Zygmunt Mazur, Hanna Mazur, Teresa Mendyk-Krajewska

Przetwarzanie i ochrona danych osobowych w dobie rozwoju gospodarki elektronicznej

Ekonomiczne Problemy Usług nr 104, 219-227

2013

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.

MUZEUM HISTORII POLSKI

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 762 EKONOMICZNE PROBLEMY USŁUG NR 104 2013

ZYGMUNT MAZUR, HANNA MAZUR, TERESA MENDYK-KRAJEWSKA
Politechnika Wrocławska

PRZETWARZANIE I OCHRONA DANYCH OSOBOWYCH W DOBIE ROZWOJU GOSPODARKI ELEKTRONICZNEJ

Wprowadzenie

Rozwijająca się gospodarka elektroniczna, wykorzystująca systemy teleinformatyczne, wymusza zdefiniowanie ontologii[1] związanych z określonym obszarem działania, opracowanie uregulowań prawnych, branżowych, lokalnych i zakładowych dotyczących bezpiecznego przechowywania, udostępniania, aktualizacji i usuwania danych (osobowych, firmowych, finansowych czy medycznych), a także wymaga tworzenia odpowiednich rejestrów i baz danych.

1. Dane elektroniczne

W urzędach i przedsiębiorstwach wykorzystuje się zaawansowane systemy informacyjne i bazy danych, jednak nadal często informacja elektroniczna jest przechowywana w postaci nieustrukturyzowanej, czyli w plikach o różnych formatach, poza systemami informatycznymi. Dokumenty elektroniczne (cyfrowe), systemy bazodanowe i rejestry danych muszą być bezpiecznie zarządzane, a ich obsługa i użytkownicy – o różnych poziomach uprawnień – wymagają systematycznego nadzoru. Następujące w ostatnich latach zmiany w sposobie prowadzenia działalności firm i przedsiębiorstw oraz w zakresie komunikowania się ludzi sprawiają, że skuteczna ochrona danych stanowi coraz większy problem. Gromadzone, przetwarzane i przesyłane dane elektroniczne, pomimo zabezpieczeń, często są przypadko-

[1] Formalnej reprezentacji danej dziedziny, czyli zbiorów pojęć i związków między nimi.

wo udostępniane podmiotom niepowołanym lub przejmowane przez osoby nieupoważnione. Niestety, pomimo stosowania różnych mechanizmów ochrony, wycieki danych mają miejsce zarówno w małych, jak i w dużych firmach. Przykładami mogą być firma Sony, z której w 2011 roku wyciekły dane z ok. 77 mln kont PlayStation Network, oraz CitiBank, skąd w czerwcu 2011 roku wyciekły dane ok. 360 tys. klientów. Brak odpowiednich zabezpieczeń doprowadził także do upublicznienia danych kilku tysięcy osób poszukujących pracy poprzez jeden z portali internetowych[2].

Działania wielu firm ukierunkowane są jedynie na stosowanie zabezpieczeń przed atakami pochodzącymi z zewnątrz, tymczasem do wycieku danych dochodzi też na skutek nieprzestrzegania ustalonych procedur przez pracowników firmy lub z powodu braku sformułowania odpowiednich zasad postępowania. Polityka bezpieczeństwa musi więc uwzględniać zagrożenia dla bezpieczeństwa danych pochodzące także z wewnątrz firmy – jej pracowników, konsultantów, audytorów. Wykorzystywanie urządzeń mobilnych, dopuszczonych do użytku przez zakład pracy, może prowadzić do niekontrolowanego kopiowania i wynoszenia danych, ich utraty lub udostępniania osobom niepowołanym. Problem stanowi również przekazywanie użytkowanych urządzeń elektronicznych (laptopów, komputerów, aparatów telefonicznych, dyktafonów, pendrive'ów) innym pracownikom, bowiem mogą oni uzyskać dostęp do nieprzeznaczonych dla nich informacji. Podobne sytuacje mogą mieć miejsce w przypadku przekazywania sprzętu do serwisu, jego reklamacji czy utylizacji.

Dla pracowników firm wykorzystujących nowe technologie oraz dla klientów usług elektronicznych powinny być przeprowadzane szkolenia z zakresu bezpieczeństwa danych i stosowania metod socjotechnicznych.

Często dużą wagę przywiązuje się do bezpieczeństwa bieżących danych, ale nie zabezpiecza się odpowiednio kopii zapasowych i danych archiwalnych. Po upływie okresu archiwizacji nośniki z danymi są wyrzucane, a tymczasem niektóre dane jeszcze przez długi czas mają istotne znaczenie (np. dane osobowe). Szczególną uwagę należy zwracać na ochronę danych wrażliwych, finansowych, medycznych i osobowych.

Usługi świadczone przez Internet nie powinny naruszać dóbr osobistych (niemajątkowych) osób fizycznych i prawnych, które podlegają ochronie cywilnoprawnej z mocy art. 23 i 24 kodeksu cywilnego. W kodeksie cywilnym brak jest jednak definicji dobra osobistego; podane są tylko jego przykłady, między innymi pod tym pojęciem rozumie się cześć, nazwisko, zdrowie, wizerunek, prawo do spokoju i prywatności.

Charakter usług świadczonych przez Internet umożliwia naruszanie dóbr osobistych, na przykład poprzez nieodpowiednie wpisy na forach internetowych, czy założenie konta z danymi innej osoby i wysyłanie obraźliwych wiadomości do jej

[2] www.giodo.gov.pl/560/id_art/4177/j/pl, [dostęp 8.01.2013].

znajomych. Z ustawy o udostępnianiu informacji gospodarczych[3] wynika, że e-usługodawca nie odpowiada za treść przechowywanych danych, jeśli nie wie o ich bezprawnym charakterze.

2. Usługi sieciowe a ochrona danych osobowych

W Polsce obowiązuje definicja danych osobowych zawarta w art. 6 ustawy o ochronie danych osobowych[4], zgodnie z którą są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (której tożsamość można określić bezpośrednio lub pośrednio). Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Taka definicja pozostawia dużą dowolność oceny, czy poniesione koszty, czas i podjęte w tym celu czynności były nadmierne, czy nie. Istnieje również możliwość swobodnej interpretacji pośredniości działań dokonanych w celu ustalenia tożsamości osoby. Zatem nie można jednoznacznie stwierdzić, czy dane wykorzystywane w systemach teleinformatycznych, takie jak: adres IP komputera, nazwa użytkownika i hasło, adres e-mail czy numer telefonu, są danymi osobowymi, ponieważ zależy to od wielu aspektów. Na przykład nazwa użytkownika (login) podana przy zakładaniu konta na forum lub w serwisie społecznościowym nieweryfikującym prawdziwości danych nie jest daną osobową, natomiast login przypisany w zakładzie pracy według zasady *imię.nazwisko* pracownika lub przydzielony studentowi jako *numer indeksu* ma charakter danych osobowych.

Obecnie wiele usług wykonywanych dotychczas bezpośrednio (w sklepie, na poczcie, w banku, biurze podróży czy w przychodni lekarskiej) jest świadczonych przy pomocy przeglądarek internetowych, jak na przykład: zakupy, płatności, rezerwacje biletów czy sprawdzanie wyników medycznych badań laboratoryjnych. Użytkownicy Internetu pozostawiają ślady swojej aktywności w wielu miejscach i w różnych postaciach. Przykładowo, ich dane mogą być dostępne z plików *cookies*[5] lub z historii przeglądanych stron. Wszystkie usługi, których prowadzenie wymaga zbierania i przechowywania danych osobowych klientów (imię, nazwisko, dane kontaktowe i kart kredytowych, PESEL itd.), powinny być realizowane na odpowiednio zabezpieczonych serwerach, wykorzystywać programy szyfrujące

---

[3] Ustawa o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych z 9 kwietnia 2010 r. (Dz.U. nr 50, poz. 424).

[4] Ustawa o ochronie danych osobowych z 29 sierpnia 1997 r. (Dz.U. z 2002 r. nr 101, poz. 926).

[5] Pliki tekstowe zapisywane na dysku twardym użytkownika podczas odwiedzania stron WWW zawierające dane o użytkowniku w celu jego rozpoznawania i w celach statystycznych.

poufne treści przed ich wysyłaniem oraz być chronione przed nieuprawnionym dostępem.

3. Dostęp do danych osobowych i ich przetwarzanie

Dzięki centralnym bazom danych i rozbudowanym systemom informatycznym coraz więcej usług może być świadczonych drogą elektroniczną. Zgodnie z ustawą o świadczeniu takich usług – dane gromadzone na serwerach usługodawców muszą być chronione, a podczas transmisji szyfrowane.

Badania przeprowadzone przez agencję TNS Polska na zlecenie Krajowego Rejestru Długów Biura Informacji Gospodarczej (funkcjonującego pod bezpośrednim nadzorem Ministerstwa Gospodarki) wykazały, że 4 mln Polaków (13%) ma dłużników finansowych, na przykład zalegających z oddaniem długu (65%) lub z wypłacaniem pensji (17%). Dotychczas dane o dłużnikach były prawnie chronione. Zmieniła to ustawa o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych z 9 kwietnia 2010 roku, w której zdefiniowano pojęcie informacji gospodarczej oraz zezwolono osobom fizycznym na upublicznianie danych dłużników w rejestrach długów prowadzonych przez Biura Informacji Gospodarczej. Dotyczy to danych związanych z działalnością gospodarczą, a nie sferą prywatną, stąd na przykład nie powinien być ujawniany numer PESEL identyfikujący osobę fizyczną oraz adres zamieszkania (jeśli jest inny niż adres podmiotu gospodarczego).

Zmiany w zakresie przetwarzania danych są obserwowane w wielu różnych obszarach życia: tradycyjne indeksy studentów są zastępowane indeksami elektronicznymi, powstają elektroniczne protokoły sądowe, coraz powszechniejsze są e-dzienniki, e-faktury, e-bilety (lotnicze, kolejowe, do kina). Zmiany te są możliwe dzięki systemom baz danych i centralnym rejestrom danych, których zabezpieczanie ma najwyższy priorytet, gdyż uzyskanie nieuprawnionego dostępu do nich jest celem działania wielu przestępców i grup hakerskich.

W myśl obowiązujących przepisów osoby, których dane są gromadzone, mają prawo do uzyskania ich w czytelnej postaci oraz do uzyskania wyczerpujących informacji co do okresu ich przechowywania, źródła pozyskania, a także celu ich udostępniania. Zasada ta nie dotyczy danych niejawnych lub objętych tajemnicą zawodową.

Zgodnie z art. 7 ustawy o ochronie danych osobowych usunięcie danych to ich zniszczenie lub taka modyfikacja, by niemożliwe było ustalenie osoby, której dotyczą. Ustawa nie wymusza więc trwałego zniszczenia danych, tylko ich anonimizację, tak by ustalenie właściciela nie było możliwe bez nadmiernych nakładów kosztów, czasu i działań. Z tego powodu dane kont na portalach internetowych często są tylko ukrywane, a nie fizycznie usuwane, pomimo takiego żądania ze strony wła-

ściciela konta. Często skasowanie profilu polega na usunięciu lub zastąpieniu wartościami losowymi imienia i nazwiska (anonimizacja danych) i ograniczeniu do niego dostępu, natomiast nie oznacza zaprzestania ich przetwarzania (np. w celach statystycznych).

Zbiory danych tworzone przez pracodawców, władze i urzędy publiczne mogą zawierać tylko dane niezbędne do realizacji danego celu. Tworzone zbiory danych osobowych muszą być w Polsce zgłaszane do Generalnego Inspektora Ochrony Danych Osobowych (GIODO) oraz wpisane do ogólnokrajowego rejestru zbiorów danych osobowych. Obecnie do GIODO wpłynęło zapytanie odnośnie stosowanych od niedawna parkometrów, które wymagają podania numeru rejestracyjnego pojazdu. Zdaniem kierowców jest to nieadekwatne do potrzeb zbieranie danych naruszające ich prywatność.

Spośród danych osobowych szczególnej ochronie podlegają dane wrażliwe, do których należą poglądy polityczne, przekonania religijne lub filozoficzne, przynależność partyjna, związkowa, wyznaniowa, pochodzenie rasowe lub etniczne, dane o stanie zdrowia, nałogach, życiu seksualnym, kodzie genetycznym, dane dotyczące karalności. Dane wrażliwe można gromadzić i przetwarzać, jeśli jest to prawnie uzasadnione.

Wprowadzanie nowych technologii wykorzystujących techniki biometryczne (ułatwiających między innymi automatyczną identyfikację osób przy kontroli wejść i wyjść oraz czasu pracy) powoduje gromadzenie przez pracodawców wizerunków twarzy i odcisków palców pracowników. Jednak ze względu na dobro pracownika dane biometryczne mogą być wykorzystywane tylko za jego zgodą.

Technologie usprawniające zarządzanie danymi i ich kontrolę umożliwiają także ich niekontrolowane kopiowanie, modyfikowanie i szybkie rozprzestrzenianie. Wszelkiego rodzaju tzw. gadżety szpiegowskie, które można legalnie nabyć, typu miniaturowe kamery, aparaty cyfrowe, dyktafony czy chipy RFID[6], wbudowane w różne przedmioty (np. guziki, zapalniczki, długopisy, zegarki, okulary, obrazy), umożliwiają w sposób niezauważalny sfotografowanie czy sfilmowanie także obiektów i dokumentów pilnie strzeżonych (zadań egzaminacyjnych, danych osobowych, projektów technologicznych, danych medycznych czy finansowych). Na przykład niewielkich rozmiarów (64 x 20 x 7 mm) pendrive-dyktafon o pojemności 4 GB umożliwia zapis nagrania z 240 godzin[7].

Miniaturowe urządzenia aktywowane głosem umożliwiają zdalny podsłuch, a więc również przechwytywanie strzeżonych danych. Monitorowanie działań wykonywanych na komputerze umożliwia na przykład Spy Logger, czyli pendrive z programem rejestrującym uruchamiane aplikacje, odwiedzane strony internetowe

---

[6] Chip RFID (*Radio-frequency identification*) – urządzenie o niewielkich rozmiarach umożliwiające automatyczną identyfikację obiektu z wykorzystaniem fal radiowych.

[7] www.sternal.co [dostep8.01.2013].

i naciskane klawisze, także wykonującym zrzuty ekranu, a nawet nagrywającym rozmowy prowadzone przez komunikatory internetowe oraz dźwięki słyszalne wokół komputera.

Odpowiednio z rozwojem urządzeń szpiegujących rośnie rynek wykrywaczy podsłuchów, kamer, zagłuszaczy odbiorników, lokalizatorów i tym podobnych urządzeń.

4. Zarządzanie tożsamością i dostępem

W celu prawidłowego zarządzania prawami dostępu do danych, określanego jako zarządzanie tożsamością i dostępem (*Identity & Access Management* – IAM) należy opracować, i ich przestrzegać, procedury precyzujące, kto i do jakich systemów i zasobów danych może mieć dostęp oraz jakie czynności może na nich wykonywać. Zakres dostępu powinien być zawsze minimalny, a jednocześnie wystarczający do wykonania powierzonych zadań i obowiązków (*least privilege*). Skuteczne planowanie, zarządzanie oraz kontrolowanie dostępu do systemów i danych wymaga stosowania scentralizowanych rozwiązań informatycznych w przedsiębiorstwie umożliwiających wygodne konfigurowanie kont i praw dostępu oraz monitorowanie działań użytkowników.

Rozwiązania IAM muszą zapewniać działania zgodne z przepisami prawnymi i branżowymi. Za bezpieczeństwo przetwarzania danych osobowych w systemie informatycznym odpowiada administrator danych nadający uprawnienia dostępu do danych poszczególnym osobom. Natomiast nadzór nad przestrzeganiem zasad w zakresie ochrony danych sprawuje administrator bezpieczeństwa informacji.

5. Ochrona danych a regulaminy dostawców usług elektronicznych

Wraz z rozwojem serwisów społecznościowych, które skupiają miliony użytkowników (np. najpopularniejszy z nich Facebook liczy 1 mld kont[8]), nastąpiło masowe upublicznianie danych (w postaci tekstowej, zdjęć i filmów), nieznane dotąd na tak szeroką skalę.

Także z innych usług internetowych, głównie e-sklepów i e-banków, korzysta coraz więcej Polaków. Z zamieszczonych na portalu GoDealla[9] statystyk wynika, że w Polsce uruchomiono 167 serwisów zakupów grupowych (stan na dzień 30.11.2012 r.). Z raportu NetB@nk przygotowanego przez Związek Banków Pol-

[8] Miliard użytkowników Facebooka, www.rp.pl/artykul/939357.html [dostęp 4.10.2012].

[9] www.godealla.pl/blog/ciekawostki-ze-swiata-zakupow-grupowych-w-polsce-i-na-swiecie -cz-1 [dostęp 30.11.2012].

skich wynika, że z bankowości internetowej w Polsce korzysta ponad 10,7 mln indywidualnych klientów oraz 1,1 mln firm[10]. Tymczasem publikowane regulaminy dotyczące usług elektronicznych są często bardzo długie, niezrozumiałe, nieprecyzyjne i zniechęcają użytkowników do ich przeczytania. Celem tych regulaminów jest przede wszystkich zabezpieczanie usługodawców przed ewentualnymi roszczeniami niezadowolonych klientów.

Problem jest poważny, gdyż rozwój e-gospodarki spowodował przeniesienie wielu form działalności do Internetu i korzystanie z e-usług w wielu sytuacjach stało się koniecznością.

Od czerwca 2012 roku prowadzony jest projekt ToS;DR (*Terms of Service; Didn't Read*), którego celem jest ocena zamieszczanych w Internecie regulaminów usługodawców w skali od A (ocena najwyższa) do E (ocena najniższa) pod kątem rzetelności, zwięzłości, czytelności i tym podobnych parametrów. Dotychczas oceniono 7 regulaminów z 61 zaplanowanych. Na stronie projektu[11] umieszczona jest lista ocenionych regulaminów wybranych portali, i na przykład portal Twitpic, ograniczający możliwość dochodzenia swoich praw przez użytkownika i wymagający zgody na dysponowanie zamieszczanymi treściami, dostał ocenę najniższą E.

Popularna bezpłatna aplikacja Instagram, po zainstalowaniu na komputerze, umożliwia założenie konta i dzielenie się zdjęciami z innymi użytkownikami programu. Istnieje jednak obawa o darmowe wykorzystywanie zamieszczanych przez użytkowników zdjęć i handel nimi. Regulamin tego programu wymaga zgody właściciela konta na wykorzystywanie jego zawartości bez żadnych rekompensat (nawet gdy zarządzający Instagramem je sprzeda).

6. Usługa geolokalizacji a ochrona prywatności

Systemy geolokalizacyjne, umożliwiające ustalenie położenia obiektu (osoby, samochodu, telefonu itd.), wykorzystują system nawigacji satelitarnej GPS (*Global Positioning System*). Urządzenia mobilne wyposażone w odbiornik GPS i odpowiednie aplikacje umożliwiają przekazywanie danych geolokalizacyjnych do portali społecznościowych. Taką funkcjonalność oferuje serwis społecznościowy Foursquare (4 mln kont) oraz Facebook (usługa *Places*). Lokalizację położenia można włączyć np. w komunikatorze Empathy i, w zależności od oprogramowania, infrastruktury i rodzaju sieci, przekazywać zebrane dane, takie jak kraj, region, położenie, obszar, ulica, budynek, długość i szerokość geograficzna, wysokość nad poziomem morza, prędkość i kierunek ruchu.

---

[10] Raport: bankowość internetowa i płatności bezgotówkowe. Podsumowanie II kwartału 2012 roku. NetB@nk, Warszawa, 2012.

[11] http://tos-dr.info [dostęp 8.01.2013].

Położenie geograficzne komputera może być ustalone przez wiele różnych programów i stron internetowych. Na przykład portal moje.ip informuje o numerze IP komputera i jego szczegółowych danych, w tym geolokalizacyjnych. Przeglądarka Mozilla Firefox pobiera dane o położeniu geograficznym użytkownika w celu inteligentnej personalizacji dostarczanych treści (np. reklam czy wyszukiwanych stron w zależności od kraju i miasta). Operatorzy telefoniczni zachęcają abonentów do instalowania odpowiedniego oprogramowania informującego o miejscu pobytu wybranych osób.

Zalety usług geolokalizacyjnych są oczywiste, ale ich użycie bez wiedzy zainteresowanego nie może mieć miejsca, zatem musi istnieć opcja wyłączenia tej funkcji. Tymczasem na przykład w Brazylii od 2011 roku wszystkie rejestrowane samochody muszą mieć zainstalowany GPS oraz chip RFID, z których dane są przekazywane do ministerstwa transportu i policji. Ma to na celu zapobieganie kradzieżom i szybkie lokalizowanie pojazdów, niestety narusza prywatność obywateli.

Automatyczna identyfikacja, geolokalizacja, monitoring i inne podobne rozwiązania muszą być stosowane rozważnie, adekwatnie do potrzeb.

Podsumowanie

Dzięki nowoczesnym technologiom istnieje możliwość niezauważalnego zbierania i przechowywania danych o obywatelach, monitorowanie ich zakupów, stylu życia, upodobań itp. Powinna jednak być zachowana równowaga pomiędzy stosowaniem nowych technologii w imię zapewnienia bezpieczeństwa i wygody obywateli, a ingerencją w ich prywatność.

Technologie bezprzewodowe i mobilne oraz automatycznej identyfikacji znacznie upraszczają i przyspieszają wykonywane prace (handlowe, finansowe, zabezpieczające, monitorujące i identyfikujące). Konieczne jest jednak podczas ich stosowania zapewnienie jak najwyższego poziomu bezpieczeństwa wykorzystywanych danych.

Coraz szerszy zasięg elektronicznego przetwarzania danych osobowych wymaga szczególnego skupienia uwagi na zapewnieniu bezpieczeństwa systemów informatycznych oraz opracowania odpowiednich regulacji prawnych.

Literatura

1. http://tos-dr.info.
2. *Miliard użytkowników Facebooka*, www.rp.pl/artykul/939357.html [dostęp 4.10.2012].

3. Raport: bankowość internetowa i płatności bezgotówkowe. Podsumowanie II kwartału 2012 roku. NetB@nk, Warszawa, 2012.
4. Ustawa o ochronie danych osobowych z 29 sierpnia 1997 r. (Dz.U. z 2002 r. nr 101, poz. 926), Warszawa.
5. Ustawa o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych z 9 kwietnia 2010 r. (Dz.U. nr 50, poz. 424).
6. www.giodo.gov.pl/560/id_art/4177/j/pl [dostęp 8.01.2013].
7. www.godealla.pl/blog/ciekawostki-ze-swiata-zakupow-grupowych-w-polsce-i-na-swiecie-cz-1.
8. www.sternal.co.

PROCESSING AND SECURITY OF PERSONAL DATA IN THE AGE OF E-COMMERCE

Summary

The development of e-commerce has changed the way of running many businesses. Data that are gathered and processed with IT systems for the purpose of offering online services often require special protection. Modern technology allows unnoticed collection of data about citizens. However, there should be a balance maintained between ensuring the security and convenience of citizens, and privacy incursion.

Translated by Zygmunt Mazur