

Polacy pod okiem kamer

Każda operacja kartą płatniczą czy połączenie telefoniczne zostawia ślad. Przeciętny Polak codziennie zostawia ich około 30. Dzięki temu operatorzy komórkowi i banki mają już informacje o prawie wszystkich dorosłych Polakach. Nasze dane zbiera też państwo, dostawcy Internetu i stacje benzynowe.

W efekcie statystyczny Polak figuruje już w przynajmniej kilkunastu bazach. Ich liczba przyrasta, bo firmy potrzebują więcej informacji o klientach.

Sami jednak równie chętnie ujawniamy informacje o sobie. Na portalach społecznościowych, takich jak Nasza-Klasa, Grono czy Golden Line, upubliczniło je 13 - 14 mln osób.

Przed inwigilacją coraz trudniej uciec. W przeciętnym polskim hipermarkecie klientów śledzi ok. 60 kamer.

Nowoczesne systemy dają ogromne możliwości zdobywania wiedzy o ludziach. Pozwala to firmom dopasować ofertę do klientów - mówi Andrzej Bochacz, prezes spółki Kamil dostarczającej systemy informatyczne do sklepów.

—d.e.

*Raport o elektronicznej
inwigilacji • B7 - 10
komentarz • A2*



Raport

o elektronicznej inwigilacji

Polacy są nieustannie pod czujnym okiem firm

TECHNOLOGIE | KAŻDEGO DNIA ZOSTAWIAMY OK. 30 ELEKTRONICZNYCH ŚLADÓW. Przechodząc pod kamerą, płacąc kartą, używając komórki czy zbierając punkty w programie lojalnościowym. Firmy inwestują duże pieniądze, aby zdobyć o nas coraz więcej informacji

PIOTR MAZURKIEWICZ

Wystarczy wyjść na ulicę, żeby znaleźć się w zasięgu kamer przemysłowych. Pod ich czujnym okiem zrobimy zakupy niezależnie od wielkości sklepu – nawet w najmniejszych, osiedlowych czeka na nas przynajmniej jedno szklane oko.

Pretekstem jest oczywiście ochrona przed kradzieżą, ale mają też inne zastosowanie. – Analizujemy dane, które w ten sposób uzyskujemy. Dzięki temu możemy lepiej określić najruchliwsze miejsca w sklepie pod kątem ustawiania tam np. stoisk promocyjnych – mówi Agnieszka Łukiewicz-Stachera, rzecznik sieci hipermarketów Real.

Ile kamer obserwuje klientów w trakcie zakupów – tego dokładnie nie wiadomo, a same sieci nie chcą podawać tego typu informacji. Zajmujące się instalowaniem takiego sprzętu firmy nieoficjalnie przyznają, że w przypadku jednego hipermarketu obserwuje nas ich nawet 60. Tylko w sklepach ogólnospożywczych ich liczba oscyluje w okolicach 300 tys. Dochodzą sklepy odzieżowe, obuwnicze i wiele innych, które także bacznie analizują takie dane. Liczone są nawet osoby przechodzące obok witryny. Wszystko czemuś służy – jedna z firm odzieżowych jedynie na podstawie udokumentowanej ka-

merami obserwacji, że wielu klientów na zakupy zabiera dzieci, zdecydowała o wprowadzeniu do sklepów specjalnej kolekcji właśnie dla nich przeznaczonych. Pomysł okazał się strzałem w dziesiątkę.

Ale na zakupach inwigilacja się nie kończy. Kartami otwieramy drzwi do miejsca pracy, korzystamy z telefonów – a każdy aparat można łatwo wysledzić i określić jego położenie z dokładnością nawet do kilkunastu

300 tys.

kamer zainstalowanych jest w polskich sklepach ogólnospożywczych

metrów. W naszym kraju ok. 20 mln osób używa komórek, więc przebieg ich dnia może zostać szczegółowo odtworzony. W Polsce banki prowadzą ok. 20 mln rachunków ROR, których historia wiele o nas mówi. Z kolei w Biurze Informacji Kredytowej zarejestrowanych jest 22 mln osób – za udostępnianie danych o naszych zaległościach banki płacą, a jeśli system wykazuje zaległości, możemy zapomnieć o kredycie.

Skrupulatnie zbierane dane mają wielką wartość. Firmy za-

pewniają, że są one chronione, ale nie jest tajemnicą, iż wiele baz jest wymienianych lub sprzedawanych. Wystarczy wysłać SMS w głosowaniu w jakimkolwiek telewizyjnym programie, by telefon przez kilka tygodni był bombardowany ofertami serwisów randkowych czy horoskopów.

– Widzimy oczywistą sprzeczność. Z jednej strony Polacy cierpią na prawdziwą obsesję prywatności. W budynkach nie ma spisów lokatorów, na domofonach nie ma tabliczek z nazwiskami, co jest normą we Francji – mówi prof. Maria Lewicka z Katedry Psychologii Społecznej Uniwersytetu Warszawskiego. – Z drugiej zaś wręcz chętnie wystawiamy się na inwigilację, chcemy instalować wszędzie kamery, dokładamy do portfeli kolejne karty, na które zbieramy punkty, wcześniej wypełniając kwestionariusz, gdzie sami podajemy wszystkie dane. To oczywisty paradoks, ale trudno to logicznie wytłumaczyć.

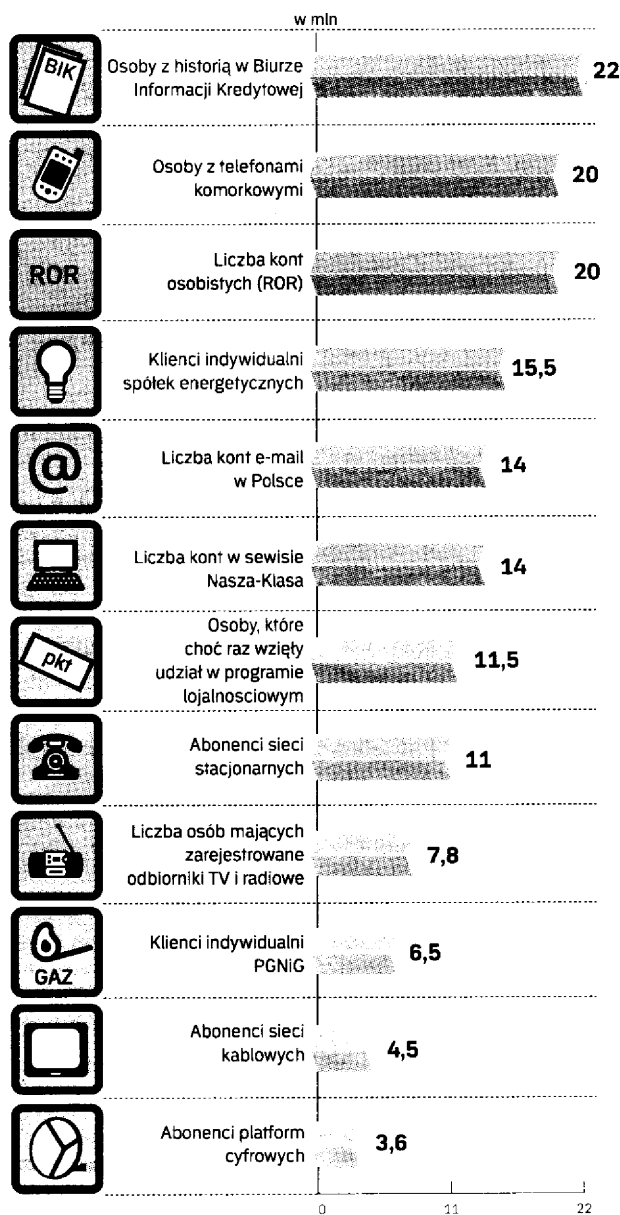
Choć raz w programie lojalnościowym wzięło udział przynajmniej 11 mln Polaków. Licząc na mgliste obiecane nagrody lub rabaty i przystępując do nich, podajemy wiele informacji o sobie. – Ich głównym zadaniem jest budowanie lojalności. Kwestia zbierania danych nie jest może tak bardzo istotna, zwłaszcza że firmy

i tak nie wykorzystują tego potencjału. Uczestnicy często się przeprowadzają, dane przestają być aktualne, dlatego trudno jest np. przysyłać informacje o interesujących ofertach. Na dodatek takie bazy są ogromne i nie jest łatwo nimi zarządzać – mówi Adam Czarnecki, wiceprezes firmy badawczej ARC Rynek i Opinia. – Nie spodziewam się dalszego boomu na programy lojalnościowe. Ich uruchamianie sporo kosztuje, a przecież nie chodzi o danie klientowi kawalka plastiku, tylko czegoś więcej. Bardziej efektywne i atrakcyjniejsze dla klientów, bo szybciej mogą zebrać punkty, wydają się programy prowadzone przez kilka firm, jednak takich zbyt wielu też nie ma.

Podobnie zakładając darmowe skrzynki e-mailowe na portalach internetowych, podajemy wiele informacji na swój temat. Polacy mają takich kont ok. 14 mln, choć w przypadku przynajmniej części z nich podawane dane mogą nie być zupełnie prawdziwe. Kopalnią danych są też serwisy społecznościowe, jak Grono, GoldenLine czy oczywiście Nasza-Klasa, gdzie działa 13 – 14 mln profili. ■

www. Więcej o elektronicznej inwigilacji na stronie

www.rp.pl



•KTO ZOSTAWIA DANE OSOBOWE

Informacje o sobie zostawiamy na każdym kroku. Największymi bazami danych osobowych dysponują banki, operatorzy telekomunikacyjni, firmy zajmujące się dostarczaniem energii elektrycznej czy gazu, właściciele serwisów internetowych. ■

Zakupy to kopalnia informacji o nas

→ Andrzej Bochacz, prezes spółki Kamil z grupy Macrologic

W: Czy firmy często zbierają informacje o klientach, choć ci nie o tym nie wiedzą?

ANDRZEJ BOCHACZ: Na razie nie jest to powszechne, ale nowoczesne systemy dają ogromne możliwości. W większości sklepów liczona jest nie tylko liczba klientów wchodzących czy robiących zakupy, ale także ci przechodzący obok – dzięki tej wiedzy firma może np. zmieniać wygląd witryny na bardziej zachęcający. **Co firmom daje taka wiedza?**

Zaskakująco dużo. Salon fryzjerski dzięki analizie profilu klientów wie, czy potrzebuje w określonych godzinach więcej

personelu do obsługi mężczyzn, kobiet czy dzieci. Z kolei firmy odzieżowe mogą lepiej dopasować ofertę zależnie od liczby klientów, np. jeśli przeważają kobiety, rozbudowują tę część oferty kosztem produktów dla mężczyzn i dzieci. **Jak firmy zbierają informacje?**

Najprostsza jest po prostu analiza monitoringu, którą automatycznie może robić system komputerowy. Jedną z firm odzieżowych, gdy zauważyła, że wielu klientów robiących zakupy w jej sklepach zabiera ze sobą dzieci, zdecydowała o wprowadzeniu dla nich kolekcji, która okazała się sukcesem.

A inne sposoby?

Są już bardziej skomplikowane, wymagają zaangażowania również klientów. Personel, przyjmując zapłatę, może zadać klientowi kilka pytań – nie tylko o kod pocztowy, ale także zainteresowania, zadowolenie z usługi itp. Firmy wprowadzają też formularze, które wypełnia personel, oceniając wygląd, wiek czy zamożność klienta. Ojciec z synem razem robiący zakupy i płacący wspólnie też wymagają odnotowania. To wbrew pozorom ważna informacja. Wszelkie tego typu dane są bardzo potrzebne przy planowaniu zaopatrzenia na

kolejne miesiące, projektowaniu nowych kolekcji, ale na tym kończy się ich zbieranie anonimowo.

Co to jeszcze firmie daje?

Już dawno temu zauważyliśmy, że w przypadku odzieży zależnie od regionu Polski sprzedają się lepiej określone kolory czy modele. Jedne miasta są bardziej konserwatywne, mieszkańcy innych szukają nowości zgodnych ze światowymi trendami. Różnią się też typowe modele – zależnie od regionu ludzie są wyżsi czy szczuplejsi. To cenna wiedza dająca wielkie oszczędności. Nie trzeba do sklepów w całym kraju wysłać tego samego, tylko od razu różnicować ofertę. **Czyli klient sam niewiele mówi o sobie, raczej jest oceniany przez system lub pracownika?**

Nie do końca, bo najwyższym stopniem zaawansowania, jeśli

chodzi o zbieranie informacji o kliencie, jest program lojalnościowy. W tym przypadku firma musi jednak zachęcić, żeby ktoś wypełnił już bardziej szczegółową ankietę i sam podał wiele informacji o sobie, jak numer telefonu, adres e-mailowy, zamieszkania, zainteresowania itd. Temu przyświeca inny cel – utrzymać klienta, lepiej go poznać. Modelowo prowadzony program polega na wysyłaniu informacji o interesujących go nowościach w ofercie, co wiemy, obserwując jego wcześniejsze zakupy, zaproszenia, np. na pokaz nowej kolekcji, by poczuł się ważny dla firmy itp. Możliwości jest wiele, ale firmy powinny mieć świadomość, że w takie programy inwestuje się w perspektywie lat. Dopiero wtedy mogą przynieść efekty. Inwestują w nie też sieci handlowe, łącząc programy z kartami kre-

dytowymi. Dzięki temu mają też dużo informacji o klientach.

Co będzie dalej?

Prawdziwe przełomy dopiero przed nami. Ogromne możliwości dają płatności dokonywane za pomocą komórek. Nie trzeba będzie nosić kart, pamiętać PIN. Klient, już wchodząc do sklepu, będzie mógł zostać zarejestrowany przez system. W jednej z polskich sieci odzieżowych zainstalowaliśmy system identyfikacji klientów przez odcisk palca.

Nie przeraża pana taka inwigilacja, z której wielu z nas nie zdaje sobie sprawy?

Już dawno nauczyłem się nie walczyć z tym, co nieuniknione. Może nie podobać się nam powszechne używanie komórek, ale co z tym możemy zrobić, po prostu tak się dzieje.

—rozmawiał Piotr Mazurkiewicz

Elektronika jest wszechobecna

TECHNOLOGIE | SYSTEMY MONITORUJĄCE SĄ WSZĘDZIE. Ślady, które zostawiamy, używając kart płatniczych, komórek czy nawigacji satelitarnej, pozwalają na kontrolę naszych ruchów. Służby wykorzystują to do walki z przestępcami, ale sięgają po nie i ci ostatni

KRZYSZTOF URBĄSKI

Telefon komórkowy, bez którego niemal nie wyobrażamy sobie już życia, to w rękach operatora najskuteczniejszy szpieg osobisty, jakiego można sobie wyobrazić. Oczywiście jeśli ktoś mu zleci taką „usługę”. Bez najmniejszego podejrzenia z naszej strony operator może zlokalizować nas z dokładnością do kilku metrów, przechwycić rozmowy, a nawet zamienić telefon w mikrofon lub kamerę. Warunek jest jeden – telefon musi być włączony.

Coraz więcej miejsc publicznych w naszych miastach jest monitorowanych. Kamery śledzą nie tylko główne ulice i place, ale również dworce, parki, przejścia podziemne czy tunele. Zidentyfikowanie samochodu, prześledzenie jego drogi, podobnie jak osoby, nie stanowi żadnego problemu.

Im więcej kart, tym więcej śladów

Elektroniczne ślady pozostawiamy znacznie częściej, niż nam się wydaje. Korzystając z bankomatu, logujemy się do systemu bankowego. Ślad transakcji zostaje zarówno na koncie, jak i w systemie administrującym siecią bankomatów. Coraz więcej bankomatów wyposażonych jest w kamery, tak jak oddziały banków. Korzystając z usług tych instytucji, przestajemy być anonimowi.

W pracy, jeśli mamy elektroniczny identyfikator, za każdym razem nasze wejście lub wyjście jest rejestrowane, nawet wtedy, gdy pracodawca nie rozlicza nas z przepracowa-

nych godzin. Takie elektroniczne karty wstępu coraz częściej pojawiają się także w instytucjach niezwiązanych z pracą zawodową, np. klubach sportowych. Im więcej tego typu kart wstępu mamy, tym częściej zostawiamy ślady swojej bytności.

Transmisja z hotelowego korytarza

Zwykle nie zdajemy sobie sprawy, jak łatwo zidentyfikować nasze ślady. Co jakiś czas, choćby przy okazji afer natury kryminalnej, możemy się o tym przekonać. Przykładem może być historia byłego szefa Ministerstwa Spraw Wewnętrznych i Administracji. Bolesnie przekonał się o tym Janusz Kaczmarek, choć jako minister tego właśnie resortu najlepiej o tym powinien wiedzieć.

5 lipca ubiegłego roku po godz. 23 ówczesny minister Janusz Kaczmarek wszedł do windy w hallu głównym hotelu Marriott w Warszawie, udał się na 40. piętro i skierował do tego samego pokoju, do którego miał wejść znany biznesmen Ryszard Krauze. Kaczmarek pozostał na korytarzu przez 11 minut z powodu nieobecności osoby, z którą miał się spotkać. Jednak wkrótce na tym samym piętrze wysiadł Ryszard Krauze i udał się do wynajmowanego przez siebie apartamentu nr 4020. Gdy biznesmen dostał się do swego pokoju, Kaczmarek przeszedł do tego samego apartamentu. Choć uczestnicy spotkania zapewne chcieli, by pozostało ono w tajemnicy, przebieg zdarzeń w hotelu Marriott stał się ogólnie znany, kiedy prokuratura ujawniła zapis z hotelowych kamer.

Szef MSWiA zlekceważył nie tylko fakt rejestrowania przez kamery wszystkich wchodzących i przebywających w hotelu. Zlekceważył też inne ślady swoich kontaktów z Krauzem: telefony komórkowe. Jak ustaliła prokuratura, Janusz Kaczmarek i Ryszard Krauze mieli telefony na kartę, które służyły im wyłącznie do porozumiewania się między sobą. Rozmawiali za ich pośrednictwem kilkadziesiąt razy także 5 lipca. Prowadzący dochodzenie funkcjonariusze CBA przeanalizowali 15 tysięcy numerów, które zalogowały się w stacji bazowej, tzw. BTS (ang. Base

Transceiver Station), hotelu Marriott w dniu, kiedy Kaczmarek odwiedził Krauzego w jego apartamencie. Śledczy ustalili też, że Krauze oprócz telefonu do kontaktów z Kaczmakiem używał kilku innych aparatów.

Komputer rzecz niebezpieczna

Jeszcze łatwiejszym źródłem wycieku informacji jest komputer osobisty. Kupując urządzenie, rejestrujemy system operacyjny, gdyż wymaga tego firma, która go wyprodukowała (najczęściej Microsoft). W ten sposób producent systemu dysponuje naszymi danymi osobowymi, a komputer, nie informując o tym użytkownika,

Każdego posiadacza telefonu komórkowego można zlokalizować, analizując dane ze stacji bazowych operatorów

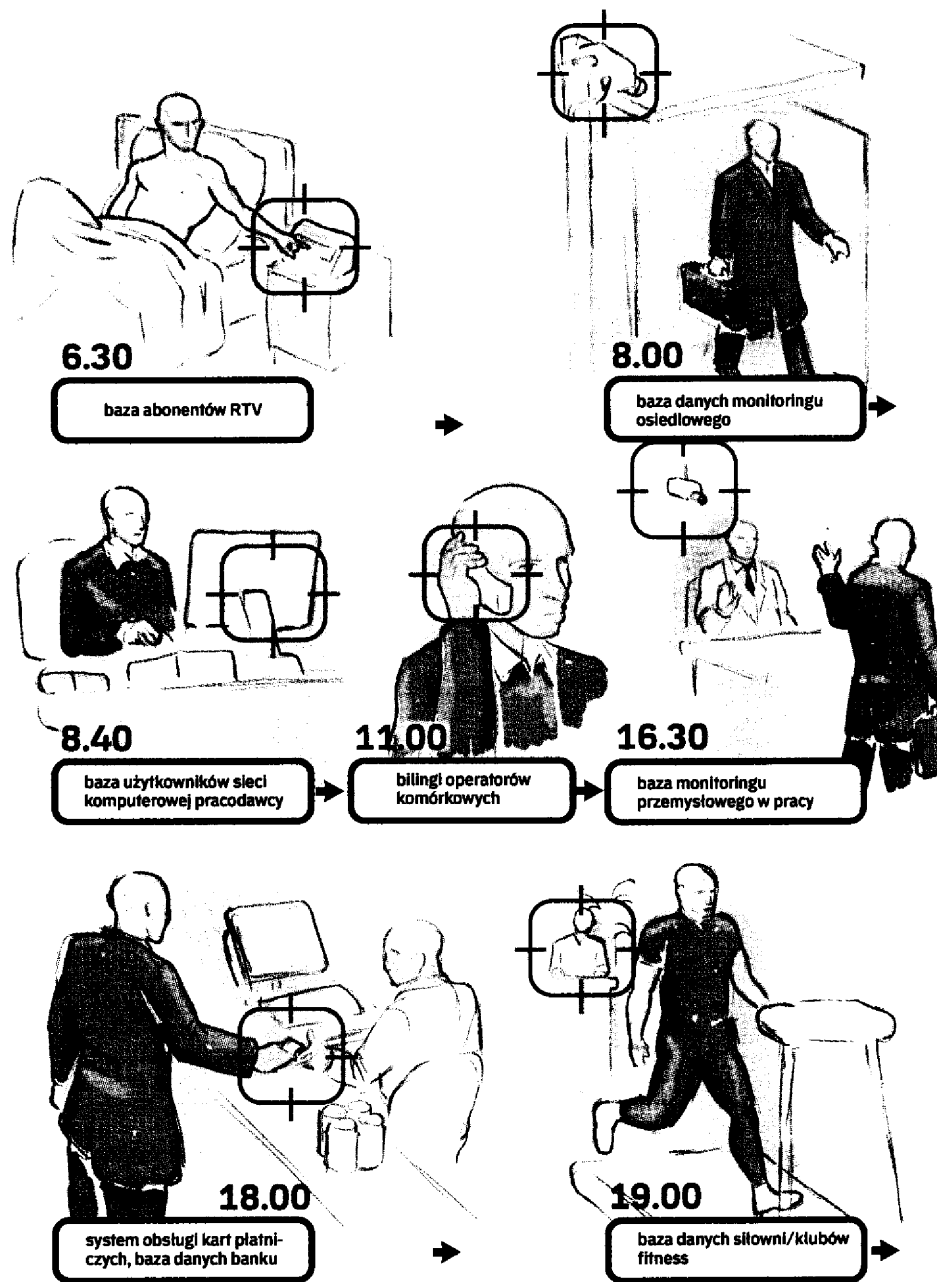
łączyć się za pomocą Internetu z centralą firmy. Co prawda firma zastrzega, że tych danych nie wykorzystuje, ale praktyka uczy, że nigdy nie ma całkowitej pewności, czy nie zostaną skradzione lub sprzedane na przykład przez jej nieuczciwych pracowników.

Korzystając z komputera na co dzień, możemy dokonywać przelewów bankowych, zakupów towarów czy biletów na wycieczkę. To zaledwie tylko kilka czynności, które można wykonać w każdej chwili przez Internet.

Ale każdy nasz ruch w sieci śledzą elektroniczni szpiedzy. Nawet pojedyncze otwarte okienko zarejestrowane jest na serwerze dostawcy usług internetowych lub w pamięci systemów zbierających informacje w celach komercyjnych. Nie mówiąc już o świadomości rozsyłanych programach śledzących, tzw. spyware'ach.

Eksperti alarmują: hakerzy stają się coraz bardziej bezczelni. Polska od lat plasuje się w czołówce krajów odnotowujących największą liczbę ich ataków. Mimo wciąż udoskonaleń systemów zabezpieczeń najważniejszym czynnikiem obronnym pozostaje rozważa użytkowników.

– Warto korzystać ze stron oferujących szyfrowanie, których adresy zaczynają się od



➤ SZCZEGÓŁY DNIA CODZIENNEGO POLAKÓW TRAFIAJĄ DO SETEK BAZ DANYCH.

Korzystając z technologii ułatwiających życie, musimy sobie zdawać sprawę, że stale zostawiamy za sobą ślady. Figuruje one w postaci setek informacji w najróżniejszych bazach danych. W razie potrzeby operator sieci komórkowej może ustalić miejsce naszego pobytu, zarządca budynku

https – podpowiada Mirosław Maj, ekspert w CERT/NASK, instytucji, która zajmuje się zabezpieczeniami w Internecie. – Bezpieczeństwo można popra-

Google, które można uznać za jeden z najwspanialszych wynalazków Internetu, skrzętnie gromadzi informacje, które mają mu pomóc w

jąc portale społecznościowe, przestępcy instalowali fałszywe profile i wchodzili w interakcje z innymi użytkownikami o znanych nazwiskach. W ten sposób uwiarygadniali się.

Według szacunków amerykańskiej firmy Cloudmark Inc., specjalizującej się w ochronie komunikatorów, nawet 40 proc. profili w portalach społecznościowych jest fałszywych. To, co się przyczyniło do sukcesu tego typu portali, a więc wiele kanałów dostępu do informacji, otwartość i liczba użytkowników, zważyło także rzesze hakerów i spamerów – uważają specjaliści z Cloudmarku.

Czy brak anonimowości powinien nam przeszkadzać? Tym, którzy mają czyste intencje, raczej nie. Niebezpieczeństwo stanowi jednak możliwość wycieku informacji i wykorzystywanie jej przez przestępców: terrorystów, złodziei lub sabotażystów, którzy stale podpatrują sposoby działania legalnych służb. ■

Jak obliczyli specjaliści zajmujący się technologiami internetowymi, jedna wizyta na stronie portalu Yahoo! sprawia, że zostaje po nas ponad 800 informacji

wić, nie korzystając z opcji zapamiętywania identyfikatora i hasła czy wylogowując się po zakończeniu pracy.

Sfałszowane profile

Korzystając z jakiegokolwiek portalu, zostawiamy po sobie kilkadziesiąt informacji. Kiedyś specjaliści poproszeni przez gazetę „New York Times” obliczyli, że odwiedzając stronę portalu Yahoo!, zostawiamy po sobie 811 informacji osobistych, a przeszukując sieć za pomocą wyszukiwarki Google, nawet jeszcze więcej.

profilowaniu usług dla klientów.

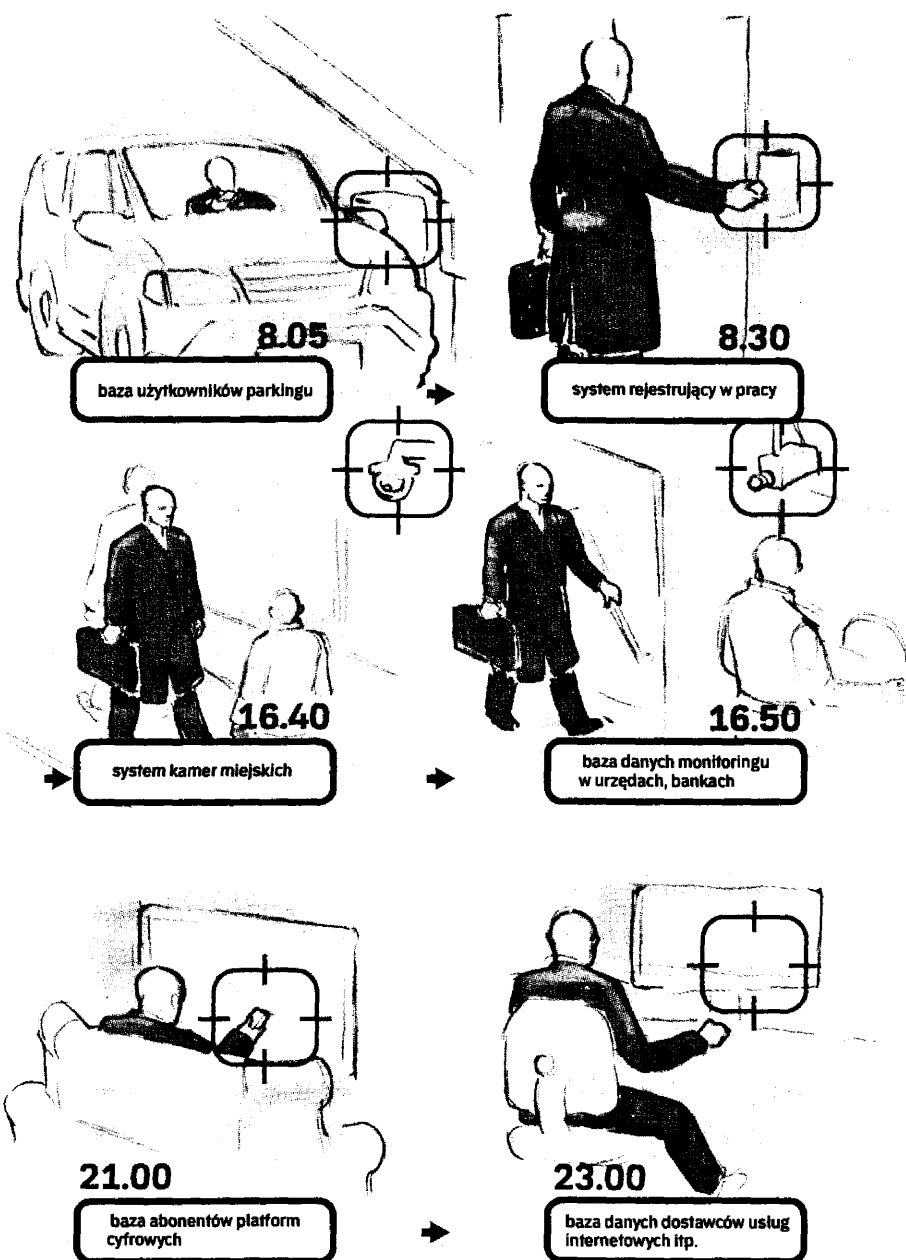
Jeszcze większym zagrożeniem są zapewne pod tym względem serwisy społecznościowe i blogi, gdzie internauci beztrudno umieszczają swoje dane osobowe. I chociaż często zniechęcają się do korzystania z tych serwisów już po krótkim czasie, zostawiają setki informacji, z których skrzętnie korzystają oszuści.

W ostatnich dniach głośno stał się przypadek przejmowania kontroli nad komputerami za pomocą fałszywych stron YouTube. Wykorzystu-

www Więcej o elektronicznych zagrożeniach

www.cert.pl

Skorzystanie z bankomatu, zakup paliwa, wejście na siłownię. Każda prosta codzienna czynność pozostawia cenną informację o naszej obecności



CZY NAM SIĘ TO PODOBA CZY NIE, NIE MA OD TEGO ODWRÓTU

sprawdzić, kiedy byliśmy w mieszkaniu, pracodawca odtworzyć godziny pracy. Dane można skompletować, choć wymaga to sporego wysiłku. Pozostaje jedynie mieć nadzieję, że informacje nie będą wykorzystywane niezgodnie z prawem. ■

Pracodawcy coraz chętniej śledzą podwładnych

INWIGILACJA W FIRMIE
Przedsiębiorstwa coraz chętniej monitorują swych pracowników. Tym bardziej że technologia dostarcza im coraz bardziej wyszukanych narzędzi kontroli

W latach 30. XX w. szef imperium obuwniczego Jan Bata zainstaltował w biurcu firmy szpiegowski gabinet w windzie, w której krążył między piętrami, nadzorując przez przeszklone ściany pracę swych ludzi. Dziś szefowie, którzy chcą mieć oko na pracowników, nie muszą się uciekać do takich konstrukcji. Skuteczny i dyskretny monitoring ułatwiają im nowe technologie.

Kamery przemysłowe instalowane w biurach, fabrykach czy sklepach mają strzec nie tylko przed intruzami z zewnątrz, ale i przed nadużyciami popełnianymi przez pracowników. Według brytyjskiego Centre for Retail Research w wielu krajach wyższe

straty powodują kradzieże dokonane przez pracowników niż klientów. Rolę kadrowego, który przed laty pilnował w biurach listy obecności, przejęły elektroniczne bramki, rejestrujące czas pracy. Monitoring poczty elektronicznej i, coraz częściej, całej aktywności internetowej pracowników pomaga zmniejszyć ryzyko wycieku poufnych danych, ograniczając też prywatne buszowanie w sieci (cyberslacking).

Według najnowszego raportu D-Link Technology Trend 80 proc. polskich pracodawców ogranicza pracownikom korzystanie z Internetu, przede wszystkim blokując dostęp do serwisów umożliwiających ściąganie muzyki i filmów. Jak oceniają eksperci firmy doradczej Deloitte i kancelarii prawnej Baker & McKenzie, firmy na całym świecie, w tym w Polsce, coraz częściej monitorują pracowników.

Popularne metody kontroli, czyli rejestracja rozmów telefonicznych i elektroniczne syste-

my rejestracji czasu pracy, wielu firmom już nie wystarczają. Teraz pracodawcy wykorzystują moduły GPS umożliwiające lokalizację aut (dzięki temu mogą nadzorować pracę np. przedstawicieli handlowych) czy systemy RFID, które pozwalają śledzić ruch pracowników w obrębie monitorowanego terenu.

Jak to się ma do ochrony ich prywatności? – Pracodawca może legalnie monitorować pracownika pod warunkiem, że kontrola i jej zasady są uzasadnione i jawne – mówi Sylwia Puzyńska z Baker & McKenzie. Jak dodaje, warto uregulować kwestię monitoringu w piśmie w regulaminie i zapisem w umowie o pracę. Wprawdzie pracodawca ma prawo do kontroli poczty pracownika, ale tylko do korespondencji służbowej. Prywatnej nie może nadzorować. Może za to wprowadzić zakaz używania firmowej poczty do celów prywatnych.

—Anita Błaszczak

Znajdź swój numer PESEL na śmietniku

TECHNOLOGIE | WYCIEKI DANYCH SĄ CORAZ CZĘSTSZE.

Nawet najlepiej strzeżona baza danych nie jest w pełni bezpieczna

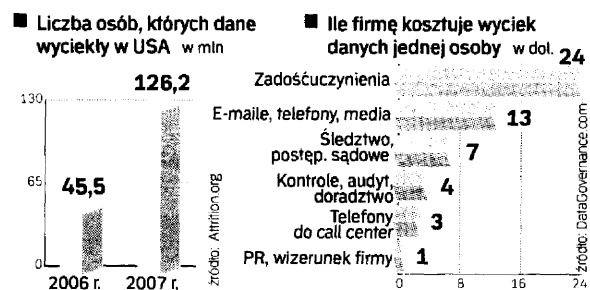
TOMASZ BOGUSZEWICZ

Osoby obawiające się o bezpieczeństwo swoich danych powinny porzucić złudzenia. Informacje o nich prędzej czy później znajdą się na stronie internetowej, w dokumentach porzuconych na wysypisku lub na dysku skradzionego komputera. Problemu wycieków poufnych danych praktycznie nie da się rozwiązać.

Firmy Polskie Badania Internetu oraz IAB Polska opublikowały właśnie raport z badania jakości obsługi klientów sklepów internetowych. Korzysta z nich 5,8 mln Polaków. Co ciekawe, aż 45 proc. badanych stwierdziło, że najważniejszym kryterium wyboru sklepu w sieci jest bezpieczeństwo danych, które muszą w nim zostawić, by sfinalizować zakupy. Inne czynniki, takie jak np. szybkość dostawy towaru, potraktowano drugorzędnie.

Mimo to nawet osoby dbające o bezpieczeństwo danych nie mogą być pewne, że informacje na ich temat nie wpadną w niepowołane ręce. Nie wystarczy wykasowanie profili w serwisach społecznościowych, portalu aukcyjnym czy księgarni internetowej. Dysponują one bowiem np. historią zamówień pozwalającą oszacować zasobność portfela.

Firmy i instytucje na całym świecie wydają miliony na zabezpieczenia. Mimo to właśnie one stanowią największe źródła wycieków. Przykładów aż nadto. W lipcu 2008 r. w Internecie znalazło się kilka tysięcy listów motywacyjnych i



NAJWIĘKSZE WYCIEKI POUFNYCH INFORMACJI W CIĄGU OSTATNICH 12 MIESIĘCY:

- Rząd Wielkiej Brytanii gubi dyski ze szczegółowymi danymi 25 mln obywateli (październik 2007 r.)
- Z magazynu banku GE Money w USA giną dane 650 tys. osób (styczeń 2008 r.)
- Informacje o 3,5 mln klientów wykradziono z komputerów kanadyjskiej firmy telekomunikacyjnej Bell Canada (styczeń 2008 r.)
- Błędy serwisu KupBilet.pl powodują, że przez kilka godzin w sieci dostępne są dane wszystkich osób zainteresowanych kupnem biletów na Euro 2008 (luty 2008 r.)
- Dane kilku tysięcy osób starających się o pracę w Banku Pekao SA trafiają do sieci (lipiec 2008 r.)
- Internetowy dom maklerski TD Ameritrade (USA) gubi dane 6 mln klientów (wrzesień 2008 r.)
- Deutsche Telekom przyznał (dwa lata po zdarzeniu), że z jego baz wykradziono informacje dotyczące ok. 17 mln klientów (październik 2008 r.)

oraz historię zakupów w sieci. Słowem wszystko, za co spore sumy – sięgające setek tysięcy dolarów – zaplaca przedstawiciele internetowej szarej strefy, głównie organizacje i osoby rozsyłające spam reklamowy. Co ciekawe, okazało się, że dane z TD Ameritrade wyciekały już od jesieni 2006 r., ale dopiero ostatnio firma przyznała, że ma problem. Informacje wykradali hakerzy forsujący zbyt słabe zabezpieczenia systemów firmy.

Problem z przechowywaniem danych mają jednak nie tylko prywatne korporacje. W listopadzie 2007 r. Wielką Brytanię wstrząsnęła wiadomość o zagubieniu przez rządowych urzędników komputerowych dysków z danymi 25 mln Brytyjczyków, czyli 40 proc. wyspiarskiej populacji. Dane zawierały nazwiska, adresy, numery kont bankowych i numery ubezpieczenia. Według Paula Stephensa, szefa organizacji konsumenckiej Privacy Rights Clearinghouse, to największy wyciek, jeśli chodzi o liczbę obywateli, których dotknęła utrata danych. Powód był prozaiczny – dyski komputerowe przeznaczone do zarchiwizowania zostały przesłane zwykłą pocztą. Dane znajdowały się w dwóch przesyłkach. Druga została nadana, mimo że pierwsza nigdy nie dotarła do celu.

Właśnie dlatego, z powodu błędów ludzkich, wycieków danych nigdy nie uda się wyeliminować. Brytyjska firma Orthus badała to zagadnienie w

kilku londyńskich korporacjach. Jej specjaliści przez 100 tys. godzin monitorowali systemy w poszukiwaniu przypadków nieuprawnionego kopiowania plików na urządzenia przenośne: pendrive'y, odtwarzacze MP3, telefony komórkowe, palmtopy i inne, oraz transferowane na zewnątrz poprzez e-mail czy wrzucane np. na serwisy społecznościowe. Wyników badania nigdy w całości nie upubliczniono prawdopodobnie ze względu na reputację przebadanych firm.

Jak jednak ujawniono, za ok. 30 proc. przypadków, w których dane trafiają na zewnątrz, odpowiadają osoby zatrudnione w działach informatyki/IT. „Mają największą wiedzę i uprawnienia. Sami zajmują się kontrolowaniem użytkowników, ale ich nie kontroluje już często nikt” – napisano we wnioskach z raportu. Jednak, jak przekonuje Maciej Moskowitz, specjalista ds. zabezpieczeń w firmie AVG, dane mogą wyciekać z zupełnie nieoczekiwanych źródeł. – Najlepszą pracą dla hakera jest zatrudnienie się na stanowisku nocnego stróża. W nocy w biurze nie ma nikogo, a ochroniarz wyciąga laptopa i podpina się do systemu. Praktycznie nie ma sposobu, by zapobiec takim przypadkom. Administratorzy strzegący bezpieczeństwa danych bawią się w kotka i myszkę z tymi, którzy chcą je wykraść. A do tego zmagają się ze zwykłą ludzką nieostrożnością – mówi ekspert. ■

100 tys.

dane tyłu pracowników brytyjskich służb zbrojnych zostały zgubione w październiku

CV osób, które starały się o pracę w Banku Pekao SA. Sprawą zajął się generalny inspektor danych osobowych. Sierpniowa kontrola przyniosła błyskotliwy wniosek: naruszone zostały w ochronie danych osobowych. Ile niepowołanych osób skopiowało dane aplikantów, zanim zniknęły one z sieci – nie wiadomo.

Polska afery błędnie jednak w porównaniu z największymi światowymi hitami wśród wycieków. Bohaterem ostatniego, z września tego roku, jest TD Ameritrade, amerykański broker online, który zagubił dane 6 mln klientów. W tym imiona, nazwiska, adresy, telefony, numery Social Security (amerykański odpowiednik PESEL)

Nasze dane to coraz cenniejszy towar

PRAWO | INFORMACJE O SOBIE ZOSTAWIAMY CODZIENNIE W WIELU MIEJSCACH.

Tymczasem firmy korzystają z tych danych, aby sprzedać nam swoje usługi i produkty

MICHAŁ KOSIARSKI

Znaczenie ma każda informacja. Nie tylko adres, imię i nazwisko, ale też upodobania, to, co kupujemy, czytamy. Rzadko jednak dostrzegamy w informacjach o sobie cenny towar, którego nie powinniśmy łatwo przekazywać innym. Może nam to utrudnić życie – zasypać naszą skrzynkę ulotkami, a e-mail spamem. Niestety, mało kto wie, jakie ma uprawnienia, gdy jakaś firma przetwarza nasze dane osobowe. W razie złamania prawa nie wiemy też, gdzie i jak dochodzić praw. Najpierw uporządkujmy kilka najważniejszych pojęć.

Dane osobowe to wszelkie informacje dotyczące konkretnej osoby, za pomocą których można ją zidentyfikować, choćby nie była wyraźnie wskazana. Zbiór danych to taki ich zestaw o charakterze osobowym, w którym są one dostępne według określonych kryteriów – chodzi o różne akta (np. pracownicze), dane w formie informatycznej, spisy, rejestry itp. Administratorem danych jest podmiot lub

osoba decydująca o celach i środkach przetwarzania danych. Może nim być urząd państwowy, przedsiębiorca itp., każdy, kto jest odpowiedzialny za utworzenie i prowadzenie zbioru danych. Za przetwarzanie danych rozumie się wykonywanie na nich jakichkolwiek operacji.

Kowalski nie jest bezradny

Jeśli nasze dane ma jakaś firma, która np. przysyła nam ulotki reklamowe, to mamy kilka możliwości interweniowania. Każda osoba, której dane są przetwarzane w zbiorze, ma prawo zwrócić się do administratora o informację na temat tych danych. Administrator musi nam udzielić takiej informacji. Ważne, że uprawnienie to jest bezpłatne, gdy o informację taką występujemy nie częściej niż co sześć miesięcy.

Administrator musi poinformować (jeżeli tak zażądamy – pisemnie) o źródle, z którego pochodzą nasze dane, celu, zakresie i sposobie ich wykorzystania. Zławiadomością jest taka, że nie mamy prawa wglądu do dokumen-

tów, a nasze żądanie nie jest też podstawą prawną ich wydania. Administrator ma aż 30 dni na udzielenie odpowiedzi. Za niedopełnienie obowiązku przekazania tych informacji grozi odpowiedzialność karna – grzywna, ograniczenie wolności albo rok więzienia (art. 54). Warto jednak uprzedzić, że wymiar sprawiedliwości rzadko ściga sprawców takich przestępstw.

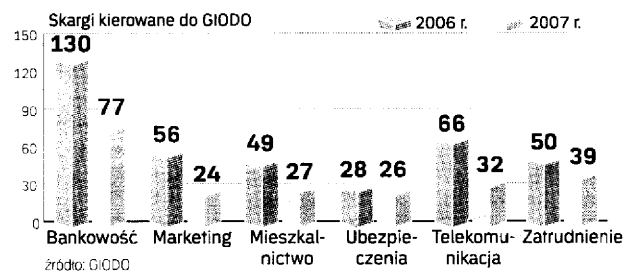
Mamy też prawo do poprawiania danych, a nawet domagania się, by administrator wstrzymał się z ich przetwarzaniem lub je usunął. Tak wynika z art. 35 ustawy. Chodzi o możliwość uzupełnienia, uaktualnienia, sprostowania, czasowego lub stałego wstrzymania ich wykorzystywania. Trzeba jednak wykazać, że dane są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem przepisów lub są zbędne do realizacji celu, dla którego je zgromadzono. Przykładowo firma, której na potrzeby konkretnego konkursu podaliśmy informacje o sobie, nie może ich wykorzystywać w innych celach. Administrator danych (czyli np. firma, która chce nam zaoferować

usługi) powinien uwzględnić nasze żądania bez zbędnej zwłoki.

Jakich roszczeń można dochodzić

Prawo sprzeciwu to kolejne uprawnienie. Przewiduje je art. 32 ust. 1 pkt 8 ustawy. Dotyczy jednak tylko dwóch sytuacji. Gdy administrator chciałby przetwarzać w celach komercyjnych dane pozyskane dla wykonania określonych przez prawo zadań publicznych (np. wydanie prawa jazdy czy paszportu) albo dane niezbędne dla prawnie usprawiedliwionego celu administratora (np. wysyłania nam wezwania sądowego). Na przykład notariusz, u którego podpisaliśmy akt notarialny, nie może przysyłać nam ulotek reklamujących ubezpieczenia czy materiały wykonawcze.

W razie sprzeciwu administrator nie musi usunąć wszystkich danych. Może sobie zostawić imię, nazwisko czy PESEL, aby uniknąć ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem. Każdy może zażądać od administratora



•SKARGI KIEROWANE DO GIODO

Mamy prawo do poprawiania swoich danych. Możemy też domagać się od administratora wstrzymania ich przetwarzania lub usunięcia. Sprawa może nawet trafić do sądu. ■

zaprzestania przetwarzania swoich danych w związku ze szczególną sytuacją (np. zagrożenie bezpieczeństwa osobistego).

Osoba, która uważa, że jej prawa zostały naruszone, a nie chce korzystać z trybu administracyjnego i karnego, może egzekwować odpowiedzialność cywilną. Zainteresowany ma prawo do odszkodowania od administratora, jeśli poniesiona przez niego szkoda jest następstwem niezgodnych z prawem operacji przetwarzania danych. Na przykład administrator przekazał dane osobowe zainteresowanego firmie marketingowej bez jego zgody (a wbrew

zastrzeżonemu sprzeciwowi), przez co klient stracił możliwość zarobku na udostępnieniu tych danych. Odszkodowanie jest wtedy niezależne od stwierdzenia winy administratora.

Naruszenie ustawy o ochronie danych osobowych też może prowadzić do naruszenia dóbr osobistych, w tym prawa do prywatności. Oznacza to, że można wystąpić z roszczeniami opisanymi w art. 23 – 24 kodeksu cywilnego. Co istotne, aby wystąpić do sądu z pozwem o ochronę dóbr osobistych, nie jest konieczne wcześniejsze stwierdzenie przez GIODO, że doszło do naruszenia przepisów. ■

Ostrożnie udostępniamy informacje o sobie

ROZMOWA | MICHAŁ SERZYCKI, generalny inspektor ochrony danych osobowych

W: Gdy wychodzimy na ulicę, odwiedzamy sklepy, przychodzimy do firmy albo do znajomych, którzy mają budynek z ochroną, to jesteśmy obserwowani przez dziesiątki kamer. Czy to zgodne z przepisami o ochronie danych osobowych?

MICHAŁ SERZYCKI: Zagadnienie monitoringu powinniśmy rozpatrywać nie tylko w kontekście ochrony danych osobowych czy dóbr osobistych, ale także przepisów szczególnych zezwalających na instalowanie kamer i uprawniających niektóre służby do kontroli czy nadzoru zarejestrowanych nimi obrazów. Podobnie jak społeczeństwa w innych krajach unijnych, niewielu z nas kwestionuje zakładanie monitoringu w celu poprawy bezpieczeństwa. Ważne jest natomiast, by podczas rejestrowania obrazu nie

dochodziło do naruszenia praw i wolności obywateli. A ponieważ nadzór wideo ogranicza naszą prywatność, na terenach, na których jest on wprowadzony, powinny być umieszczone tablice informujące o jego istnieniu. Administratorzy systemów dozoru wizyjnego powinni zaś dbać o zgodne z prawem, w tym z ustawą o ochronie danych osobowych, postępowanie z zarejestrowanymi obrazami. Ważne jest przede wszystkim zadbanie o bezpieczne gromadzenie i przechowywanie zapisów z kamer, tak by nie dostały się one w ręce osób nieuprawnionych. W niektórych przypadkach zarejestrowane obrazy możemy bowiem uznać za dane osobowe. O ile bez dodatkowych informacji trudno byłoby zidentyfikować tysiące osób przewijających się po ulicach pod okiem ka-



FABER PASTERSKI

mery, to już w przypadku obrazów ludzi siedzących w samochodach, które można powiązać z numerami rejestracyjnymi aut, można mówić o danych osobowych. Uważam jednak, że potrzebna jest ustawa o wideofilmowaniu, która kompleksowo i szczegółowo ureguluje funkcjonowanie monitoringu wizyjnego.

Coraz częściej jesteśmy też proszeni o wpisy do książek wejść i wyjść...

Administratorzy budynków mogą stosować taki sposób identyfikacji odwiedzających je osób. Muszą jednak dopełnić obowiązków informacyjnych – wpisujący się powinni wiedzieć, w jakim celu są zbierane te dane, w jakim zakresie, kto jest ich administratorem. Trzeba też zabezpieczyć książki wejść i wyjść po zakończeniu wpisów, aby nie trafiły w niepowołane ręce, lub je zniszczyć.

Co zrobić z ulotkami wysypującymi się ze skrzynki pocztowej?

Trzeba korzystać z uprawnień, jakie każdemu z nas daje ustawa o ochronie danych osobowych – np. z prawa do sprzeciwu wobec dalszego przetwarzania danych do celów marketingowych – i je egzekwować. Zalecałbym też ostrożność w wyrażaniu zgody na przetwarzanie danych osobowych, w tym na przekazanie naszych danych innym podmiotom. Konsekwencje takiej decyzji możemy bowiem odczuć w postaci choćby zaśmieconej ulotkami skrzynki pocztowej.

Skąd mamy wiedzieć, czy firma przysyłająca nam ulotki legalnie weszła w posiadanie naszych danych?

O tym, że firma ma zamiar sprzedać nasze dane, musimy być poinformowani i mamy prawo się na to nie zgodzić. Jeśli zaś doszło do handlu danymi za naszą zgodą, to ten, kto je kupił, powinien nas o tym zawiadomić. Wtedy mamy prawo zastrzec, że nie może on ich wykorzystywać. Niestety, dane, jako jeden z cennych i poszukiwanych w biznesie towarów, trafiają często do nieuczciwych firm, które ignorują obowiązki informacyjne wynikające z ustawy o ochronie danych osobowych. Trzeba jednak przyznać, że dzięki współpracy nawiązanej przez GIODO

ze Stowarzyszeniem Marketingu Bezpośredniego, która zaowocowała podpisaniem porozumienia oraz stworzeniem kodeksu dobrych praktyk, liczba skarg na postępowanie firm tego sektora stopniowo się zmniejsza.

Na co zwracać uwagę przy podawaniu danych?

Przed podawaniem swoich danych nie uciekniemy. Dlatego czytamy dokładnie umowy i – zwłaszcza – klauzule zgody umieszczone zwykle w wydzielonym miejscu pod tekstem. Pamiętajmy, że nie mogą się one znajdować w treści umowy, bo podpisanie jej jest równoznaczne z podpisaniem zgody na działania marketingowe, na które gościć się nie musimy. Ważne jest też, aby z klauzuli wynikało, w jakim celu i zakresie zbierane są nasze dane, kto je będzie wykorzystywał oraz komu zostaną przekazane. Zgoda musi być wyraźna, nie może być dorozumiana ani wymuszona.

Na kłatkach schodowych nie ma list lokatorów. Czy to wymóg ochrony danych osobowych?

To dowód na dobrą znajomość praw i obowiązków wynikających z ustawy. Mieszkańcy muszą się bowiem zgodzić na publikację ich danych na liście i jeśli sobie tego nie życzą, to mają do tego prawo. Nie znaczy to jednak, że wisząca na klatce lista musi być pełna. Jeśli tylko nieliczni zgodzą się, aby ich imiona i nazwiska umieścić na liście lo-

katorów, to nie ma przeciwwskazań, aby taką listę z tymi kilkoma nazwiskami wywiesić.

Jakie nowe wyzwania stoją przed GIODO?

Obecnie największym wyzwaniem jest właściwe uregulowanie zagadnień dotyczących rozwoju nowoczesnych technologii. Za najważniejsze uważam przy tym takie wyważenie praw i obowiązków osób komunikujących się przez Internet, by z jednej strony nie hamować tej formy wymiany informacji, a z drugiej zapewnić odpowiednią ochronę prywatności. Ustawa o ochronie danych osobowych powstawała bowiem w czasie, kiedy nie było powszechną praktyką stosowanie podpisu elektronicznego, bankowości elektronicznej, hot spotów czy tworzenie profili behawioralnych. Za każdym z tych obszarów kryją się sprawy wymagające odpowiedniego uregulowania. A obecnie proponuję wiele zdrowego rozsądku i ostrożności przy ujawnianiu w sieci dotyczących nas informacji i danych osobowych. Powinniśmy zawsze pamiętać, że Internet jest całością i jeżeli na różnych forach zostawiamy różne informacje na swój temat, to nic nie stoi na przeszkodzie, aby je zebrać i wykorzystać wbrew pierwotnemu celowi, w jakim zostały umieszczone. Żyjemy w czasach, gdzie nie surowce naturalne, lecz szybki dostęp do informacji ma największą wartość.

– rozmawiał Michał Kosiarski

•GDZIE SIĘ ZWRÓCIĆ O POMOC

Od dziesięciu lat w Polsce działa generalny inspektor ochrony danych osobowych. Jego siedziba mieści się w Warszawie przy ul. Stawki 2. Inspektor ma swoją stronę internetową: www.giodo.gov.pl. Do GIODO można wystąpić m.in. ze skargą w sprawie naruszenia danych osobowych. GIODO – jeśli uzna naszą skargę za zasadną – może nakazać przywrócenie stanu zgodnego z prawem. Nie ma natomiast możliwości nakładania kar finansowych. Do GIODO można także wystąpić z prośbą o niewiążącą interpretację przepisów o ochronie danych osobowych. Najpierw jednak warto się zapoznać z poradnikiem na stronie internetowej, bo ktoś już być może pytał o to urzędników i zamieścili oni odpowiedź w Internecie. ■



Hubert Salik

Totalna inwigilacja wciąż nam nie grozi

Jedną z wielu cech społeczeństwa totalitarnego jest to, że rządzący nim chcą mieć jak największą wiedzę o swoich obywatelach. I chcą tę wiedzę wykorzystywać. Paradoksalnie, wyjątkowo otwarte na obywateli społeczeństwo informacyjne najbardziej nas do tego przybliża.

Większość naszych codziennych działań pozostawia po sobie ślady. Najgorsze jest to, że zupełnie niechciane. Figurujemy w dziesiątkach baz danych, więc gdy korzystamy z kart kredytowych, surfujemy po Internecie, kupujemy usługi czy tankujemy paliwo, zostawiamy w tych bazach informacje o naszych działaniach. Gdy wchodzimy do pracy, hipermarketu czy metra, nasze twarze są rejestrowane przez kamery przemysłowe.

Gdyby te informacje ktoś zebrał, powstałaby całkiem ciekawa historia o nas samych. Nie byłyby to jednak wielowymiarowe sylwetki ludzi z ich przekonaniami i poglądami. W większości przypadków byłby to zbiór naszych preferencji jako konsumentów. Czyli dokładnie to, czego potrzebują marketerzy, aby wiedzieć, jaką reklamę nam pokazać i co można nam sprzedać.

Jeśli więc nic złego nie robimy, nie mamy się czego obawiać. Choć już sama możliwość total-

nej inwigilacji wywołuje ciarki na plecach.

Jednak, gdyby jakiś totalitarny wódz przyszłości chciał

oprzeć na zostawianych przez nas śladach swoją władzę, miałby z tym problem. Mógłby namierzać jednostki, ale nie mógłby zniewolić społeczeństwa.

Widać to chociażby w Chinach, które starają się ograniczyć swobodę korzystania z Internetu. Te próby są skuteczne tylko na krótką metę. Bo nawet chiński socjalistyczny kapitalizm uległ globalnej wiosce.

Totalitarnym przywódcom marzy się, by mieć takie informacje o obywatelach, które dadzą im władzę pełną i nieograniczoną. A w tym celu musieliby poznać nie tylko informacje osobowe, ale przede wszystkim mieć wiedzę o naszych myślach i przekonaniach.

To nam na razie nie grozi. Nie jesteśmy także niewolnikami technologii, która zbiera o nas informacje. Jesteśmy niewolnikami sprzedawców.

Pamiętajmy jednak, że coraz częściej ogromne ilości danych, które zalegają w setkach tysięcy baz, dla nas samych są niezbędne w pracy. W epoce, gdy gospodarka produkcyjna staje się usługową, sami coraz częściej jesteśmy sprzedawcami.

➔B7 - 10