienie identyfikacji radiowej wymaga stworzenia ogromnych baz danych zawierających dane pochodzące z jednoznacznych identyfikatorów. Informacje te mogłyby zostać powiązane z danymi osobowymi, szczególnie w miarę zwiększania się pojemności pamięci komputerowej i zdolności przetwarzania danych.

d) Identyfikatory mogą być odczytywane, bez względu na przesłaniające je przedmioty, przez czytniki, które można w sposób niewidoczny zainstalować w niemal każdym środowisku, w jakim gromadzą się ludzie. Czytniki można wbudować w terakotę, wpleść w dywan, ukryć w wejściach do pomieszczeń czy w meblach, przez co osoba nie ma praktycznie możliwości zorientowania się, kiedy jej dane są skanowane.

e) Gdy do danych osobowych przypisuje się jednoznaczny numer identyfikatora RFID, możliwe jest śledzenie lub rejestrowanie wzorców zachowań osób bez ich wiedzy i zgody.

f) Nietrudno jest wyobrazić sobie świat, w którym czytniki RFID składają się na wszechobecną globalną sieć. Taka sieć nie wymagałaby jednak wszechobecnych czytników. Służby odpowiedzialne za pobieranie opłat za wjazd do Londynu są w stanie wyśledzić wszystkie pojazdy przekraczające granice centrum miasta dzięki stosunkowo małej liczbie strategicznie rozmieszczonych kamer. W ten sam sposób możliwe byłoby zbudowanie sieci strategicznie rozmieszczonych czytników RFID. Nie wolno jednak do tego dopuścić.

4.4 W siódmym programie ramowym na rzecz badań i rozwoju Komisja przedstawiła już wytyczne w zakresie etycznych zastosowań analizowanej technologii, jako że oddziałuje ona na bezpieczeństwo danych i ochronę prywatności („Przewodnik dla wnioskodawców" — projekty współpracy, s. 54) ([3]). Identyfikacja radiowa jest doskonałym przykładem zmieniającej się relacji pomiędzy technologią a prawem do prywatności w zakresie gromadzenia i udostępniania danych, czy też oczekiwaniami społeczeństwa w odniesieniu do takiej prywatności. Problemy dotyczące ochrony prywatności pojawiają się wszędzie tam, gdzie gromadzi się i przechowuje, w formie cyfrowej lub jakiejkolwiek innej, dane umożliwiające jednoznaczną identyfikację osoby lub osób. Niedostateczna kontrola udostępniania takowych danych bądź jej brak mogą rodzić obawy związane z prywatnością. Problem ochrony prywatności najczęściej dotyczy danych z dziedziny zdrowia, informacji pochodzących z rejestru karnego, danych finansowych, genetycznych i dotyczących miejsca pobytu. Z punktu widzenia identyfikacji radiowej kluczowym zagadnieniem jest miejsce pobytu.

4.5 W swoich wytycznych ([4]) w sprawie zapewniania ochrony danych i prywatności Komisja określiła osiem obowiązujących zasad dobrego postępowania. Zgodnie z nimi dane:

— muszą być przetwarzane w sposób uczciwy oraz zgodny z prawem;

— muszą być przetwarzane w określonych celach;

— muszą być adekwatne do celów, istotne w odniesieniu do danego zagadnienia i nie powinny poza nie wykraczać;

— muszą być dokładne;

— muszą być przechowywane tylko tak długo, jak długo to konieczne;

— muszą być przetwarzane z poszanowaniem praw osoby, której dotyczą;

— muszą być bezpieczne;

— nie mogą być przekazywane do krajów, w których nie ma odpowiedniej ochrony.

Wytyczne te odnoszą się w pełni do kwestii ochrony prywatności i bezpieczeństwa danych związanej z zastosowaniami RFID.

([3]) http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsCallPage&call_id=11.

([4]) Dyrektywa w sprawie ochrony danych 95/46/EC art. 6.

4.6 Zdaniem EKES-u podstawowe zasady należytego postępowania przedstawiają się następująco:

— Użytkownicy technologii identyfikacji radiowej muszą upubliczniać swoje strategie i praktyki; nie powinny istnieć żadne tajne bazy danych osobowych.

— Obywatele mają prawo wiedzieć, kiedy towary w sprzedaży detalicznej zawierają identyfikatory czy czytniki RFID. O każdym przypadku odczytu identyfikatora, mającym miejsce w handlu detalicznym, powinny wiedzieć wszystkie strony.

— Użytkownicy technologii identyfikacji radiowej muszą powiadamiać o powodach stosowania identyfikatorów i czytników. Zbieranie informacji powinno być ograniczone do zaspokojenia bieżących celów.

— Użytkownicy technologii identyfikacji radiowej są odpowiedzialni za jej wdrożenie oraz działanie w granicach przepisów i wytycznych w zakresie bezpieczeństwa danych. Są oni również odpowiedzialni za bezpieczeństwo i prawidłowe działanie systemu oraz jego baz danych.

4.7 Nie jest jeszcze pewne, w jaki sposób zasady te miałyby być realizowane w praktyce. Najlepiej byłoby, gdyby każde przedsiębiorstwo zajmujące się transakcjami z udziałem konsumentów, np. handlem detalicznym, etykietowaniem, kontrolą dostępu i usługami transportowymi, dawało klientom jakąś gwarancję ich przestrzegania, swego rodzaju kartę klienta. Ponadto EKES proponuje następujące wytyczne:

a) Należy zakazać kupcom zmuszania klientów do nabywania produktów zawierających aktywne lub uśpione identyfikatory bądź narzucania im takich produktów. Powinna istnieć między innymi możliwość dołączania identyfikatorów do opakowania, czy stosowania zdejmowanych identyfikatorów, na wzór metek na towarach.

b) Klienci powinni mieć możliwość usunięcia lub dezaktywacji wszelkich identyfikatorów umieszczonych na należących do nich przedmiotach.

c) Identyfikacji radiowej zasadniczo nie powinno się stosować do śledzenia osób. Śledzenie ludzi jest niewłaściwe, bez względu na to, czy ma to miejsce na przykład przy użyciu identyfikatorów umieszczonych na odzieży, towarach, biletach czy jakichkolwiek innych produktach.

d) Identyfikacja radiowa nie powinna być stosowana w sposób, który mógłby wykluczać lub ograniczać anonimowość.

e) Właściwe organy powinny wyraźnie wskazać, że zastosowania, o których mowa w punkcie c) i d), będą dopuszczalne jedynie w wyjątkowych okolicznościach i to po uprzednim formalnym powiadomieniu takiego organu.

4.8 Można rozważać pewne wyjątki od powyższych zasad w przypadku, gdy:

— dana osoba zdecyduje się skorzystać z możliwości utrzymania aktywności identyfikatora dla własnej wygody;

— dana osoba wyrazi swoją zgodę na śledzenie w miejscu o krytycznym znaczeniu, takim jak szczególnie ściśle chronione budynki oraz instytucje publiczne i prywatne;

— dana osoba zdecyduje się na korzystanie z zastosowań, które ją zlokalizują i zidentyfikują w taki sam sposób jak ma to już miejsce w momencie korzystania z telefonów komórkowych, kart bankomatowych, adresów internetowych itp.

Wszelkie tego rodzaju wyjątki powinny być zgłaszane właściwemu organowi.

4.9 Kategorią zastosowań, którą można by uznać za ogólny wyjątek, jest śledzenie osób lub towarów w otoczeniach, w których znajdują się przejściowo. W transporcie lotniczym etykietami RFID można by oznaczać bagaż przy jego odprawie w celu zwiększenia bezpieczeństwa oraz zapewnienia, że trafi on we właściwe miejsce, pasażerowie natomiast mogliby mieć identyfikatory celem usprawnienia obsługi i poprawy punktualności lotów oraz przyspieszenia kontroli bezpieczeństwa. Innym zastosowaniem mogłoby być śledzenie pacjentów po ich przyjęciu do szpitala na operacje. Warunkiem dopuszczalności tej kategorii zastosowań byłaby pewność dezaktywacji etykiet czy identyfikatorów na koniec danego procesu o charakterze przejściowym.

4.10 Identyfikacja radiowa nie jest technologią dojrzałą, tak więc nie pojmujemy jeszcze jej pełnego potencjału. Z jednej strony może ona przynieść niewyobrażalne korzyści naszej cywilizacji technicznej, z drugiej jednak może być największym zagrożeniem technologicznym prywatności i wolności. Zdaniem EKES-u zastosowania RFID należy rozwijać, przestrzegając ściśle kodeksu etycznego w zakresie poszanowania prywatności, wolności i bezpieczeństwa danych, niemniej należy kontynuować ów rozwój pod warunkiem zapewnienia niezbędnych zabezpieczeń.

4.11 Podsumowując, można stwierdzić, że w dziedzinach, w których dozwolone są zastosowania identyfikacji radiowej, ich wdrażanie powinno być w pełni przejrzyste dla wszystkich zainteresowanych stron. Zasadniczo dopuszczalne są zastosowania mające na celu poprawę obsługi towarów. Zastosowania umożliwiające identyfikację osób są zasadniczo niedopuszczalne, z wyjątkiem otoczenia, w którym osoby te znajdują się przejściowo. Zastosowania pozwalające na powiązanie osób z towarami mogą być dopuszczalne w celach marketingowych. Zastosowania identyfikujące osoby poprzez towary, które zakupiły, są generalnie niedopuszczalne. Ponadto niektóre zastosowania są nieodpowiednie w wolnym społeczeństwie i nie powinno się na nie zezwalać. Podstawowym zaleceniem ze strony Komisji dla państw członkowskich musi być bezwzględna potrzeba zachowania prywatności i anonimowości.

Bruksela, 11 lipca 2007 r.

Przewodniczący

Europejskiego Komitetu Ekonomiczno-Społecznego

Dimitris DIMITRIADIS