

Łukasz Kamieński

Zachipowana rzeczywistość?

Kultura i Polityka : zeszyty naukowe Wyższej Szkoły Europejskiej im. ks.
Józefa Tischnera w Krakowie nr 16, 114-126

2014

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach
dozwolonego użytku.

ZACHIPOWANA RZECZYWISTOŚĆ?¹

Abstrakt

Technologia chipów RFID staje się standardową metodą znakowania towarów w przemyśle, handlu, logistyce i siłach zbrojnych, szybko zastępując przestarzały kod kreskowy. Chipy S-RFID wykorzystujące lokalizację satelitarną umożliwiają dokładną lokalizację oznakowanego obiektu w czasie niemal rzeczywistym. Coraz częściej pojawiają się fantastycznonaukowe w duchu pomysły i wizje znakowania ludzi implantowanymi biochipami RFID nowej generacji, które umożliwią, na przykład, odnajdywanie porwanych ludzi, śledzenie miejsca pobytu pewnych kategorii osób (na przykład zagubionych pacjentów chorych na alzheimera) czy żołnierzy na polu bitwy. Zagadnienie „etykietowania” ludzi budzi poważne kontrowersje i dylematy etyczne związane z dyskusją na temat „cyfrowego społeczeństwa nadzoru”, Orwellońskiego państwa Wielkiego Brata, ryzyka cyborgizacji oraz antynomii wolność/prawo do prywatności *versus* bezpieczeństwo.

Słowa kluczowe

technologia RFID, znakowanie i identyfikacja, biochipy, wojsko, społeczeństwo chipowe



„Prawdziwa wartość technologii RFID leży nie w tym, co dzisiaj można dzięki niej osiągnąć, ale w tym, co będzie możliwe w przyszłości” (Estevez 2005: 9).

W lipcu 2014 roku media doniosły, że naukowcy z amerykańskiego Massachusetts Institute of Technology oraz firmy MicroCHIPS stworzyli implantowanego antykoncepcyjnego chipa, pozwalającego zapobiegać ciąży przez 16 lat poprzez regularne wydzielanie odpowiednich

* **dr Łukasz Kamiński** – adiunkt w Instytucie Amerykanistyki i Studiów Polonijnych Uniwersytetu Jagiellońskiego, specjalizuje się w strategicznych aspektach stosunków międzynarodowych oraz historii i teorii wojny. Autor monografii *Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych* (2009), *Farmakologizacja wojny. Historia narkotyków na polu bitwy* (2012) oraz *Nowy wspaniały żołnierz. Rewolucja biotechnologiczna i wojna w XXI wieku* (2014).

¹ Praca naukowa finansowana ze środków budżetowych na naukę w latach 2010–2014 jako projekt badawczy *Nowe technologie i ich wpływ na zmianę oblicza wojny. Science fiction czy przyszłość zachodniego sposobu prowadzenia wojny?* (N N116 389539). Rozwinięcie myśli zawartych w tym artykule, w tym na temat wykorzystania chipów przez amerykańskie siły zbrojne, można przeczytać w: Ł. Kamiński (2014), *Nowy wspaniały żołnierz. Rewolucja biotechnologiczna i wojna w XXI wieku*, Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego: 225–246.

dawek hormonu (30 mikrogramów lewonorgestrelu dziennie). Chip można włączać i wyłączać w dowolnej chwili za pomocą pilota (Kinkead 2014). Urządzenie – ta specyficzna cyborgiczna metoda kontroli płodności – wkrótce wkroczy w fazę testów klinicznych i być może już w roku 2018 będzie dostępne na rynku. Zanim jednak tego typu biochipy wpływające na funkcje życiowe organizmu i zachowanie człowieka zaczną się upowszechniać, na popularności zyskają i upowszechnią się znacznie prostsze ludzkie chipy radiowe RFID służące głównie identyfikacji.

Od chipów RFID do S-RFID

RFID (*radio-frequency identification*) jest techniką identyfikacji wykorzystującej fale radiowe do przesyłania danych. W użyciu znajdują się dwa rodzaje etykiet RFID: aktywne i pasywne. Te pierwsze są zasilane za pomocą wmontowanych baterii, dlatego mają krótką żywotność, ale szerszy zasięg i większą pojemność zapisu danych na mikrochipie, są jednak drogie, kosztują bowiem 50–100 dolarów za sztukę. Te drugie są zasilane za pomocą energii przekazywanej przez czytnik za pośrednictwem fal radiowych, mają mniejszą pojemność zapisu danych i mogą być odczytane tylko ze stosunkowo małej odległości, są za to tanie – kosztują 10–60 centów za sztukę. Etykiety aktywne są odczytywane automatycznie za pomocą urządzeń zainstalowanych w różnych punktach, natomiast etykiety pasywne odczytuje się za pomocą ręcznych czytników zbliżeniowych. Pasywne RFID są aktywowane przez sygnał radiowy wysyłany przez czytniki. W zależności od częstotliwości fal radiowych chipy mają zasięg od kilkudziesięciu centymetrów (120–150 kHz) do nawet 200 metrów (3,1–10 GHz), mają różne rozmiary (zwykle około 2×2 lub 4×4 cm), są wyposażone w antenę w postaci małego zwoju, za pomocą której odbierają i przesyłają sygnały radiowe. Mają też przypisany unikatowy kod identyfikacyjny (zwykle 64-bitowy), który odebrany przez czytnik stanowi klucz dostępu do danych na temat oznakowanego obiektu. Odczytanie kodu może powodować na przykład wyświetlenie profilu osoby lub karty towaru albo pozytywną autoryzację i otwarcie drzwi.

Początki technologii RFID sięgają II wojny światowej, kiedy Brytyjczycy, chcąc ułatwić pierwszym systemom radarowym odróżnianie przyjaciół od wrogów, zaczęli w swoich i sojuszniczych samolotach instalować przekaźniki radiowe. Pierwsze chipy radiowe stworzono w latach 60. – znalazły one zastosowanie do znakowania ciężarówek, uprawnionych do wjazdu na teren kompleksu wojskowego Los Alamos

National Laboratory. Od lat 90., wraz z miniaturyzacją elektroniki, spadkiem ceny chipów oraz powstawaniem rozbudowanych komputerowych baz danych, chipy RFID zaczęły się upowszechniać w siłach zbrojnych, a w 1993 roku amerykańska armia rozpoczęła wdrażanie aktywnych metek RFID. Głównym bodźcem wprowadzania ich do użycia były duże problemy ze sprawnością łańcucha dostaw, jakie ujawniła wojna w Zatoce Perskiej. Intensywność i szybkość działań oraz ogromna liczba przesyłanych towarów spowodowały, że armia nie była w stanie precyzyjnie śledzić transportów sprzętu i zaopatrzenia, a tym samym zapewnić dowództwu dokładnych informacji na ich temat. Słynna amerykańska firma handlowa Wal-Mart wyznaczyła styczeń 2005 roku jako termin, od kiedy jej 130 najważniejszych dostawców musiało za pomocą pasywnych etykiet RFID znakować wszystkie dostawy towarów przesyłanych do dwóch głównych centrów dystrybucyjnych firmy w Teksasie. Dosłownie idąc w ślad za gigantem sieci supermarketów, Pentagon postanowił wykorzystać identyfikację RFID na jeszcze szerszą niż dotychczas skalę w celu śledzenia i kontrolowania dostaw wojskowych zwłaszcza w strefie działań zbrojnych. Również od stycznia 2005 roku firmy dostarczające części zamienne, urządzenia oraz ubrania do magazynów wojskowych (*depots*) w Pensylwanii i Kalifornii zostały zobowiązane do znakowania zawartości każdej palety za pomocą pasywnej etykiety RFID (Erwin 2004: 19; Ames 2005: 1, 8).

W związku z tym Departament Obrony stał się największym na świecie użytkownikiem technologii RFID, posiadającym najbardziej rozbudowaną globalną sieć zautomatyzowanego śledzenia przesyłek (Estevez 2005: 5; Moore i in., 2006). Inteligentna technologia znakowania niezwykle udoskonaliła zarządzanie dostawami w ramach złożonego systemu *Total Asset Visibility* (TAV), dzięki czemu w przeddzień rozpoczęcia operacji w Iraku, w marcu 2003 roku, Pentagon mógł w każdej chwili śledzić 250 tysięcy kontenerów (*Military Orders RFID Tracking*, 2002).

Aktywne i pasywne RFID umożliwiają śledzenie informacji na temat tego, gdzie dany obiekt wcześniej się znajdował, to znaczy kiedy po raz ostatni został odczytany, ale nie pozwalają monitorować tego, gdzie znajduje się w danej chwili. Udoskonalenie technologii i połączenie etykiet RFID z urządzeniem GPS oraz komunikacją satelitarną w postaci 3G RFID w/SATCOM (*Third Generation Radio Frequency Identification with Satellite Communications*) pozwala już jednak na śledzenie ruchu przesyłki w czasie niemal rzeczywistym bez potrzeby tworzenia specjalnej lokalnej infrastruktury, a więc anten i czytników odbierających i przesyłających dane. Za pomocą komunikacji satelitarnej chipy

S-RFID przekazują informacje o lokalizacji danej przesyłki do centrów kontroli dostaw. Powstaje w pełni zautomatyzowany system logistycznego zarządzania łańcuchami dostaw towarów.

Narodziny chipowych społeczeństw

Etykiety RFID, które w niedalekiej przyszłości zastąpią kody kresowe, stały się wyjątkowo popularne, a ich sprzedaż w 2012 roku wzrosła o 17% w porównaniu z rokiem wcześniejszym, osiągając wartość 7,67 miliarda dolarów (*RFID Market* 2012). Za ich pomocą znakowane są nie tylko towary w supermarketach, książki w bibliotekach, karty płatnicze (*smart-cards*), różnego rodzaju karty identyfikacyjne, ale są one również wykorzystywane w celu kontrolowania postępu prac na liniach produkcyjnych, śledzenia bagaży na lotnisku, ewidencjonowania wyposażenia, pobierania opłat (szczególnie popularne na wyciągach narciarskich) oraz rejestracji czasu pracy. Etykiety pełnią też funkcję popularnych „kart dostępu”, pozwalają bowiem na szybką identyfikację osób uprawnionych na przykład do wejścia do konkretnego pomieszczenia lub dostępu do chronionych danych. Nie trzeba wpisywać żadnych kodów czy haseł ani przejeżdżać kartą po czytniku. Dane są automatycznie odczytywane i weryfikowane. Skradzione samochody, które oznakowano za pomocą technologii RFID, można znacznie łatwiej odnaleźć i odzyskać (Swedberg 2005).

W 1998 roku Malezja jako pierwszy kraj na świecie wprowadziła nowe e-paszporty wyposażone w chipy RFID, które nie tylko zawierały dane osobowe posiadacza, ale także zapisywały dokładną historię jego podróży (datę i miejsce przekroczenia granicy). Za przykładem Malezji podażyły inne państwa (USA w 2006 roku), wprowadzając paszporty z wbudowanym mikroprocesorem zawierającym dane biometryczne oraz znacznik RFID. W przyszłości standardowo wszystkie dokumenty identyfikacyjne będą „inteligentnymi dokumentami tożsamości” wyposażonymi w mikrochipy RFID (zob. Smith i in., 2011).

Po 2004 roku niektóre szkoły, między innymi w Danii, Japonii, Korei Południowej, Stanach Zjednoczonych i Wielkiej Brytanii, zaczęły wprowadzać programy metkowania ubrań, plecaków i legitymacji uczniów w celu monitorowania ich obecności w szkole (w salach lekcyjnych, toaletach i stołówkach), zapobiegania pojawieniu się osób nieuprawnionych i ewentualnych prób porwań dzieci (Williams 2007). Przykładowo władze japońskiej prefektury Osaka wyposażyły uczniów wszystkich publicznych szkół podstawowych w etykiety identyfikacji elektronicznej, a jedną z obietnic wyborczych Partii Liberalno-

-Demokratycznej podczas kampanii w 2008 roku było „upowszechnienie systemów monitorowania dzieci za pomocą technologii RFID” (Ema i Fujigaki 2011: 134). Inny przykład to Tucson Unified School District w amerykańskim stanie Arizona, gdzie w 2006 roku testowano oparty na technologii RFID-GPS system BusPass, monitorujący wsiadanie i wysiadanie uczniów ze szkolnego autobusu (O’Connor 2006). Docelowo rodzice będą otrzymywali na telefon komórkowy SMS, że ich dziecko właśnie przyszło lub wyszło ze szkoły. Niezwykle pomocne może się także okazać chipowanie osób w podeszłym wieku cierpiących na demencję i chorobę Alzheimera, które na wypadek zgubienia się można będzie szybko odnaleźć.

Masowe wykorzystanie technologii RFID wiąże się również ze znakowaniem zwierząt hodowlanych za pomocą chipowych zawieszek i implantów. Praktyka ta stała się popularna od końca lat 90., szczególnie w okresie epidemii BSE (choroby szalonych krów), jako wyjątkowo szybki sposób identyfikacji i użyteczny mechanizm zarządzania stadami. Od początku XXI wieku upowszechniło się ponadto znakowanie zwierząt domowych, dzięki czemu można łatwo namierzyć zaginione psy i koty. Skoro zaś możliwe jest skuteczne metkowanie zwierząt, to podobna metoda może być stosowana również u ludzi. Chip wielkości ziarenka ryżu umieszczony w małej szklanej tubie najczęściej wszczepia się w ramię, dłoń lub kark. Pierwszą osobą, która nosiła w sobie implantowany chip RFID, był profesor cybernetyki Kevin Warwick z Uniwersytetu w Reading w Wielkiej Brytanii. W sierpniu 1998 roku w ramach projektu *Cyborg 1.0* na dziewięć dni wszczepił go sobie do lewego ramienia. Czytniki mogły śledzić jego ruchy w budynku uniwersyteckim, a komputer, jak relacjonował, „mówił mi cześć, gdy wchodziłem przez główne drzwi, włączał oświetlenie na korytarzu i kiedy tylko się zbliżałem, automatycznie otwierał drzwi do laboratorium” (2009: 123). Wraz z dalszą miniaturyzacją elektroniki etykietowanie ludzi będzie coraz tańsze i prostsze, a tym samym stanie się bardziej popularne.

W 2004 roku ekskluzywny klub nocny Baja Beach w Barcelonie, a potem także jego filia w Rotterdamie, zaoferował swoim specjalnym klientom usługę wszczepienia chipa RFID pozwalającego na szybką identyfikację, wstęp do strefy dla VIP-ów oraz wygodne i bezgotówkowe zamawianie drinków (czytnik rozpoznaje klienta i automatycznie dopisuje kolejną pozycję do jego rachunku). Dzięki tej wyjątkowej biochipowej karcie VIP dostępnej za 125 euro klienci mogli przychodzić do klubu bez pieniędzy i bez dowodów tożsamości (Purohit 2004). Jak napisała dziennikarka CNN, która, przygotowując reportaż, sama poddała się na próbę chipowej opłacie członkowskiej, „przypominało to udział w dziwacznym eksperymencie społecznym albo w kiepskim

filmie o Jamesie Bondzie” (Curnow 2004). Sporo trudności sprawiło jednak później lekarzom usunięcie z jej ciała tej elektronicznej karty klubowej.

W 2004 roku mikrochipy wszczepiono prokuratorowi generalnemu Meksyku Rafaelowi Macedo de la Concha i 160 członkom jego urzędu. Oficjalnie w celu zabezpieczenia dostępu do specjalnie chronionych pomieszczeń i wrażliwych danych w siedzibie prokuratury, chociaż spekulowano, że być może także jako zabezpieczenie na wypadek porwania (Weissert 2004; Bly 2005: 60). Zresztą wśród zamożnych mieszkańców Meksyku oraz niektórych innych państw Ameryki Łacińskiej popularna stała się „chipowa polisa ubezpieczeniowa”: implanty RFID zintegrowane z nadajnikami satelitarnymi umożliwiające lokalizację na wypadek porwania dla okupu. W 2004 roku koszt takiej usługi wynosił jednorazowo 4 tysiące dolarów oraz ponad 2 tysiące dolarów rocznej opłaty. Ponieważ w latach 2004–2007 liczba porwań w Meksyku wzrosła o 40% i według nieoficjalnych statystyk w 2007 roku uprowadzonych mogło zostać nawet 7 tysięcy osób, takie chipowe zabezpieczenie szybko zaczęło zdobywać popularność (Rosenberg 2008).

W 2004 roku amerykańska Agencja do spraw Żywności i Leków (FDA) wydała zgodę na wprowadzenie na rynek produkowanego przez firmę VeriChip Corporation (po połączeniu ze Steel Vault Corporation w 2009 roku funkcjonująca jako PositiveID Corporation) implantowanego biochipa identyfikacyjnego o nazwie VeriChip. Tym samym FDA zezwoliła na chipowanie w celach medycznych ludzi powyżej 12. roku życia, a zwłaszcza pacjentów z cukrzycą, po udarze, cierpiących na demencję, alzheimera oraz po transplantacji organów.

Wielką zaletą ludzkich biochipów będzie to, że w nagłych sytuacjach, na przykład w razie wypadku, lekarz zeskanuje pacjenta i będzie miał natychmiastowy dostęp do jego danych medycznych. Biochipy mogą więc dosłownie ratować życie, ułatwiając także lokalizowanie zaginionych i zasypanych w wyniku katastrof. Do października 2007 roku 900 amerykańskich szpitali zarejestrowało się w systemie identyfikacji pacjenta VeriMed firmy VeriChip, który „błyskawicznie i dokładnie identyfikuje osoby przybywające do oddziałów ratunkowych, a z którymi nie ma kontaktu werbalnego” (*VeriChip Corporation Adds...*, 2007). W przyszłości nie będą potrzebne żadne biometryczne paszporty ani dowody osobiste, ponieważ osoby uzyskujące pełnoletniość będą otrzymywały „implantowaną obywatelską identyfikację elektroniczną”. Nie trzeba będzie posiadać ani nosić żadnych dokumentów, bo „zindeksowane” ciało będzie zintegrowane z chipowym dokumentem. Można pójść jeszcze dalej i zamiast biochipowych dowodów osobistych wyobrazić sobie znakowanie noworodków za pomocą elektronicznej

metki identyfikacyjnej. W gruncie rzeczy niektóre kliniki już od dawna obręczają dzieci tuż po porodzie za pomocą opasek z RFID, gdyż jest to znacznie pewniejszy sposób zapobiegania przypadkowej zamianie dzieci niż tradycyjnie stosowane opaski. Na przykład metodę tę już w 2001 roku wdrożył kalifornijski Szpital Dziecięcy Lucile Packard w Palo Alto (Collins, 2005).

Kontrowersje

W niedalekiej przyszłości wszczepianie biochipów będzie coraz bardziej popularne, w szczególności wraz z ich postępującą miniaturyzacją. W związku z tym w szerszym kontekście społecznym pojawiają się obawy i wątpliwości natury etycznej związane głównie z prawem do prywatności oraz umacnianiem się „społeczeństwa nadzoru”. Krytycy zwracają uwagę na niebezpieczeństwo nieustannej kontroli, od której nie sposób będzie uciec, bowiem chipowanie przekształci ludzi w nosicieli ich własnych elektronicznych profili, których nie będą mogli ukryć, zgubić, wyrzucić, nie będą mogli odmówić pokazania dowodu osobistego, ponieważ zawsze będą identyfikowalni i identyfikowani przez odpowiednie służby. W takim „cyfrowym społeczeństwie nie ma się *gdzie* ukryć, *nic* też nie pozostaje prywatne” (Michael i Michael 2010: 13). Społeczeństwo będzie automatycznie, na bieżąco i ciągle kontrolowane przez czytniki, a jeśli chipy będą połączone z satelitami, co niewątpliwie stanie się standardem, to bardzo trudno będzie ukryć miejsce swojego pobytu. Być może niektórym rodzicom taki system „opieki rodzicielskiej” będzie dawał poczucie czuwania nad bezpieczeństwem dzieci, jednak w wypadku dorosłych sprawa jest wyjątkowo kontrowersyjna. O telefonie komórkowym, przysłowiowej „elektronicznej smyczy”, mówi się, że zniszczył prawo do prywatności i możliwość „ucieczki” od społeczeństwa, zwłaszcza od pracy. Mimo wszystko jednak telefon możemy wyłączyć albo nie odebrać połączenia. W wypadku implantowanych biochipów nie będzie takiej możliwości, chyba że zdecydujemy się je usunąć, chociaż taki akt może oznaczać pogwałcenie prawa. Ponadto istnieje poważny problem związany z bezpieczeństwem danych, które mimo szyfrowania i blokowania można wykraść. Hakerzy udowodnili, że mogą nie tylko przechwycić sygnał wysyłany przez chip, ale również sklonować go, a tym samym skopiować unikatowy kod dostępu do powiązanej z nim tożsamości zmagazynowanej w przestrzeni wirtualnej (Szczys 2011). Jeśli etykiety nie zostaną „zamknięte”, co jest częstą praktyką, ponieważ umożliwia nadpisywanie i zmianę danych na chipach, wówczas

hakerzy mogą zrobić z nimi niemal wszystko. Mogą na przykład zamienić etykiety produktów – skopiować dane z RFID taniego wina i wkleić je do RFID drogiego trunku albo do etykiety cenowej, powiedzmy żółtego sera, załadować kod karty-klucza do drzwi, tak że za pomocą sera można będzie dostać się do pomieszczenia (Newitz 2006). Świat RFID przypomina Internet we wczesnych latach jego rozwoju, kiedy nikt na poważnie nie myślał o zagrożeniach ani zabezpieczeniach. Ponieważ nie sposób zapobiec upowszechnianiu się mikrochipów radiowych, w przyszłości będą powstawać zaawansowane systemy ich zabezpieczeń i techniki szyfrowania danych.

Pisarka fantastyki naukowej Elizabeth Moon zainicjowała publiczną debatę na temat tego, czy dobrym pomysłem byłoby powszechne elektroniczne znakowanie dzieci tuż po urodzeniu. Na antenie radia BBC powiedziała: „Nalegałabym, by każdy posiadał umieszczony na stałe unikatowy dokument tożsamości – coś w rodzaju kodu kreskowego – implantowany chip, który zapewniałby prosty, szybki i tani sposób identyfikowania jednostek” (Neal 2012). Na początek może mało inwazyjna wizja, jaką nakreślił William Mitchell – podczas rutynowych wizyt u stomatologa chipy RFID można umieszczać w płom-bach, a potem dzięki nim dokonywać zakupów, otwierać drzwi etc. (2003: 77).

W społeczeństwie przyszłości, w którym „etykietowanie” obywateli będzie normą, odczytanie chipa umożliwi dostęp do profilu danej osoby, który połączony z różnymi bazami danych będzie zawierać, oprócz informacji biometrycznych, także wiedzę na temat chorób, grupy krwi, genotypu, karalności, nałogów, sympatii politycznych, historii miejsc pobytu, spotkań z podejrzanymi osobami etc. Państwo „Wielkiego Brata” stanie się instytucją stosującą ponowoczesną, elektroniczną, zautomatyzowaną, ciągłą i prowadzoną w czasie rzeczywistym lokalizację, identyfikację oraz nadzór, którą M.G. i Katina Michaelowie nazywają *Überveillance* (2010: 9–16). Koncepcja ta opiera się na zaproponowanym w 1988 roku przez Rogera Clarke’a terminie *dataveillance*, oznaczającym „konsekwentne wykorzystanie systemów danych osobowych w celu badania lub monitorowania działań jednej lub wielu osób” (1988: 499). Jak piszą Michaelowie, „to, co w świecie *dataveillance* jest statyczne lub nieciągłe, dzięki *Überveillance* staje się ciągłe i osadzone” (2010: 9). „Ciągłe” w znaczeniu nieprzerwanej zautomatyzowanej lokalizacji i identyfikacji w czasie rzeczywistym i „osadzone” w znaczeniu implantowania do ciała. *Überveillance* jest też wszechogarniające, bowiem dostarcza informacji na temat tego, „kto” (identyfikacja), „gdzie” (lokalizacja), „kiedy” (czas), ale potencjalnie również „dlaczego” (motywacja), „z jakim skutkiem” (efekt), a nawet

„jak” (metoda/plan). Na ryzyko chipowej inwigilacji zwróciły także uwagę Katherine Albrecht i Liz McIntyre w książce pod wymownym tytułem: *SpyChips: How Major Corporations and Government Plan to Track Your Every Move with RFID* (2005). Ich zdaniem, gdy każdy towar, jaki kupujemy, będzie wyposażony w RFID, korporacje zdobędą totalną wiedzę na temat swoich klientów, dzięki czemu reklama stanie się niesłychanie celowa i spersonalizowana. Niemal każdy ruch ludzi będzie śladowany w czasie rzeczywistym niczym w Orwellovskim świecie *Roku 1984*. Charlie Schmidt ujął rzecz następująco: „Firmy takie jak Gillette będą monitorowały używanie ich produktów w twoim domu. Gdy wyrzucisz jedno ostrze do śmieci, nowe będzie już w drodze” (za Albrecht i McIntyre 2005: 85). Albrecht i McIntyre piszą: „Czytniki ukryte w drzwiach, ścianach, wystawach i podłogach mogą przeszukiwać chipy RFID ukryte w twoich ubraniach i innych przedmiotach osobistych, by ustalić twój wiek, płeć i preferencje” (2005: 3). Te same skanery, które są wykorzystywane do skanowania towarów w sklepach, będą mogły być stosowane do identyfikowania klientów. Zachipowanie pracowników umożliwi całkowite nadzorowanie ich wydajności. Firma Amazon już niemal idealnie zsynchronizowała pracę ludzi i maszyn – każdy pracownik przygotowujący zamówione towary do wysyłki jest wyposażony w czujnik. „Jeżeli pracownik zbyt wolno porusza się między półkami, włącza się alarm, a przełożony dostaje na bieżąco informacje o «szybkości» swojego podwładnego”. Jeden z pracowników wyznał dziennikarzowi BBC: „Jesteśmy jak maszyny, roboty. Choć trzymaliśmy nadajnik w rękach, czuliśmy się, jakbyśmy mieli go wszczepionego w siebie” (*BBC demaskuje...*, 2013). W przyszłości implantowane chipy zastąpią zewnętrzne czujniki...

Zachipowany żołnierz przyszłości

W październiku 2011 roku firma PositiveID ogłosiła, że podpisała umowę na dostawę biochipów dla izraelskiej armii, które, jak niejasno stwierdzono, mają służyć „przygotowaniu na wypadek katastrof i zarządzaniu w sytuacjach kryzysowych” (Sterling 2011). Jednym słowem, izraelskie siły zbrojne na poważnie zainteresowały się technologią implantowania żołnierzy.

Od dłuższego czasu amerykańska Agencja Zaawansowanych Obronnych Projektów Badawczych (DARPA) finansuje kilka projektów badawczych w ramach programu służącego udoskonaleniu technologii RFID. W niedalekiej przyszłości „metkowanie” amerykańskich żołnierzy za pomocą biochipów S-RFID stanie się normą. Zastosowanie tej

metody znakowania jako biotechnologicznego zamiennika wojskowych nieśmiertelników w celu identyfikacji zaginionych i zabitych wydaje się pragmatyczne i uzasadnione. Chipy mogą też uratować życie wielu żołnierzom, pomagając w ich szybkim namierzeniu i dając lekarzom błyskawiczny dostęp do ważnych danych medycznych (grupy krwi, ewentualnych chorób, przyjmowanych leków, uczuleń etc.). A jednak inne zastosowanie bioelektronicznych metek będzie miało bardziej doniosłe znaczenie dla sił zbrojnych: automatyczna elektroniczna identyfikacja i lokalizacja oddziałów w czasie rzeczywistym. Ciało żołnierza przesyłające dane automatycznie i na dystans będzie można zlokalizować z dużą dokładnością. Chipy umożliwią idealny mechanizm kontroli i zarządzania personelem podczas operacji, a dowództwo będzie dysponowało wszystkimi niezbędnymi danymi na temat każdego żołnierza. Znaczniki S-RFID pozwolą na jeszcze lepszą świadomość sytuacyjną w postaci aktualizowanych na bieżąco cyfrowych map lokalizacji własnych sił: ludzi, sprzętu i robotów.

Todd Guggisberg z U.S. Army Command and General Staff College prognozuje już nie fantastycznonaukowy scenariusz: „gdy żołnierze wysiadają z samolotu C-17 Globemaster w afgańskim Bagramie, RFID automatycznie uaktualnia dane osobowe jednostki, aktywizuje konto przydziału zadań, [...] sprawdza aktualność danych kontaktowych w razie wypadku oraz grupowe ubezpieczenie na życie [...]” (2011: 18). RFID-GPS wszczepione w ramię lub kark spowoduje, że żołnierz będzie widoczny zawsze i wszędzie, będzie w pełni osiągalny i wykrywalny.

123

Konkluzja

Zachipowani ludzie staną się bioniczni nie tylko dlatego, że fragment świata techniki – mikrochip – będzie na długi czas (być może w przyszłości na całe życie) obecny w ich ciałach, ale także dlatego, że staną się elementem elektronicznych sieci, poprzez chipy S-RFID-GPS ich ciała będą się komunikować w czasie rzeczywistym z rozbudowanymi systemami identyfikacji, śledzenia, kontroli, zarządzania i przeszukiwania... Chipowanie będzie równocześnie wyraźnym przykładem „samokontrolowania i samokodowania pozwalających na szybszą ścieżkę dostępu” (Sparke 2008: 147). Automatyczna identyfikacja umożliwi błyskawiczne i łatwe wchodzenie do strzeżonych budynków i pomieszczeń, odprawę lotniczą, przekraczanie granic, przejazd autostradą, zakupy etc. Za pomocą fal radiowych ludzkie ciała połączone z systemami komputerowymi, a więc z wirtualną rzeczywistością

stością, staną się nie tylko bardziej bioniczne, ale też – by przywołać sformułowanie Emily Martin – bardziej „elastyczne” (1994). Na szerszą skalę bardziej „elastyczni” i bioniczni będą w pierwszej kolejności, jak się wydaje, amerykańscy żołnierze.

Bibliografia

- Albrecht, Katherine i McIntyre, Liz (2005), *SpyChips: How Major Corporations and Government Plan to Track Your Every Move with RFID*, Nashville, TN: Nelson Current.
- Ames, Ben (2005), *Pentagon Continues to Push on Suppliers to Use RFID*, „Military and Aerospace Electronics”, 16 (9), s. 1, 8.
- BBC demaskuje warunki pracy w Amazonie (2013), „Onet”, <http://technowinki.onet.pl/biznes-i-finance/bbc-demaskuje-warunki-pracy-w-amazonie/h8p03> [2 stycznia 2013].
- Bly, Robert W. (2005), *The Science in Science Fiction: 83 SF Predictions That Became Scientific Reality*, Dallas, TX: BenBella Books Inc.
- Clarke, Roger (1988), *Information Technology and Dataveillance*, „Communications of the ACM”, 32 (5), s. 498–512.
- Collins, Jonathan (2005), *RFID Delivers Newborn Security*, „RFID Journal”, <http://www.rfidjournal.com/articles/view?1372> [5 czerwca 2014].
- Curnow, Robyn (2004), *The Price to Pay for VIP Status*, „CNN”, <http://edition.cnn.com/2004/TECH/10/05/spark.bajabeach> [4 lipca 2014].
- Ema, Arisa i Fujigaki, Yuko (2011), *How Far Can Child Surveillance Go? Assessing the Parental Perceptions of an RFID Child Monitoring System in Japan*, „Surveillance and Society”, 9 (1–2), s. 132–148.
- Erwin, Sandra (2004), *Pentagon Officials Refining Requirements for Smart Tags on Military Shipments*, „National Defense Magazine”, 89 (611), s. 19–20.
- Estevez, Alan (2005), *RFID Vision in the DOD Supply Chain*, „Army Logistician. Professional Bulletin of United States Army Logistics”, 37 (3), s. 5–9.
- Guggisberg, Todd (2011), *How RFID and Smartphones Will Help Revolutionize Army Sustainment*, „Army Sustainment”, 43 (6), s. 18.
- Kinlead, Gwen (2014), *A Contraceptive Implant with Remote Control*, „MIT Technology Review”, 4 July 2014, <http://www.technologyreview.com/news/528121/a-contraceptive-implant-with-remote-control> [26 lipca 2014].
- Martin, Emily (1994), *Flexible Bodies: Tracking Immunity in American Culture from the Days of Polio to the Age of AIDS*, Boston: Beacon Press.
- Michael, M.G., Michael Katina (2010), *Toward a State of Überveillance*, „IEEE Technology and Society Magazine”, 29 (2), s. 9–16.
- Military Orders RFID Tracking (2002), „RFID Journal”, <http://www.rfidjournal.com/articles/view?186> [5 czerwca 2014].
- Mitchell, William J. (2003), *Me++: The Cyborg Self and the Networked City*, Cambridge, MA: The MIT Press.

- Moore, M.R., Buckner M.A., Crutcher R.I., Ewing P.D., Smith S.R. (2006), *Total Asset Visibility: RFID Efforts Support Seamless Asset Tracking for the 21st Century Army*, „Military Technology”, 30 (8), s. 36–41.
- Neal, Meghan (2012), „Human Barcode” Could Make Society More Organized, but Invades Privacy, Civil Liberties, „New York Daily News”, <http://www.nydaily-news.com/news/national/human-barcode-society-organized-invades-privacy-civil-liberties-article-1.1088129> [18 lipca 2014].
- Newitz, Annalee (2006), *The RFID Underground*, „Wired”, <http://www.wired.com/wired/archive/14.05/rfid.html> [20 lipca 2014].
- O'Connor, Mary Catherine (2006), *Tucson Schools Considering RFID BusPass*, „RFID Journal”, <http://www.rfidjournal.com/articles/view?2383> [5 czerwca 2013].
- Purohit, Chetna, *Technology Gets under Clubbers' Skin* (2004), „CNN”, <http://edition.cnn.com/2004/WORLD/europe/06/09/spain.club/index.html> [4 lipca 2014].
- RFID Market (2012), IDTechEx, <http://www.idtechex.com/research/articles/rfid-market-reaches-7-67-billion-in-2012-up-17-from-2011-00004585.asp> [2 czerwca 2014].
- Rosenberg, Mica (2008), *Satellites Track Mexico Kidnap Victims with Chips*, „Reuters”, <http://www.reuters.com/article/2008/08/22/us-mexico-crime-chips-idUSN2041333820080822> [20 lipca 2014].
- Smith, Karen Louise, McPhail Brenda, Ferenbok Joseph, Tichine Alex, Clement Andrew (2011), *Playing with Surveillance: The Design of a Mock RFID-based Identification Infrastructure for Public Engagement*, „Surveillance and Society”, 9 (1–2), s. 149–166.
- Sparke, Matthew (2008), *Fast Capitalism/Slow Terror: Cushy Cosmopolitanism and Its Extraordinary Other*, [w:] Louise Amoore, Marieke de Goede (red.), *Risk and the War on Terror*, London: Routledge, s. 133–157.
- Sterling, Bruce (2011), *Verichip's Back – in Israel*, „Wired”, http://www.wired.com/beyond_the_beyond/2011/10/arphid-watch-verichips-back-in-israel [18 lipca 2014].
- Swedberg, Claire (2005), *Triple RFID Protection for Cars*, <http://www.rfidjournal.com/articles/view?1304> [2 czerwca 2014].
- Szczys, Mike (2011), *Passive RFID Tag Cloning*, „Hack a Day”, <http://hackaday.com/2011/09/30/passive-rfid-tag-cloning> [14 lipca 2014].
- VeriChip Corporation Adds More Than 200 Hospitals to Its VeriMed Patient Identification System at the American College of Emergency Physicians (ACEP) Conference (2007), „BusinessWire”, <http://www.businesswire.com/news/home/20071011005335/en/VeriChip-Corporation-Adds-200-Hospitals-VeriMed-Patient> [23 lipca 2014].
- Warwick, Kevin (2009), *Augmenting Human Beings*, [w:] Peter Healey, Steve Rayner (red.), *Unnatural Selection: The Challenges of Engineering Tomorrow's People*, London–Sterling, VA: Earthscan, s. 121–126.
- Weissert, Will (2004), *Microchips Implanted in Mexican Officials*, „NBC News”, http://www.nbcnews.com/id/5439055/ns/technology_and_science-tech_and_gadgets/t/microchips-implanted-mexican-officials/#.Ua9389g4y48 [20 lipca 2014].
- Williams, Christopher (2007), *Schoolkid Chipping Trial “A Success”*, „The Register”, http://www.theregister.co.uk/2007/10/22/kid_chipping_doncaster_go [12 lipca 2014].



Łukasz Kamiński – an assistant professor at the Institute of American Studies and Polish Diaspora of the Jagiellonian University, Kraków. An expert in the areas of the strategic aspects of international relations and the history and theory of war. The author of the monograph *Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych* (2009), as well as of *Farmakologizacja wojny. Historia narkotyków na polu bitwy* (2012) and *Nowy wspaniały żołnierz. Rewolucja biotechnologiczna i wojna w XXI wieku* (2014).

Abstract

The RFID chip technology is becoming a standard method for product labelling in industry, trade, logistics and armed forces, quickly replacing the outdated bar codes system. S-RFID chips, using satellite locations, allow for identification of the precise location of a labelled product in almost real-time. There are ever more science fiction-like concepts and ideas of labelling people with implanted, new-generation RFID biochips which make it possible, among others, to find kidnapped people, pinpoint the exact location of certain groups of people (e.g. lost Alzheimer's patients) or soldiers on a battlefield. Being highly controversial, the issue of "labelling" people poses ethical dilemmas relating to the debate on "a digital surveillance society," Orwell's Big Brother's state, the risk of cyborgization, and the dichotomy between freedom/right to privacy and security.

126

Keywords

RFID technology, labelling and identification, biochips, armed forces, chip society