JOURNAL of COMPUTER SCIENCES INSTITUTE

JCSI 4 (2017) 108-111
Wysłane: 2017-01-07
Przyjęte: 2017-01-18

Ochrona danych osobowych w ujęciu przepisów państwa Polskiego a organu Generalnego Inspektora Ochrony Danych Osobowych

Damian Harasim*

Politechnika Lubelska, Instytut Informatyki, Nadbystrzycka 36B, 20-618 Lublin, Polska

Streszczenie. Artykuł opisuje oraz rozwija zagadnienie danych osobowych oraz ich współczesnej ochrony. Przedstawia organ Generalnego Inspektora Ochrony Danych Osobowych, pracy Biura Inspektora oraz prezentuje przykładowe wyniki ich pracy. Dla artykułu zostało przeprowadzone badanie ankietowe polegające na zbadaniu małej grupy osób w celu potwierdzenia słuszności działalności instytucji.

Słowa kluczowe: GIODO; dane osobowe; ochrona

*Autor do korespondencji.

Adres e-mail: damian.harasim@pollub.edu.pl

Personal data protection in terms of provisions of the Polish state and the authority of the General for Personal Data Protection

Damian Harasim*

Institute of Computer Science, Lublin University of Technology, Nadbystrzycka 36B, 20-618 Lublin, Poland

Abstract. The article describing and expand issue personal data and their contemporary protection. Present apparatus the Inspector General for Personal Data Protection and show example results of their work. For the article was conducted survey consisting in examining the small Group of people in order to confirm the rightness activity of the institutions.

Keywords: GIODO; personal data, protecting

*Corresponding author.

E-mail address: damian.harasim@pollub.edu.pl

1. Wstęp

W ostatnich latach mogliśmy zaobserwować wzmożone wysiłki pojedynczych osób lub całych grup hackerskich wykradających głównie bardzo cenne informacje, na które w głównej mierze składały się chronione prawnie dane osobowe. Niejednokrotnie pojedyncze wycieki zawierały nie tylko dane teleadresowe, ale i również numery kont bankowych czy kart kredytowych. W 2016 roku, słynny serwis Yahoo oficjalnie poinformował, że w 2014 jego serwery padły ofiarą ataku a do sieci wyciekły informacje o koło 500 milionach kont użytkowników zawierających takie dane jak: loginy, adresy e-mail, numery telefonów, daty urodzin czy kryptograficznie zabezpieczone hasła [1]. Są to oczywiście zjawiska bardzo niebezpieczne dla osób, których dane zostały wykradzione, gdyż w skrajnych przypadkach mogą prowadzić do defraudacji pieniędzy z kont bankowych.

2. Generalny Inspektorat Ochrony Danych Osobowych.

Polska posiada w swoich aparatach państwowych organ, jakim jest Generalny Inspektor Ochrony Danych Osobowych, w skrócie GIODO. W jego skład wchodzi pięć departamentów:

1) Departament Rejestracji
2) Departament Prawny
3) Departament Inspekcji
4) Departament Informatyki
5) Departament Skarg

Samo GIODO, najprościej ujmując, jest to jednoosobowe stanowisko, a osoby na nie są powoływane na 4 letnią kadencję przez Sejm Rzeczpospolitej Polskiej. Dotychczas urząd ten sprawowało sześciu Inspektorów, obecnie jest to Pani Edyta Bielak-Jamaa, wybrana 22 kwietnia 2015 roku. Inspektor realizuje swoją pracę poprzez Biuro Generalnego Inspektora Danych Osobowych a obowiązki Inspektora znajdują się w art. 12 ustawy o ochronie danych osobowych z 1997 roku [2]. Poza tym, Generalny Inspektor zajmuje się prowadzeniem ogólnokrajowego, jawnego rejestru zbioru danych osobowych zgłoszonych do rejestracji, art. 42 ust. 1 powyższej ustawy.

2.1. Dane osobowe

Za dane osobowe w rozumieniu litery prawa, uważa się każdą informację jaka może umożliwić identyfikację lub prowadzić do umożliwienia identyfikacji osoby fizycznej, przy czym należy zaznaczyć, iż nie istnieje prawnie określony zbiór, jakie dane mogą być danymi osobowymi. I nie chodzi tutaj o jednolitą informację, na przykład konkretnie identyfikujący wiersz w bazie danych a również o relacje pomiędzy tabelami w bazie, których złożenie prowadzi do identyfikacji podmiotu. Samo przetwarzanie takich danych również jest szeroko pojętym procesem. Na szczęście jego definicja została zawarta w art. 7 ust. 2 ustawy o ochronie danych osobowych i kryją się pod tym jakiekolwiek operacje wykonywane na danych osobowych.

Biuro Generalnego Inspektora opublikowało na swojej stronie internetowej [3], szereg „odpowiedzi na pytania" gdzie znajdują się wytyczne mogące pomóc w zrozumieniu tego problemu. I tak, możemy się dowiedzieć iż administrator danych do przetwarzania danych osobowych zgodnie z przepisami „musi spełniać przynajmniej jeden z warunków decydujący o tym, że takie działanie jest legalne", dopełnił obowiązku zgłoszenia zbioru danych do rejestracji GIODO (poza wyjątkami z art. 43 ust.1 ptk.1-11 ustawy o ochronie danych osobowych), stosował środki techniczne oraz organizacyjne zapewniające przetwarzanym danym odpowiedni poziom bezpieczeństwa, dopełnił obowiązku informacyjnego, dokonał szczególnej staranności w celu ochrony interesów osób, których dane dotyczą oraz respektował prawa osób, których dane dotyczą [4]. Powyższy opis stanowiska, będący wyjaśnieniem jednego z artykułów ustawy, jest jednym z wielu jakie może znaleźć w interpretacjach Głównego Inspektora.

Wracając do danych osobowych, warto zwrócić uwagę na ich interpretację przez GIODO. Zostało wcześniej powiedziane, iż nie istnieją żadne ustawowo spisane zbiory jakie dane są danymi osobowymi a więc ich interpretacja może być różna, w zależności od poziomu jej zrozumienia.

GIODO na swojej stronie internetowej umieścił zbiór kilku przykładowych danych osobowych, jakie On uznaje (a niektóre jedynie w pewnych sytuacjach) za dane osobowe. I tak możemy za dane osobowe wg. GIODO uznać:

1) Numer IP
2) Numer PESEL
3) Numer telefonu
4) Adres e-mail
5) Numer rachunku bankowego

Na tle powyższego zestawienia ciekawie prezentuje się numer VIN pojazdu [5]. Art.6 ustawy o ochronie danych osobowych stwierdza, iż za informację osobową nie uważa się danych, dzięki którym określenie osoby fizycznej wymaga nadmiernych kosztów, czasu lub działań. I tak, dla przeciętnego człowieka taki numer nie stanowi informacji na podstawie której można zidentyfikować konkretną osobę. Jednakże już dla administratora danych jakim będzie w tym wypadku minister właściwy do spraw administracji publicznej, numer VIN stanowi jedną z wielu powiązanych ze sobą informacji jakie posiada wraz z tym numerem. I to właśnie dla niego, taka składowa będzie uznawana za daną osobową, gdyż nie wymaga to od niego wyłożenia nadmiernych kosztów na jej uzyskanie.

2.2. Biometria

W kontekście danych osobowych warto wspomnieć o coraz popularniejszej metodzie autoryzacji – biometrii. Chociaż jest to dość nowa metodyka dążąca do zbierania fizycznych danych, również podlega ustawie o ochronie danych osobowych ponieważ w myśl art. 6 ust. 2, zbiera ludzkie cechy fizyczne.

Dotychczas sposób dostępu do komputera, telefonu czy konta bankowego polegał na ustaleniu pary login + hasło, pojedynczego numeru PIN, profilu zaufanego bądź podaniu zestawu danych w czasie wizyty w oddziale banku lub infolinii. Biometria pozwoliła na znaczne uproszczenie tego procesu, wystarczy nam odcisk kciuka przyłożonego do czytnika, jak np. w telefonach marki Apple czy Samsung zawierających dedykowane czytniki linii papilarnych. Jednak taki poziom wygody może nie koniecznie iść z bezpieczeństwem danych. Jak bardzo może być to niebezpieczne zjawisko, dowiedzieliśmy się w 2014 roku w czasie konferencji zatytułowanej „Chaos Communication Congress". W jej czasie, Jan Krissler jedynie na podstawie zwykłych zdjęć dokonał rekonstrukcji odcisku palca niemieckiej minister obrony Ursuli Gertrud von den Leyen [8]. Jest to jeden z wielu obecnie przykładów słabości zabezpieczenia dostępu poprzez odcisk palca. A przecież dotykając przeróżnych codziennych przedmiotów, odciski pozostają wszędzie. Na szczęście biometria nie stoi w miejscu i ewoluuje. Do dzisiaj doczekaliśmy się np. biometrii „Finger Vein" wykorzystującej unikalny dla każdej osoby, układ naczyń krwionośnych znajdujących się wewnątrz jej palca. Rozwiązanie zostało zastrzeżone patentem US7526111 B2. Jest to nie zależne od wieku ułożenie naczyń na których wpływ może mieć jedynie choroba. Z takiego rozwiązania coraz częściej korzystają instytucje bankowe, a przykładem może być bank BPH który od stycznia 2013 roku korzysta z tej technologii do uwierzytelniania klientów banku.

GIODO w swoim raporcie [7] cytuje bardzo ciekawą opinie Grupy Roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Twierdzi ona, iż wraz z rozwojem biotechnologii rodzi się niepokój związany ze zmniejszeniem wrażliwości ludzi, będącego wynikiem ekspansji w życiu codziennym tego rozwiązania. I trudno się tej opinii nie dziwić. Rosnąca akceptacja społeczna jest motorem napędowym większości innowacji na rynku. Jednakże filarem danych biometrycznych jest ich niezmienność, co jest przeciwieństwem zabezpieczeń znanym nam dotychczas. Polityki bezpieczeństwa korporacji kładą dość wysoki nacisk na częstą zmianę haseł oraz ich różnorodność (na przykład blokada ponownego użycia haseł z ostatnich 12 miesięcy).

3. Badanie

Badanie przeprowadzone w ramach tej pracy, polegało na udowodnieniu następującej hipotezy: „Przeciętna osoba jest w stanie rozpoznać poprawnie prawidłowe dane osobowe opierając się wyłącznie na treści artykułu ustawy." Zostało ono przeprowadzone dnia 16 grudnia oraz 4 stycznia na terenie kampusu Politechniki Lubelskiej oraz ankiety internetowej, pośród studentów wydziału Elektrotechniki i Informatyki. Łącznie w badaniu brało udział 16 przypadkowo wybranych osób. Pytania zostały oparte o wcześniej zaopiniowane dane osobowe oraz ogólne przez Generalnego Inspektora. Miało to na celu możliwe zanegowanie postawionej wcześniej hipotezy.

Ankieta była całkowicie anonimowa oraz zawierała 8 pytań, na których odpowiedzi należało oznaczyć obrysowując obwódką bądź przekreślając poprawną odpowiedź. Ankieta zawierała krótki opis wstępu wraz z instrukcją wypełnienia, przytoczony art. 6 ustawy o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz następujące pytania:

1) Płeć
2) Czy pracowałeś/łaś lub nadal pracujesz?

3) Czy miałeś styczność z pojęciem „danych osobowych”?
Czy Twoim zdaniem za dane osobowe:
4) Uznaje się numer telefonu?
5) Uznaje się numer rachunku bankowego?
6) Nie uznaje się numeru IP?
7) Nie uznaje się numeru karty miejskiej?
8) Uznaje się numer VIN pojazdu?

Uczestnicy do wyboru mieli następujące odpowiedzi. Dla pytania pierwszego: „Mężczyzna” lub „Kobieta”, dla pytania drugiego oraz trzeciego: „Tak” lub „Nie” oraz na pytania od czwartego do ósmego: „Tak”, „Nie”, „Zależy”, gdzie pod odpowiedzią „Zależy” zgodnie z opisem zawartym w ankiecie, należało rozumieć dane, jakie przytacza art. 6 ust. 3. Pytanie 5 oraz 6 zostały celowo sformułowane w kontekście negacji by lepiej sprawdzić zrozumienie ustawy.

3.1. Wyniki badania

Legenda: Pytanie 1: M – „Mężczyzna”, K – „Kobieta”; dla pytań 2-8: T – „Tak”, N – „Nie”, Z –„Zależy”

Tabela 1. Wyniki ankiety

	Pytanie	Pytanie	Pytanie	Pytanie	Pytanie	Pytanie	Pytanie	Pytanie
Osoba 1	M	T	T	T	T	N	T	N
Osoba 2	K	T	T	Z	Z	Z	Z	N
Osoba 3	M	T	T	T	T	N	N	N
Osoba 4	M	T	T	T	T	T	T	N
Osoba 5	M	N	N	Z	Z	T	N	N
Osoba 6	M	N	T	T	Z	T	T	N
Osoba 7	M	N	N	T	T	T	T	N
Osoba 8	M	N	T	T	T	T	T	N
Osoba 9	M	N	T	T	T	T	T	N
Osoba 10	M	T	T	T	T	T	T	N
Osoba 11	M	T	T	T	T	N	N	T
Osoba 12	M	N	T	T	T	N	T	N
Osoba 13	M	N	T	T	T	N	T	N
Osoba 14	M	N	T	T	T	N	T	N
Osoba 15	M	N	T	T	T	T	T	N
Osoba 16	M	N	T	T	Z	Z	T	N

Otrzymane wyniki nie dają nam konkretnej odpowiedzi na postawioną wcześniej hipotezę, ale mimo wszystko rezultaty są ciekawe. 37,5% badanych aktualnie pracuje lub wcześniej pracowało i każdy z nich spotkał się do tej pory z pojęciem danych osobowych. Jednakże już tylko 80% uczestników znajdujących się w grupie niepracujących, miało styczność z tym pojęciem. Jest to zaskakujący rezultat, nawet pomimo tak małej grupy ankietowej. Badania były przeprowadzane na wydziale uczelni technicznej, na którym nie powinno być ono dla nikogo obce. Można wysnuć hipotezę, iż konkretnych przepisów czy ich interpretacji, młodzi ludzi uczą się dopiero w czasie swoich początków kariery zawodowej, pomimo, iż są studentami i powinni na własną rękę zdobywać wiedzę z takich zagadnień.

Daje nam to obraz mniej więcej następujący obraz sytuacji. Wiedza społeczeństwa wciąż rośnie, zdecydowanie można stwierdzić, iż każdy współczesny człowiek jest bardziej doinformowany i świadomy otaczającego go świata od swoich rodziców. Dostęp do informacji dzięki powszechności telewizji, radia oraz Internetu ma ku temu niezaprzeczalny wpływ. Jednak opierając się na grupie ankietowej, ludzie nie zdają sobie sprawy z pojęcia danych osobowych. Można uznać to za błahostkę, jednakże ciężko uznać, iż wynika to z ludzkiego pojęcia na ten temat. O ile numer telefonu oraz rachunek bankowy został jednoznacznie uznany za daną osobową co jest w pewnym stopniu logicznie uzasadnione, gdyż o wadze tych informacji jesteśmy informowani już na etapie podpisywania umów czy to z bankiem czy operatorem sieci telefonicznej. Tym bardziej, iż od 2017 roku, każda karta SIM musi być zarejestrowana, co wynika z ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. 2016 poz. 904) [10], a użytkownicy telefonów komórkowych, poza oferowanymi profitami wiążącymi się z przeniesieniem numeru, mają też obowiązek wyrazić zgodę na przetwarzanie danych osobowych – a co z tym się wiąże – zapoznania się z tym, co jest uważane przez operatora za dane osobowe, zwyczajowo w paragrafach zawierających politykę prywatności. Odmiennie prezentuje się numer IP, który jest uważany za daną ogólną. GIODO w swoim opracowaniu pt. „ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych” [6,9] stwierdza, iż sam numer IP jest elementem, jaki może posłużyć do identyfikacji osoby fizycznej. Na przykład zestawiając abonenta internetowego z informacją o abonencie telefonicznym otrzymujemy dane osobowe wprost identyfikujące osobę. Trzy z pośród 11 osób jednoznacznie uznało adres IP za daną osobową i tylko jedna opowiedziała zgodnie z opinią GIODO, iż zależy od sytuacji. Podobnie ma się sytuacja z numerem VIN gdzie 100% osób udzieliło odpowiedzi innej, niż ta zaopiniowana przez Generalnego Inspektora.

4. Wnioski

Jest złudną nadzieją, iż dane przetrzymywane na serwerach różnych instytucji są w pełni zabezpieczone przed nieautoryzowanym dostępem osób trzecich. Należy mieć na uwadze, iż badanie zostało przeprowadzone dla małej liczby osób co może prowadzić do wyciągnięcia mylnych wniosków w stosunku do ogółu społeczeństwa. Ankieta ukazała problem jakim jest ogólny brak wiedzy z zakresu ochrony danych osobowych, z rozpoznaniem informacji będących danymi chronionymi a ogólnymi. Instytucje publiczne jak i prywatne radzą sobie z tym problemem na wiele sposobów od wprowadzenia wewnętrznych umów poufności po wdrażanie polityki bezpieczeństwa informacji. Jednakże istnieją odgórne aparaty państwowe stojące na straży poufności informacji oraz służące pomocą w precyzowaniu przepisów prawa. GIODO jest dla nas szczególnie ważnym organem a jego obowiązki z roku na rok rosną z powodu rozwoju branży technologicznej. Przepisy prawne są konstruowane w sposób dość ogólny, by sprawdzać się w jak największej ilości przypadków co powoduje nie rzadko problemy z jego interpretacją lub powoduje błędy w interpretacji. GIODO staje na straży poprawnego rozumienia ustaw w swoim zakresie kompetencji.

Dzięki niemu i jego mocy opiniowania ustaw osoby fizyczne jak i podmioty mogą korzystać z jasno uzasadnionych wytłumaczeń często powielanych problemów interpretacyjnych.

Literatura

[1] Yahoo Security Notice September 22, 2016, https://help.yahoo.com/kb/account/sln28092.html [27.12.2016]

[2] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, http://isip.sejm.gov.pl/DetailsServlet?id=WDU19971330883 [27.12.2016]

[3] Odpowiedzi na pytania dotyczące ustawy o ochronie danych osobowych, http://www.giodo.gov.pl/317/j/pl/ [27.12.2016]

[4] Jakie warunki musi spełnić administrator danych, aby przetwarzać dane osobowe zgodnie z ustawą o ochronie danych osobowych, http://www.giodo.gov.pl/317/id_art/3201/j/pl/ [27.12.2016]

[5] Czy numer vin pojazdu stanowi dane osobowe w rozumieniu ustawy o ochronie danych osobowych?, http://www.giodo.gov.pl/319/id_art/2836/j/pl/ [27.12.2016]

[6] Czy adres ip komputera należy do danych osobowych?, http://www.giodo.gov.pl/319/id_art/2258/j/pl/ [27.12.2016]

[7] Raport o ochronie danych osobowych GIODO, http://www.giodo.gov.pl/plik/id_p/10383/j/pl/ [27.12.2016]

[8] Rekonstrukcja odcisku palca niemieckiej minister obrony Ursuli Gertrud von den Leyen, wideo z konferencji, https://www.youtube.com/watch?v=VVxL9ymiyAU [27.12.2016]

[9] Abc zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych, http://www.giodo.gov.pl/plik/id_p/1560/j/pl/ [27.12.2016]

[10] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20160000904 [27.12.2016]

[11] Sakowska-Baryła M., Kontrolowanie przez GIODO przetwarzania danych osobowych, „Kontrola Państwowa" 2016, nr 2, s. 28-46

[12] Przywora B., Z problematyki kontroli przetwarzania i ochrony danych osobowych przez Generalnego Inspektora Ochrony Danych Osobowych. Jawność i jej ogranicznia. Zadania i kompetencje (red. Szmulik B., Szpor G.), C.H. Beck, Warszawa 2015, Wyd. I, stron 400, ISBN 978-83-255-7664-6.

[13] Kawecki M., Generalny Inspektor Ochrony Danych Osobowych jako centralny organ administracji państwowej, Przegląd Prawa Technologii Informacyjnych ICT Law Review z 2013 r. Wyd. I.

[14] Byrski J., Tajemnica prawnie chroniona w działalności bankowej, Wydawnictwo C.H. Beck, Warszawa 2010, stron 417, ISBN: 978-83-255-1892-9

[15] Krzysztofek M., Tajemnica bankowa i ochrona danych osobowych w praktyce bankowej, Wyd. LexisNexis, Warszawa 2010, stron 324, ISBN: 9788376203249