Michał Czerniawski

Prawne aspekty identyfikacji z użyciem fal radiowych (RFID)

Kwartalnik Prawa Publicznego 10/3, 95-116

2010

KWARTALNIK PRAWA PUBLICZNEGO
ROK X • NR 3/2010 • UKSW – WARSZAWA • TNOiK – TORUŃ • ISSN 1642–9591

Michał Czerniawski*

PRAWNE ASPEKTY IDENTYFIKACJI Z UŻYCIEM FAL RADIOWYCH (RFID)

1. Wstęp

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r., w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[1] w punkcie 2 preambuły stanowi, iż „systemy przetwarzania danych są tworzone po to, aby służyły człowiekowi; muszą one, niezależnie od obywatelstwa czy miejsca stałego zamieszkania osób fizycznych, szanować ich podstawowe prawa i wolności, szczególnie prawo do prywatności, oraz przyczyniać się do postępu gospodarczego i społecznego, rozwoju handlu oraz dobrobytu jednostek". Gwałtowny rozwój społeczeństwa informacyjnego – społeczeństwa, w którym niezwykle cennym towarem stało się szczególne dobro niematerialne, jakim jest informacja, doprowadził do rozwoju technologii, które ułatwiają pozyskiwanie i przetwarzanie najróżniejszych rodzajów danych, w tym danych osobowych. Wiele z technologicznych nowości stanowi potencjalne zagrożenie dla naszej prywatności, a jedną z technologii, której rozwój niesie ze sobą poważne konsekwencje w dziedzinie ochrony danych osobowych jest RFID[2], czyli identyfikacja z uży-

* Mgr Michał Czerniawski – doktorant na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego.

[1] Dz.U. WE 1995 Nr L 281/31.

[2] Ang. Radio Frequency Identification.

ciem fal radiowych. Technologia ta, będąca na początku jedynie interesującą alternatywą dla kodów kreskowych, niemal niezauważalnie wyrosła na istotny element naszego życia codziennego, a duży wpływ na jej upowszechnienie mają szybko spadające koszty produkcji znaczników RFID.

Współcześnie transpondery RFID znajdują zastosowanie nie tylko w logistyce czy monitoringu, ale także w przedmiotach codziennego użytku, takich jak karty miejskie[3], elektroniczne legitymacje studenckie[4], bezstykowe karty płatnicze[5] czy nawet w kartach kibica polskiej Ekstraklasy[6]. Także – coraz popularniejsze na świecie – płatności dokonywane poprzez zbliżenie telefonu do odpowiedniego czytnika przeprowadzane są z użyciem technologii RFID. Jednocześnie jesteśmy świadkami coraz bardziej radykalnych zastosowań znaczników RFID, włączając w to wszczepianie chipów RFID pod skórę ludziom, o czym szerzej w dalszej części niniejszego opracowania.

2. Zasady działania technologii RFID

Przed przejściem do dalszych rozważań, należałoby pokrótce omówić zasady działania technologii RFID. Identyfikacja z użyciem fal radiowych opiera się na przechowywaniu danych na niewielkich elektronicznych transponderach. Transponder RFID (nazywany też znacznikiem lub tagiem) jest radiowym urządzeniem nadawczym lub nadawczo-odbiorczym wysyłającym sygnał zawierający kodowane dane identyfikacyjne tylko w odpowiedzi na pobudzenie sygnałem radiowym o określonej częstotliwości[7].

Co do zasady system RFID składa się z systemu komputerowego (posiadającego bazę danych), czytnika (zawierającego nadajnik i dekoder) oraz transponderów, które mogą mieć różnorodną postać – nalepki, etykiety, nitu itp. Znaczniki RFID można podzielić na trzy kategorie: a) pasywne (nie posiadają własnego źródła zasilania, zasilane sygnałem radiowym z czytnika); b) pasywno-aktywne; c) aktywne (posiadające własne źródło zasilania). Dane zapisane

[3] Jak choćby Warszawska Karta Miejska.

[4] Przykładowo technologia RFID została zastosowana w co najmniej części elektronicznych legitymacji studenckich, wprowadzonych na mocy Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z 2.11.2006 r. w sprawie dokumentacji przebiegu studiów (Dz.U. Nr 224, poz. 1634).

[5] Takich jak np. MasterCard PayPass.

[6] Za: *System Ekstraklasa, Karta kibica, Wymagania dla systemów stadionowych, wersja 3.0.*

[7] Definicja za: A. Orłowski, K. Kaczan, A. Staszak, E. Tomaszuk, *Analiza tendencji rozwoju technik RFID oraz laboratorium badawcze technik RFID*, Warszawa 2008, s. 9.

w znacznikach RFID można zabezpieczać poprzez szyfrowanie. Zaszyfrowane znaczniki możemy podzielić na znaczniki: a) z zabezpieczoną informacją w trakcie transmisji (zaszyfrowany jest sygnał radiowy, za pomocą którego przesyłane są dane); b) z zabezpieczoną informacją na nośniku (zaszyfrowane są dane zapisane w pamięci znacznika) oraz c) z zaszyfrowaną tak transmisją jak i informacją. Transpondery można też podzielić ze względu na możliwości zapisu na nich danych. Według tego kryterium możemy rozróżnić znaczniki: a) przeznaczone tylko do odczytu; b) na których można zapisać informację tylko jeden raz; c) na których można zapisywać informację wielokrotnie.

Znaczniki RFID coraz częściej umieszczane są w elektronicznych chipach czy też z pozoru zwykłych etykietach. Etykiety RFID (zwane też „inteligentnymi" etykietami) występują w różnych rozmiarach oraz mogą być wykonane z różnych materiałów, włączając w to papier i tworzywa sztuczne. Postęp technologiczny umożliwił drukowanie etykiet RFID[8]. Dzięki użyciu specjalnych drukarek z wbudowanym dekoderem RFID, możliwe jest, aby w momencie drukowania etykiety, jednocześnie zapisywać dane w pamięci znacznika. Etykiety RFID przeznaczone są przeważnie do jednorazowego użytku i stosuje się je między innymi do znakowania palet, kartonów bądź produktów detalicznych w celach logistycznych. Chipy mają tę przewagę w stosunku do etykiet, iż posiadają większą pamięć, co pozwala zapisać na nich większą ilość danych niż ma to miejsce w przypadku etykiet. Najbardziej kontrowersyjnym rodzajem chipów RFID są tzw. biochipy, znaczniki umieszczane w żywych organizmach zwierzęcych i ludzkich mające na celu ich identyfikację bądź ustalenie miejsca pobytu.

3. Zastosowanie technologii RFID

Technologia RFID znajduje zastosowanie w coraz większej liczbie dziedzin naszego życia. Wciąż najszerzej stosowana jest w logistyce (znaczniki RFID umożliwiają zapisanie znacznie większej ilości oraz znacznie dokładniejszych danych dotyczących określonego obiektu, niż kod kreskowy; ponadto umożliwiają one dokładne monitorowanie trasy, jaką pokonuje oznakowany obiekt[9], a zastosowanie fal radiowych pozwala na odczytanie znaczni-

[8] Szerzej o tym osiągnięciu przykładowo: L. Grossman, *New RFID Tag Could Mean the End of Bar Codes*, Wired.com z 26.3.2010 r.

[9] Aby lepiej zobrazować możliwości znaczników RFID posłużę się przykładem: Kod kreskowy identyfikuje przedmioty określone co do gatunku np. dwulitrowe opakowanie soku jabł-

ka z pewnej odległości, bez konieczności np. otwierania kartonu z towarem), oraz we wszelkiego rodzaju kartach zbliżeniowych (karty płatnicze, karty do otwierania drzwi w biurach, hotelach etc.). Chipy z transponderami RFID są powszechnie używane w paszportach elektronicznych (zwanych też paszportami biometrycznymi). Z polskiej perspektywy technologia RFID jest istotna także dlatego, iż projektowane elektroniczne dowody osobiste (tzw. pl.ID) mają być wyposażone właśnie w chipy RFID. Zgodnie z zapowiedziami Ministerstwa Spraw Wewnętrznych i Administracji, dokument ten zawierał będzie nie tylko podpis elektroniczny, lecz także spełniać będzie funkcję klucza, umożliwiającego dostęp do danych dotyczących obywatela[10] znajdujących się w rejestrach państwowych. Znaczniki RFID są też coraz szerzej stosowane do znakowania zwierząt, znakowania książek w bibliotekach czy też pomiaru czasu na imprezach sportowych (np. uczestnicy biegu dostają opaski startowe z transponderem RFID, zaś na linii mety rozłożone są maty emitujące pole magnetyczne, „odczytujące" numery transponderów).

4. Identyfikacja z użyciem fal radiowych a prawo

Wiele państw, zwłaszcza państwa europejskie, nie pozostało obojętnych na szybki rozwój technologii RFID. Zagadnienie przetwarzania danych osobowych przy wykorzystaniu kart elektronicznych było, między innymi, przedmiotem zainteresowania Grupy ds. ochrony danych osobowych (tzw. grupa CJ-PD) działającej przy Radzie Europy. Grupa ta jeszcze w 2004 r. przygotowała wytyczne dotyczące przetwarzania danych osobowych przez karty zawierające inteligentne chipy[11]. W Unii Europejskiej szczególną uwagę roz-

kowego marki Hortex. Każde dwulitrowe opakowanie soku jabłkowego Hortex ma ten sam kod kreskowy. Natomiast dzięki zastosowaniu technologii RFID każde opakowanie soku jabłkowego Hortex może mieć swój własny, unikalny kod. Takie rozwiązanie rewolucjonizuje dystrybucję towarów, umożliwiając, poprzez odpowiednie rozmieszczenie czytników RFID, dokładną analizę trasy, jaką pokonuje konkretne opakowanie. Dzięki zastosowaniu identyfikacji z użyciem fal radiowych jesteśmy w stanie dostarczyć konkretne opakowanie soku jabłkowego Hortex do konkretnego sklepu i umieścić je na konkretnej, z góry oznaczonej półce (w przypadku, gdy posiada ona czytnik RFID).

[10] Informacja za Centrum Projektów Informatycznych Ministerstwa Spraw Wewnętrznych i Administracji, dostępna na: http://cpi.mswia.gov.pl/portal/cpi/38/195/plID.html (stan na: 20.10.2010 r.).

[11] Guiding principles for the protection of personal data with regard to smart cards, przyjęte przez Europejski Komitet ds. Współpracy Prawnej (CDCJ) na 79. spotkaniu plenarnym, które odbyło się 11–14.5.2004 r.

wojowi technologii RFID poświęciła Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (dalej: Grupa Robocza Artykułu 29)[12]. W 2005 roku wydała ona dokument roboczy poświęcony temu zagadnieniu[13]. Także w opublikowanym przez wyżej wymienioną grupę dokumencie „Przyszłość Prywatności" wspomniano zagadnienie RFID[14]. Dodatkowo, w Programie Prac na lata 2010–2011[15], Grupa Robocza Artykułu 29 zadeklarowała poświęcenie szczególnej uwagi m.in. wyzwaniom technicznym, do których zaliczyła „oceną skutków w odniesieniu do ochrony danych prywatności i danych w zakresie identyfikacji radiowej (RFID)"[16]. Jednocześnie, Komisja Europejska od kilku lat przedstawia kolejne Mapy Drogowe[17] dotyczącą podejmowanych przez nią inicjatyw w kwestii RFID i Internetu Przedmiotów. 12.5.2009 r. opublikowała ona swoje zalecenia dotyczące tego zagadnienia[18], w których zwraca uwagę na zagrożenia dla prywatności i ochrony danych osobowych, jakie niesie ze sobą upowszechnianie się identyfikacji z użyciem fal radiowych. Zgodnie z art. 288 Traktatu o Unii Europejskiej[19], zalecenia nie mają jednak mocy wiążącej wobec państw członkowskich.

Pomimo podjęcia wyżej wymienionych inicjatyw, nie powstała jeszcze unijna regulacja bezpośrednio poruszająca kwestię RFID. Grupa Robocza Artykułu 29, we wspomnianym już dokumencie roboczym, przedstawiła dość ogólne wytyczne dla producentów oraz innych podmiotów zajmujących sie technologią RFID, które mają im pomóc w przestrzeganiu zasad określonych w unijnych dyrektywach, w szczególności w dyrektywie 95/46/WE i dyrektywie 2002/58/WE[20]. Celem wytycznych jest stworzenie podstaw dla przyszłych

[12] Grupa robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określa art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

[13] Working document on data protection issues related to RFID technology, wydany 19.1.2005 r. (brak oficjalnego tłumaczenia w języku polskim), 10107/05/EN WP 105.

[14] The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, dokument przyjęty 1.12.2009 r., s. 15, 2356/09/EN WP 168.

[15] Program prac na lata 2010–2011 przyjęty 15.2.2010 r., 265/10/PL WP 170.

[16] Ibidem, s. 3.

[17] Ang. roadmap.

[18] Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, SEC(2009) 585 SEC(2009)586.

[19] Wersje skonsolidowane Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, Dz.Urz.UE 2008 Nr C 115/1.

[20] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.7.2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej.

unijnych standardów, które umożliwią rozwój technologii RFID bez naruszania prywatności obywateli. Nieco bardziej szczegółowe propozycje zawierają zalecenia przygotowane przez Komisję Europejską. Komisja Europejska proponuje m.in. nałożenie na administratorów systemów RFID obowiązku przeprowadzenia i przedłożenia odpowiedniemu organowi (w przypadku Polski – Generalnemu Inspektorowi Ochrony Danych Osobowych, dalej: GIODO, chyba, że w systemie nie będą przetwarzane dane osobowe) – na 6 tygodni przed wdrożeniem konkretnej technologii RFID – oceny skutków, jakie może ona nieść dla ochrony danych osobowych i prywatności[21]. Jak wspomniałem, ww. zalecenia nie są wiążące dla państw członkowskich. Mimo to, w ciągu 3 lat od opublikowania zaleceń Komisja Europejska zobligowała się przedstawić raport z ich implementacji, efektywności i skutków, jakie odniosły[22]. Warto w tym miejscu zwrócić uwagę na pewną tendencję pojawiającą się w pracach Unii Europejskiej, która nie występuje w, także zmagających się z zagadnieniem RFID, Stanach Zjednoczonych Ameryki, tj. na nakładanie odpowiedzialności za zgodność technologii z zasadami ochrony danych osobowych nie tylko na podmioty wykorzystujące systemy RFID, ale także na ich producentów.

Grupa Robocza Artykułu 29, w opracowanym przez siebie dokumencie roboczym rozpoznała trzy główne typy zagrożeń, jakie niesie ze sobą identyfikacja z użyciem fal radiowych:

(i) użycie technologii RFID do zbierania informacji powiązanych pośrednio bądź bezpośrednio z danymi osobowymi (np. sprzedawca, zestawiając dane z czytnika RFID umieszczonego przy kasie z danymi z karty kredytowej kupującego, jest w stanie ustalić, do kogo trafił konkretny egzemplarz towaru);

(iii) użycie technologii RFID do przechowywania danych osobowych na znacznikach RFID (np. zapisanie danych osobowych na chipie umieszczonym w paszporcie elektronicznym);

(iv) użycie technologii RFID do śledzenia osoby, bez jej identyfikowania (np. śledzenie przez sieć sklepów nawyków zakupowych osoby posługującej się kartą programu lojalnościowego wystawioną na okaziciela).

Listę zagrożeń dla prywatności i ochrony danych osobowych, jakie może ze sobą nieść technologia RFID przygotowano także w Kanadzie, kraju, który tak jak Unia Europejska, przywiązuje dużą wagę do ochrony prywatności.

[21] Por. Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, pkt 5.

[22] Por. ibidem, pkt 20.

Federalny Komisarz ds. Prywatności wyodrębnił następujące zagadnienia związane z technologią RFID:

(i) korzystając z identyfikacji z użyciem fal radiowych, informacje można pozyskiwać z ukrycia;
(ii) technologia może być wykorzystywana do śledzenia osób, na przykład jeśli znaczniki zostały umieszczone w ubraniu czy samochodzie i istnieje sieć odpowiednio rozmieszczonych czytników;
(iii) tworzenie precyzyjnych profili konkretnych osób może przybrać znaczne rozmiary, dzięki możliwości łatwego identyfikowania i przyporządkowywania przedmiotów do konkretnej osoby;
(iv) dane zebrane z pomocą RFID mogą być łatwo wykorzystane w innym celu, niż ten, dla którego zostały zebrane[23].

5. Identyfikacja z użyciem fal radiowych a zapisy ustawy o ochronie danych osobowych

5.1. Definicje

Zgodnie z art. 6 ust. 1 polskiej ustawy o ochronie danych osobowych[24] (dalej: u.o.d.o.), za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Na podstawie ust. 2 tegoż artykułu, osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Zgodnie z ust. 3 tegoż artykułu, informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

O ile w przypadku znaczników RFID zawierających w swojej pamięci dane osobowe (takich jak na przykład te umieszczone w chipach znajdujących się w paszportach elektronicznych), nie powinno budzić wątpliwości, iż mamy do czynienia z przetwarzaniem danych osobowych, o tyle w sytuacji,

[23] Za: *RFID Technologies and Consumers in The Retail Marketplace* wydane przez Industry Canada, s. 5, dostępne na: http://www.ic.gc.ca/eic/site/oca-bc.nsf/vwapj/RFID_en.pdf/$FILE/RFID_en.pdf (stan na: 15.10.2010 r.).

[24] Ustawa z 29.8.1997 r. o ochronie danych osobowych (t.j.: Dz.U. z 2002 r., Nr 101, poz. 926 ze zm.).

gdy znacznik RFID nie zawiera żadnych danych osobowych, a jedynie numer identyfikacyjny znacznika, należy dokonać analizy, czy tenże numer można uznać za dane osobowe. W przypadku, gdy ww. numer identyfikacyjny uda się zestawić z innymi informacjami, na przykład osoba z Warszawską Kartą Miejską na okaziciela (korzystającą z technologii RFID) kilkakrotnie zapłaciła za tę kartę swoją kartą kredytową, można w mojej ocenie uznać numer identyfikacyjny znacznika RFID za dane osobowe. Kwestia jest jednak skomplikowana. Zgodnie z zapisami u.o.d.o., abyśmy mieli do czynienia z danymi osobowymi, określenie tożsamości danej osoby nie powinno wymagać nadmiernych kosztów, czasu lub działań. Dlatego też każdy przypadek należy rozpatrywać indywidualnie, mając na względzie wielkość nakładów, jakich wymaga określenie tożsamości konkretnej osoby.

5.2. Zasady przetwarzania danych osobowych

Ustawa o ochronie danych osobowych w art. 7 ust. 2 definiuje przetwarzanie danych jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie. W takiej sytuacji nie budzi wątpliwości, iż przechowywanie jakichkolwiek danych na znaczniku RFID jest ich przetwarzaniem. Ustawa, wzorem dyrektywy 95/46/WE, wprowadza szereg zasad dotyczących przetwarzania danych osobowych, w szczególności nakłada na administratora danych osobowych obowiązki. Zgodnie z art. 7 ust. 4 u.o.d.o., administratorem danych osobowych jest podmiot, decydujący o celach i środkach przetwarzania danych osobowych. Do obowiązków administratora danych należy dysponowanie prawną, określoną w u.o.d.o., podstawą przetwarzania danych osobowych, udzielenie osobie, której dane dotyczą informacji m.in. o celu zbierania danych (szczegółowy zakres obowiązku informacyjnego określa art. 24 oraz art. 25 u.o.d.o.), zabezpieczenie przetwarzanych danych oraz zgłoszenie zbioru danych osobowych do GIODO.

W art. 7 ust. 1 u.o.d.o. definiuje zbiór danych osobowych jako każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. W mojej ocenie administratorzy systemów RFID, w których, w jakikolwiek sposób, znaczniki mogą być przyporządkowane do konkretnych osób, powinni mieć świadomość, iż przetwarzane przez nich dane mogą stanowić dane osobowe w rozumieniu u.o.d.o. Na przykład, nie budzi wątpliwości, iż administrator systemu RFID w sklepie, w którym imienne karty programu lojalnościowego są zestawiane z danymi ze znaczni-

ków RFID umieszczonych w towarach, przetwarza dane osobowe. Jednakże w pewnej ilości przypadków ocena, czy istnieje ryzyko, iż zbiór danych systemu RFID stanie się zbiorem danych osobowych, jest niemożliwa przed rozpoczęciem przetwarzania danych. Dopuszczam możliwość, w której administrator systemu sam nie jest świadomy, iż przetwarza w swoim zbiorze danych, dane osobowe np. pod postacią numeru identyfikacyjnego znacznika RFID. L. Edwards i J. Hatcher słusznie zauważają, że to, czy administrator będzie miał do czynienia z danymi osobowymi, może zależeć od okoliczności całkowicie losowych, takich jak to, czy klient zapłaci za zakupy gotówką, czy kartą kredytową albo czy kasjer przez pomyłkę nie dezaktywuje znacznika RFID przy kasie[25]. Brak świadomości przetwarzania danych osobowych nie zwalnia jednak administratora z przestrzegania obowiązków, które nakłada na niego u.o.d.o. oraz Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29.4.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[26].

Tak w Polsce, jak i na terenie całej Unii Europejskiej obowiązują zasady dotyczące przetwarzania danych osobowych. Zgodnie z art. 23 u.o.d.o. musi istnieć podstawa do przetwarzania danych osobowych (najczęściej jest nią zgoda osoby, której dane dotyczą). Ponadto, dane powinny być aktualne i odpowiednio zabezpieczone; osoba, której dane dotyczą powinna znać cel ich przetwarzania, a także posiadać informację o podmiocie odpowiedzialnym za przetwarzanie danych; powinna także mieć dostęp do danych i prawo ich poprawiania oraz usuwania danych w określonych przypadkach; administrator danych osobowych jest odpowiedzialny za przestrzeganie powyższych zasad.

5.2.1. Podstawa przetwarzania danych osobowych

Jak wspomniałem, najczęściej spotykaną podstawą do przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą. W mojej ocenie w przypadku technologii RFID zgoda na przetwarzanie danych osobowych powinna być udzielona z wyraźnym zaznaczeniem, iż osoba, która ją wyraża jest świadoma, iż dane będą pozyskiwane przy wykorzystaniu identyfikacji

[25] L. Edwards, J. Hatcher, *Consumer Privacy Law 2: Data Collection, Profiling and Targeting* [w:] *Law and the Internet*, red. L. Edwards, Ch. Waelde, Oxford 2009, s. 523.

[26] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29.4.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

z użyciem fal radiowych. Oczywiście przy zbieraniu zgody powinien być precyzyjnie podany cel zbierania danych.

O ile samo udzielenie zgody na przetwarzanie danych z użyciem technologii RFID nie budzi kontrowersji, o tyle poważnym problemem dla administratora danych może okazać się sytuacja, w której osoba wycofuje zgodę na przetwarzanie swoich danych. Problem ten dostrzegła m.in. Grupa Robocza Artykułu 29[27]. Zgodnie z uodo, przez usuwanie danych osobowych rozumie się ich zniszczenie lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą. W przypadku wycofania zgody na przetwarzanie danych osobowych zapisanych w pamięci znacznika RFID, oznacza to konieczność dezaktywacji znacznika, bądź też usunięcia danych (pod warunkiem, że jest to technologicznie możliwe). Operacja ta wymaga specjalistycznego sprzętu i przez to może być przeprowadzona tylko w miejscach dysponujących odpowiednim zapleczem technologicznym. W związku z powyższym Grupa Robocza Artykułu 29 stoi na stanowisku, iż tak producent jak i podmiot rozmieszczający znaczniki powinni upewnić się, że transponder można dezaktywować bez większych problemów, na przykład w miejscu, w którym nabyto przedmiot zabezpieczony znacznikiem.

Inną kwestią związaną z zaprzestaniem przetwarzania danych osobowych, jest zagadnienie utylizacji chipów RFID zawierających dane osobowe. Na przykład w Kanadzie Federalny Komisarz ds. Prywatności w toku prac nad paszportami elektronicznymi wymusił na agencji odpowiedzialnej za wdrożenie e-paszportów, wprowadzenie procedury utylizacji zwracanych dokumentów (dotychczasowa praktyka polegała na znakowaniu i zwracaniu paszportów, które utraciły już ważność, ich właścicielom). W przypadku paszportów elektronicznych ich zwrot właścicielom niesie ze sobą ryzyko, iż dane, w tym dane biometryczne, zawarte w chipie umieszczonym w paszporcie, który utracił już ważność, mogłyby być odczytane przez osoby trzecie bez zgody i wiedzy ich posiadaczy. O ile wciąż większość chipów umieszczonych w paszportach elektronicznych na świecie co do zasady powiela informacje wydrukowane w paszporcie (takie jak imię, nazwisko, data urodzenia, miejsce urodzenia, etc.), o tyle można już teraz dostrzec tendencję do umieszczania na chipach coraz większej ilości unikalnych danych biometrycznych.

5.2.2. Obowiązek informacyjny

Z kwestią podstawy prawnej, w szczególności uzyskania zgody, związany jest obowiązek informacyjny. Obowiązek informacyjny nałożony jest

[27] Por. Working document on data protection issues related to RFID technology, pkt 5.4.

na administratora danych osobowych przez art. 24 i art. 25 u.o.d.o. Administrator danych osobowych jest zobowiązany poinformować osobę, której dane dotyczą m.in. o adresie swojej siedziby, celu zbierania danych, odbiorcach danych oraz prawie dostępu do treści swoich danych. W mojej ocenie dalszy rozwój technologii RFID powinien skłonić ustawodawcę do rozważenia specyficznego obowiązku informacyjnego związanego z RFID. Rozróżniłbym dwa rodzaje obowiązku informacyjnego związanego z identyfikacją z użyciem fal radiowych. Pierwszym jest udzielenie, przy pozyskiwaniu zgody na przetwarzanie danych, informacji o zasadach działania tej technologii tak, aby wyrażający zgodę był w pełni świadomy jej konsekwencji, w szczególności okoliczności, iż identyfikacja następuje radiowo, często bez wiedzy osoby, której dotyczy. Drugi obowiązek informacyjny polegałbym na odpowiednim oznakowaniu przedmiotu wyposażonego w transponder RFID (przykładowo umożliwiającym łatwe rozróżnienie kart płatniczych z transponderem od „zwykłych" kart stykowych). Swoistym precedensem są w tym wypadku paszporty elektroniczne, które na okładce mają wytłoczony, doskonale widoczny, specjalny symbol informujący o tym, iż konkretny paszport wyposażony jest w chip RFID. Wydaje się także wskazane, aby czytniki RFID reagowały (np. poprzez sygnał dźwiękowy lub świetlny), gdy odczytują znacznik RFID, tak aby osoba będąca w posiadaniu przedmiotu wyposażonego w transponder zdawała sobie sprawę, iż ktoś uzyskał dostęp do jego zawartości.

Informowanie osób o obecności tak znaczników RFID w produktach, jak i czytników RFID poprzez ich odpowiednie znakowanie zaleca także Komisja Europejska[28]. Ponadto sugeruje ona dezaktywację lub usuwanie znacznika z produktu w punkcie jego sprzedaży, chyba, że konsument wyrazi zgodę na jego pozostawienie[29]. Powyższe zalecenie nie dotyczy znaczników stosowanych w handlu, które nie niosą ze sobą zagrożenia dla prywatności lub ochrony danych osobowych (np. używanych wyłącznie dla usprawnienia logistyki).

5.2.3. Prawo dostępu do treści swoich danych oraz ich poprawiania

Innym zagadnieniem, o naturze podobnej do problemu powstającego w przypadku wycofania zgody na przetwarzanie danych, jest kwestia uzyskania dostępu do swoich danych zapisanych na znaczniku RFID i ich poprawiania. Zgodnie z art. 32 u.o.d.o., każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawar-

[28] Por. Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, pkt. 8 i 9.

[29] Por. ibidem, pkt 11.

tych w zbiorach danych. Zgodnie z ust. 6 tegoż artykułu, każdej osobie przysługuje prawo do żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

W dobie technologii RFID, na przykład, osoba posiadająca paszport biometryczny zazwyczaj wie, jakie dane osobowe zapisano w pamięci chipa umieszczonego w paszporcie, jednak nie jest w stanie w żaden sposób uzyskać do nich dostępu[30]. Dotychczas, przy wykorzystaniu tradycyjnych metod identyfikacji (dowód osobisty, tradycyjny paszport), osoba, której dane dotyczą zawsze wiedziała, jakie dane osobowe służą do jej weryfikacji, gdyż były one wydrukowane w posiadanym przez nią dokumencie i widoczne gołym okiem. Wiedziała więc, czy są one kompletne, aktualne i prawdziwe. Wraz z rozwojem technologii RFID, wydaje się, że korzystanie z prawa dostępu do swoich danych, w przypadku nie wypracowania odpowiednich standardów, może być utrudnione, a administratorzy danych osobowych mogą łatwo dopuścić się naruszenia przepisów u.o.d.o.

Dodatkowo, jak już wcześniej wspomniałem, tylko niektóre typy znaczników RFID pozwalają na edycje raz zapisanych danych. Znaczniki wielokrotnego zapisu są znacznie droższe od ich „jednorazowych" odpowiedników, stąd rzadko stosowane. Ogranicza to znacząco możliwość korzystania przez osoby, których dane dotyczą z uprawnienia do poprawiania swoich danych. W obecnej sytuacji edycja danych wiąże się więc *de facto* z koniecznością zniszczenia obecnego znacznika RFID i zapisania zmienionych danych na nowym urządzeniu.

5.2.4. Zabezpieczenie danych osobowych

Zgodnie z art. 36 ust. 1 u.o.d.o., administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. W szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

---

[30] Sposobem na uczynienie zadość temu uprawnieniu mogłoby być np. rozmieszczenie ogólnodostępnych czytników RFID w punktach paszportowych.

Sporym problemem w przypadku identyfikacji z użyciem fal radiowych może okazać się odpowiednie zabezpieczenie danych osobowych. Powszechnie używane zabezpieczenia – nawet te zastosowane w paszportach elektronicznych – są słabe i łatwe do złamania[31]. Już dziś osoba dysponująca odpowiednimi, stosunkowo niedrogimi, urządzeniami nie ma problemu z uzyskaniem dostępu do zawartości znacznika. Można przy tym rozróżnić dwa rodzaje zabezpieczeń: a) szyfrowanie danych zapisanych w pamięci transpondera; b) szyfrowanie sygnału radiowego wysyłanego przez znacznik RFID.

Dopóki powszechnie używane znaczniki są w stanie przekazywać dane tylko na bardzo małe odległości, problem odpowiedniego zabezpieczenia zawartości znacznika nie jest poważnym zagrożeniem dla ochrony danych osobowych. Powstają jednak coraz bardziej zaawansowane technologicznie transpondery i niektóre z nich (np. aktywne chipy, używane do znakowania i śledzenia migracji dzikich zwierząt) są już w stanie emitować sygnał radiowy na znaczne odległości. Kwestią czasu jest, gdy staną się one standardem, a wtedy administratorzy danych osobowych staną przed poważnym problemem, jak odpowiednio zabezpieczyć przetwarzane z użyciem technologii RFID dane.

5.3. Kazus Warszawskiej Karty Miejskiej

Jedną z ciekawszych spraw dotyczących RFID w Polsce było postępowanie administracyjne w sprawie przetwarzania danych osobowych użytkowników Warszawskiej Karty Miejskiej przez Zarząd Transportu Miejskiego w Warszawie (dalej: ZTM). W wydanej 3.7.2009 r. decyzji[32], GIODO nakazał zaprzestanie pozyskiwania oraz usunięcie przetwarzanych w systemie ZTM, numerów spersonalizowanych Warszawskich Kart Miejskich, pozyskanych w trakcie dokonywania ich kolejnych skasowań, jeżeli kasowania nie miały na celu aktywacji biletów zakodowanych na Warszawskich Kartach Miejskich. *De facto* mamy tu do czynienia z numerami transponderów RFID umieszczonych w kartach. Kasowniki oraz bramki wejściowe do metra to nic innego jak urządzenie wyposażone w czytnik RFID. Nie budzi wątpliwości, iż numer spersonalizowanej – z wydrukowanym imieniem i nazwiskiem oraz zdjęciem posiadacza – karty miejskiej jednoznacznie identyfikuje jej użytkownika.

[31] O przełamaniu zabezpieczeń jednego z najpopularniejszych standardów kart RFID na świecie – MiFare Classic (na świecie jest ponad 2 mld kart z transponderem w tym standardzie) można poczytać szerzej np. w magazynie „Computerworld", dostępny na: http://www.computerworld.pl/news/162429_1/Odkryte.zabezpieczenia.RFID.html (stan na: 20.10.2010 r.).

[32] Sygn. DIS/DEC-598/24248/09 dot. DIS-K-421/88/09.

GIODO uznał dane pozyskiwane z użyciem karty za dane geolokacyjne, umożliwiające lokalizacje konkretnej osoby. Gdyby nie ingerencja GIODO, ZTM do dziś zbierałby olbrzymie ilości danych osobowych posiadaczy spersonalizowanych kart miejskich pozwalających ustalić nie tylko miejsce ich pobytu, ale także mogących zdradzać takie informacje, jak nawyki czy miejsce zamieszkania i pracy. Pierwotnym zamierzeniem Zarządu Transportu Miejskiego było zbieranie danych m.in. w celu dokonywania analiz, planowania, organizacji i koordynacja układu komunikacyjnego oraz rozkładu jazdy, a także nadzór nad bieżącym funkcjonowaniem transportu zbiorowego. GIODO słusznie uznał jednak, że ZTM musi zadowolić się informacją statystyczną, ilościową, tj. ile osób, gdzie i kiedy korzystało z danego środka transportu, bez identyfikowania tychże osób.

6. RFID a biometria i dane sensytywne

Kategorią znaczników RFID o szczególnej doniosłości dla ochrony danych osobowych są chipy zawierające dane biometryczne. Najpopularniejszym przykładem tego rozwiązania są paszporty elektroniczne. Aktualnie, istnieją dwa standardy paszportów elektronicznych: BAC[33] i EAC[34]. Paszporty w systemie BAC (obecnie jest to najpopularniejszy standard paszportów biometrycznych) zawierają tylko jedną cechę biometryczną. Od 29.6.2009 r. Polska używa w swoich paszportach standardu EAC, w którym chip RFID zawiera dwie dane biometryczne: odciski palców oraz obraz twarzy. Innymi cechami biometrycznymi, które w najbliższej przyszłości mogą zostać użyte do identyfikacji konkretnej osoby, są m.in. wygląd tęczówki oka czy też układ żył na wewnętrznej stronie dłoni. Takie dane mają tę przewagę nad obecnie używanymi informacjami biometrycznymi, iż w przeciwieństwie do odcisków palców oraz wyglądu twarzy, są danymi których po sobie nigdzie nie pozostawiamy (odciski palców zostają na wszystkim czego dotkniemy, wygląd twarzy mogą zarejestrować np. kamery monitoringu), dzięki czemu dostęp do nich jest mocno utrudniony[35]. Czyni to wspomniane metody identyfikacji bezpiecz-

[33] Ang. Basic Access Control.

[34] Ang. Extended Access Control.

[35] Szerzej o zaletach wykorzystania w biometryce układu żył na palcach bądź dłoniach pisze przykładowo Bruce Schneier, kryptograf i specjalista z zakresu bezpieczeństwa teleinformatycznego, na swoim blogu: http://www.schneier.com/blog/archives/2007/08/another_biometr.html (stan na: 21.10.2010 r.).

niejszymi, niż te, które są stosowane obecnie. Przyszłościową wydaje się być zwłaszcza identyfikacja z użyciem układów żył – jako mniej inwazyjna i łatwiejsza do akceptacji niż identyfikacja z użyciem tęczówki[36].

Art. 27 ust. 1 u.o.d.o. zabrania przetwarzania tzw. danych sensytywnych, do których zalicza między innymi dane o stanie zdrowia. W tym miejscu chciałbym posłużyć się przykładem tęczówki oka, której kształt stanowi dane biometryczne, a z której stanu już dziś można uzyskać informację o niektórych dolegliwościach danej osoby[37]. W mojej ocenie można więc rozważyć uznanie wyglądu tęczówki za dane biometryczne umożliwiające uzyskanie informacji o stanie zdrowia konkretnej osoby, czyli za dane sensytywne. Wydaje się zatem, że na przykład zastosowanie w biurach identyfikacji z użyciem dostępnych już w Polsce czytników tęczówki oka, może stanowić naruszenie u.o.d.o.

Dane sensytywne można także zbierać poprzez samo śledzenie osób z wykorzystaniem identyfikacji z użyciem fal radiowych (choćby poprzez zestawienie danych ze znacznika z innymi bazami danych – np. ustalenie, że osoba nosząca męski sweter ze znacznikiem kilkukrotnie spędziła noc w klubie dla homoseksualistów). Dane te są zbierane pośrednio i wymagają zestawienia z innymi bazami danych (w podanym powyżej przykładzie męskiego swetra wymagany jest dostęp do bazy danych sklepu, w którym ubranie zakupiono i do bazy danych klubu, przy założeniu, że stosuje on technologię RFID). Już teraz technologia RFID bywa używana do śledzenia osób, gdy wymagają tego względy bezpieczeństwa. Na przykład w Japonii technologię RFID zastosowano w kilku szkołach i przedszkolach do znakowania uczniów[38]. Zastosowanie systemu RFID pozwoliło na uproszczenie procesu monitorowania obecności dzieci na terenie placówki dydaktycznej. Innym interesującym przykładem zastosowania technologii RFID w celu śledzenia ludzi jest system stworzony przez NTT i Dainippon Printing pozwalający rodzicom uczniów na zdalne obserwowanie swoich pociech dzięki czytnikom RFID i kamerom internetowym umieszczonym w klasach. W tym celu rodzic loguje się na odpowiedniej stronie internetowej i podaje dane swojego dziecka. Lokalizacja dziecka odbywa się poprzez zlokalizowanie znacznika RFID o danym numerze identyfikacyjnym. Po ustaleniu miejsca pobytu dziecka, do rodzica prze-

[36] Szerzej na ten temat por. S. Berrong, *Biometrics Put to the Test*, „Security Management" 2010, nr 2, s. 60–65.

[37] Istnieje nawet cały system medycyny naturalnej oparty wyłącznie o analizę tęczówki, zwany Irydologią.

[38] Za: RFID in Japan http://rfidinjapan.wordpress.com/category/security/ (stan na: 23.10.2010 r.).

syłany jest obraz z kamery ustawionej w miejscu, w którym aktualnie znajduje się uczeń[39].

7. Identyfikowanie ludzi z użyciem biochipów

Inną kwestią, którą chciałbym poruszyć w niniejszej publikacji, jest zagadnienie wszczepiania chipów RFID ludziom. Choć temat ten dla niektórych może wydawać się zagadnieniem bardziej z dziedziny „science fiction" niż rzeczywistym, umieszczanie chipów RFID pod ludzką skórą ma już na świecie miejsce od kilku lat. Jak łatwo dostrzec, tego typu działanie rodzi poważne pytania związane z ochroną danych osobowych.

Pionierem w dziedzinie wszczepiania ludziom chipów jest amerykańska spółka Verichip. Zgodę na wszczepianie chipów ludziom wydała amerykańska Agencja ds. Żywności i Leków[40]. W 2008 r. na świecie było ponad 2,5 tysiąca osób z wszczepionymi chipami RFID[41]. Jak można się spodziewać, przez ostatnie dwa lata liczba ta na pewno wzrosła. Aktualnie jednym z głównych zastosowań biochipów jest umożliwienie szybkiej identyfikacji osób z zaawansowaną chorobą Alzheimera. Ponadto, technologia zwana VeriMed jest także stosowana do szybkiej identyfikacji pacjentów, którzy np. utracili przytomność, bądź z innych powodów nie ma z nimi kontaktu. Umożliwia ona szybki dostęp do dokumentów medycznych pacjenta i ustalenie, czy ma on na przykład alergię na niektóre medykamenty, bądź czy choruje na choroby mogące mieć wpływ na jego leczenie np. cukrzycę. W 2008 r. w USA w pilotażowym programie identyfikacji pacjentów uczestniczyło 110 szpitali[42]. Zgodziły się one na umieszczenie odpowiednich czytników RFID na swoich izbach przyjęć i skanowanie przywożonych pacjentów w poszukiwaniu wszczepionych chipów[43].

---

[39] Za stroną Studenckiego Koła Naukowego Cybernetyki Politechniki Warszawskiej: http://cyber.ise.pw.edu.pl/index.php?option=com_content&task=view&id=38&Itemid=2626 (stan na: 23.10.2010 r.).

[40] Ang. Food and Drug Administration, w skrócie: FDA, informacja za C. Heinrich, *RFID and Beyond*, Indianapolis 2005, s. 179.

[41] Dane za: L. Laytner, *Verichip to Implant Alzheimer's Patients*, „Meritum Media" z 3.11.2008 r., dostępne na: http://www.meritummedia.com/health/verichip-to-implant-alzheimers-patients (stan na: 5.5.2010 r.).

[42] Ibidem.

[43] W całości zagadnieniu stosowania w szpitalach technologii RFID do oznaczania tak przedmiotów jak i ludzi poświęcony jest artykuł J.A. Fisher i T. Monahan, *Tracking the social dimensions of RFID systems in hospitals*, „International Journal of Medical Informatics" 2008 vol. 77, s. 176–183.

Chipy RFID są wszczepiane ludziom także z innych, niż medyczne, pobudek. W 2004 r. szerokim echem w mediach odbiło się wprowadzenie technologii RFID w Baja Beach Club w Barcelonie[44]. Bywalcy klubu mogą wszczepić sobie pod skórę chip, umożliwiający dostęp do strefy VIP oraz płacenie za drinki. Także za tym projektem stał amerykański VeriChip.

Z punktu widzenia ochrony danych osobowych, jeżeli biochip został wszczepiony na dłuższy okres czasu, konkretna osoba może zostać przyporządkowana do numeru chipu, który jej wszczepiono. W ten sposób numer chipu staje się jej daną osobową. W takim przypadku administrator systemu RFID staje się administratorem danych osobowych i musi uczynić zadość obowiązkom nakładanym na administratorów danych przez przepisy u.o.d.o.

Zagadnienie wszczepiania biochipów ludziom było już szeroko dyskutowane w USA. W 2007 r. w Kalifornii[45] oraz w Północnej Dakocie[46] uchwalono prawo zabraniające przymusowego wszczepiania chipów ludziom (np. przez pracodawców). Jeszcze w 2006 r. podobną regulację wprowadzono w Wisconsin[47] a stany Georgia i New Hampshire powołały grupy robocze mające zajmować się technologią RFID[48]. Obecnie, w stanach New Hampshire[49] i Alaska[50] trwają prace nad regulacjami dotyczącymi identyfikacji z użyciem fal radiowych. New Hampshire, już w 2006 r., zakazało identyfikacji z użyciem RFID pasażerów pojazdów oraz samych pojazdów[51]. Ze względu na ilość danych o osobie z wszczepionym chipem, jakie potencjalnie można zgromadzić, oraz na zagrożenie, jakie uzyskane w ten sposób dane osobowe mogą nieść dla prywatności, moratorium na wszczepianie biochipów ludziom wydaje się być najlepszym rozwiązaniem, gwarantującym, iż technologia RFID nie będzie rozwijać się w niebezpiecznym dla ludzi kierunku. Zwłaszcza, że nie-

[44] Za S. Morton, *Barcelona clubbers get chipped*, BBC News, 29.9.2004 r., dostępne na: http://news.bbc.co.uk/2/hi/technology/3697940.stm (stan na: 20.10.2010 r.).

[45] S.B. 362, 2007–2008 Reg. Sess. (Cal. 2007). Informacja za: ACLU-NC, *California RFID Bill Signed Into Law Today By Governor*, dostępna na: http://www.aclunc.org/issues/technology/blog/california_rfid_bill_signed_into_law_today_by_governor.shtml (stan na: 20.10.2010 r.).

[46] S.B. 2415, 60th Leg. Sess. (N.D. 2007).

[47] A.B. 290, 2005 Leg. Sess. (Wis. 2006). Więcej informacji w: M. L. Songini, *Wisconsin law bars forced RFID implants*, „Computerworld" z 12.6.2006 r., dostępne na: http://www.computerworld.com/s/article/111542/Wisconsin_law_bars_forced_RFID_implants (stan na: 20.10.2010 r.).

[48] H.R. 1558, 2005–2006 Leg. Sess. (Ga. 2006); H.B. 203, 2006 Sess. (N.H. 2006).

[49] H.B. 686-FN.

[50] S.B. 293.

[51] H.B. 1738, 2006 Sess. (N.H. 2006).

ustannie pojawiają się nowe wyzwania związane z biochipami. Na przykład w 2010 r., Mark Gasson, pracownik naukowy jednego z amerykańskich uniwersytetów, sam wszczepił sobie biochip a następnie zaraził go komputerowym wirusem[52]. Wirus został zaprogramowany w ten sposób, aby przegrywać się ze znacznika na czytniki RFID. Wizja wirusów komputerowych rozprzestrzeniających się z jednego wszczepionego człowiekowi biochipa na następne i na przykład wykradających nasze dane, z uwagi na wspomniane już, słabe zabezpieczenia technologii RFID, wydaje się całkiem realna. Ponieważ nie sposób dokładnie przewidzieć kierunku rozwoju biochipów, zakaz ich wszczepiania ludziom wydaje się dobrym rozwiązaniem, pozwalającym chronić naszą prywatność i dane osobowe.

8. Krytyka RFID

Coraz silniejsza obecność identyfikacji z użyciem fal radiowych w życiu codziennym wywołała na świecie silną falę krytyki[53]. Powstały organizacje konsumenckie, które widząc w RFID zagrożenie dla naszej prywatności, sprzeciwiają się dalszemu rozwojowi tej technologii. Najbardziej znaną ze wspomnianych organizacji jest CASPIAN[54], który w ramach swojej działalności publikuje m.in. metody „obrony" przed technologią RFID stosowaną w supermarketach i doradza, aby na przykład płacić za zakupy tylko i wyłącznie gotówką, czy też zrezygnować z udziału w programach lojalnościowych prowadzonych przez sklepy. Sprawą zajmuje się też wiele organizacji interesu publicznego takich jak: Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC) czy kanadyjski Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC). Ponadto technologia RFID wywołuje sprzeciw niektórych środowisk chrześcijańskich, które postrzegają

[52] Szerzej o tej historii w: *Could Humans Be Infected by «Computer Viruses?* na stronie Science Daily: http://www.sciencedaily.com/releases/2010/05/100526095830.htm (stan na: 8.10.2010 r.).

[53] Powstało wiele publikacji na temat negatywnego wpływu RFID na naszą prywatność oraz niezliczona ilość stron internetowych. Jedną z najpopularniejszych publikacji poruszających ten temat jest książka „Spychips" autorstwa K. Albrecht i L. McIntyre, autorki roztaczają w niej orwellowską wizję przyszłości, w której rządy oraz międzynarodowe korporacje szpiegują zwykłych obywateli za pomocą chipów RFID.

[54] CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering), działania tej organizacji związane z walką z RFID można śledzić na stronie internetowej www.spychips.com (stan na: 15.10.2010 r.).

biochipy, jako biblijne znamię Bestii[55]. Część badaczy wskazuje jednak, że stosunek konsumentów do RFID jest często kształtowany przez emocje i wynika z braku informacji o zasadach funkcjonowania tej technologii[56]. Wydaje się, że to, co wzbudza największe obawy, to fakt, iż fale radiowe są niewidzialne i jesteśmy skanowani przez czytniki RFID bez naszej wiedzy.

Technologia RFID była także przedmiotem kilku kontrowersyjnych eksperymentów. Do najbardziej znanych należy akcja przeprowadzona w 2003 roku, w Cambridge w Wielkiej Brytanii, przez jeden z supermarketów. W sklepie tym umieszczono maszynki do golenia Gillette Mach3 (te niewielkie, ale drogie maszynki, często padały łupem złodziei) na tzw. inteligentnych półkach[57], czyli półkach z wbudowanym czytnikiem RFID. Rejestrowały one, kiedy klient podnosił z półki maszynkę (zabezpieczoną znacznikiem RFID) a umieszczony przy półce automat symultanicznie robił klientowi zdjęcie. Następne zdjęcie robiono klientowi płacącemu za maszynkę, po czym ochrona porównywała zdjęcia, sprawdzając czy każdy, kto wziął maszynkę z półki, zapłacił za nią przy kasie[58]. Opisany eksperyment służył wyłapaniu złodziei. Ten sam mechanizm, z równą skutecznością, mógłby jednak być zastosowany na przykład w marketingu. Precyzyjne informacje o osobach nabywających konkretny produkt, które można z jego pomocą uzyskać, pozwoliłyby na dokładne profilowaniu klientów i wyeliminowanie zawodnego „ludzkiego czynnika" z procesu zbierania danych o konsumentach. Eksperyment w supermarkecie zakończono, między innymi z powodu protestu klientów przed wspomnianym sklepem.

9. „Internet Przedmiotów" jako nasza przyszłość

W tym miejscu warto pokrótce wspomnieć o tym, do czego może prowadzić rozwój technologii RFID. Niemal wszyscy badacze zagadnienia identyfikacji z użyciem fal radiowych przyszłość upatrują w „Internecie Przedmio-

[55] W Internecie jest mnóstwo artykułów a nawet filmów dedykowanych tej kwestii. Przykładowo: M. Rozbicki, *Mikroczipy – kto przyjmie „znamię bestii" z* 11.11.2009 r., dostępny na: http://www.eioba.pl/a109649/mikroczipy_kto_przyjmie_znamie_bestii (stan na: 20.10.2010 r.).

[56] Tak przykładowo w: M. Boslau i B. Lietke, *RFID is in the Eye of the Consumer – Survey Results and Implications* [w:] *Marketing from the Trenches: Perspectives on the Road Ahead,* red. N. Papadopoulos, C. Veloutsou, Ateny 2006, s. 9.

[57] Ang. smart shelves.

[58] Za: *The car dup their sleeve*, „The Guardian" z 19.7.2003 r., dostępny na: http://www.guardian.co.uk/lifeandstyle/2003/jul/19/shopping.features (stan na: 27.10.2010 r.).

tów"[59]. Internet Przedmiotów to system, w którym w oparciu o technologię RFID, przedmioty będą w stanie komunikować się ze sobą bez udziału ludzi[60]. Często spotykanym przykładem funkcjonowania Internetu Przedmiotów jest lodówka, która rejestruje co z niej wyjęto i w ten sposób sporządza listę zakupów, ostrzega nas, że mamy na dany produkt alergię, bądź też potrafi ustalić z której fermy pochodzą zakupione właśnie jajka. Innym przykładem działania Internetu Przedmiotów jest ubranie wyposażone w chip, które samo „informuje" pralkę o optymalnej temperaturze w jakiej należy je prać[61]. Domy, będące prototypami rozwiązań oferowanych przez Internet Przedmiotów i zwiastunami tego, co może nastąpić w przyszłości już istnieją – na przykład właścicielem jednego z nich jest założyciel Microsoftu, Bill Gates.

Już wkrótce możemy znaleźć się w świecie, w którym ceny w sklepie dostosowywać się będą do konkretnego konsumenta i jego historii zakupów zapisanej na chipie RFID, a przekroczenie prędkości stwierdzać się będzie automatycznie, na podstawie pomiaru średniej prędkości samochodu wyposażonego w tablicę rejestracyjną z chipem, jadącego po autostradzie, wzdłuż której rozstawiono czytniki RFID[62]. Potencjał tej technologii jest olbrzymi, dlatego jest wielce prawdopodobnym, że przyszłość będzie należeć do RFID i Internetu Przedmiotów. Potwierdzają to nie tylko coraz to nowe osiągnięcia technologiczne we wspomnianych dziedzinach, ale także działania podejmowane przez ustawodawców. Już kilka lat temu Komisja Europejska powołała zespoły zajmujące się zjawiskiem Internetu Przedmiotów, jak również opublikowano kilka oficjalnych dokumentów unijnych poświęconych temu zagadnieniu[63]. Istnieje też oficjalna strona internetowa Unii poświęcona tej tematyce[64]. Warto wspomnieć, iż Internet Przedmiotów był też jednym z tematów tegorocznej Konferencji Europejskich Rzeczników Ochrony Danych i Prywatności[65].

---

[59] Ang. Internet of Things.

[60] Tak zwana komunikacja M2M (ang. Machine-to-Machine).

[61] Za raportem firmy Siemens, *Transforming Production with Tiny Transponders*, dostępnym na: http://www.siemens.com/innovation/en/publikationen/publications_pof/pof_fall_2002/industry_articles/transponders.htm (stan na: 19.10.2010 r.).

[62] Przykład za S. D. Gilbert, *Digital Footprints: The Use of RFID Technology for General Law Enforcement*, artykuł dostępny za pośrednictwem SSRN: http:// www.ssrn.com

[63] Pełna lista tychże dokumentów dostępna jest na: http://www.iot-visitthefuture.eu/index.php?id=49 (stan na: 19.10.2010 r.).

[64] Adres tej strony to: http://www.iot-visitthefuture.eu/ (stan na: 19.10.2010 r.). Z listą oficjalnych dokumentów unijnych dotyczących RFID można zapoznać się na: http://www.iot-visitthefuture.eu/index.php?id=59 (stan na: 19.10.2010 r.).

[65] Por. program konferencji dostępny na stronie GIODO: http://www.giodo.gov.pl/plik/id_p/1907/j/pl/ (stan na: 19.10.2010 r.).

10. Podsumowanie

Lucas Introna nazwał prywatność wartością, którą „dobrze mieć", czymś, z czego łatwo rezygnujemy w obliczu innych istotnych spraw, takich jak na przykład bezpieczeństwo[66]. W mojej ocenie, z prywatności rezygnujemy nie tylko w obliczu spraw istotnych, ale także błahych, choćby dla naszej wygodny. Technologia RFID, w większości przypadków, nie tyle identyfikuje daną osobę, co ułatwia jej identyfikację. Pełna identyfikacja z użyciem RFID to tylko kwestia czasu. Technologia RFID z pewnością uczyni nasze życie łatwiejszym, przykłady obrazujące jej możliwości, takie jak opisana powyżej lodówka, przemawiają do ludzkiej wyobraźni. Kwestią czasu jest to, kiedy technologia RFID złoży nam propozycję nie do odrzucenia, oferując nową, jeszcze wyższą jakość życia, za cenę niewielkich wyrzeczeń, m.in. w sferze prywatności. Już teraz, na przykład przystępując do programów lojalnościowych, konsumenci wymieniają informacje o swoich preferencjach i nawykach na punkty, które sklepy zamieniają na nagrody. Informacje o sobie ludzie sprzedają całkiem dobrowolnie. Dlatego też w mojej ocenie prawo powinno nie tyle dogonić, ile wyprzedzić rozwój technologii RFID i wyznaczyć standardy ochrony danych osobowych, które już na etapie projektowania nowych urządzeń wyeliminują ryzyko naruszenia prywatności. W pracach nad ww. standardami można zastanowić się nad zastosowaniem odpowiednika, coraz szerzej stosowanej w Unii Europejskiej, tzw. Zasady Zapobiegania[67]. W skrócie, zasada ta polega na tym, iż podmiot chcący wdrożyć nową technologię musi udowodnić, że jest ona nieszkodliwa, w tym wypadku – że nie niesie ze sobą negatywnych konsekwencji w dziedzinie prywatności i ochrony danych osobowych. W podobnym kierunku, oceny zagrożenia przed implementacją nowej technologii, zmierzają zalecenia dotyczące RFID wydane przez Komisję Europejską.

Ponadto, w mojej ocenie, koniecznym jest znowelizowanie istniejącego ustawodawstwa tak w Polsce, jak i w całej Unii Europejskiej, i nałożenie w przy-

[66] Por. Lucas D. Introna, *Privacy and the Computer: Why We Need Privacy In the Information Society*, Metaphilosophy, 28(3), s. 274.

[67] Ang. Precautionary Principle. Więcej o Zasadzie Zapobiegania można dowiedzieć się przykładowo z lektury artykułu R. Andorno, *The Precautionary Principle: A New Legal Standard for a Technological Age*, dostępnego na: http://www.ethik.uzh.ch/ibme/team/mitarbeitende/andorno/precautionaryprinciple.pdf (stan na: 19.10.2010 r.).

padku technologii RFID dodatkowych obowiązków informacyjnych na administratora danych, nakazujących wyraźne informowanie osób mających do czynienia z tą technologią o podstawowych zasadach jej działania i konsekwencjach, jakie ona ze sobą niesie. Dodatkowo, obiekty wyposażone w transponder RFID powinny być specjalnie znakowane. W szczególności dotyczy to towarów w sklepach – tak, aby konsument miał świadomość obecności znacznika i mógł, na przykład, upewnić się, że został on dezaktywowany po dokonaniu zakupu. Liczę także, że prędzej czy później pojawią się, tak jak miało to już miejsce w niektórych stanach USA, regulacje prawne dotyczące identyfikacji z użyciem fal radiowych, które, ograniczając niektóre z jej zastosowań, pomogą chronić prywatność. Na nic jednak zdadzą się same akty prawne, jeżeli brak będzie odpowiedniej wiedzy. Tym, co może ocalić nas przed utratą kontroli nad naszymi danymi osobowymi i prywatnością są wyedukowani użytkownicy nowych technologii, takich jak RFID, świadomi zasad ich funkcjonowania i zagrożeń jakie niosą one ze sobą.