Bezpieczeństwo danych osobowych

obecnie i zgodnie z

RODO

experto24.pl

Spis treści

Bezpieczeństwo to podstawa potrzeba każdego człowieka od momentu urodzenia aż po kres życia. Pojęcie „bezpieczeństwo" wywodzi się z łacińskiego *sine cura* i oznacza stan bezpieczny. W literaturze funkcjonuje wiele definicji bezpieczeństwa. Ich różnorodność wynika przede wszystkim z tego, że pojęcie to jest interdyscyplinarne i dotyczy wielu różnych obszarów zainteresowania nauki.

Abraham Maslow umieścił bezpieczeństwo jako fundamentalną potrzebę ludzką tuż za potrzebami fizjologicznymi. Innymi potrzebami ujętymi przez niego w piramidzie potrzeb człowieka są potrzeba afiliacji, potrzeba uznania czy samorealizacji. Warto także podkreślić, że jest to również podstawowa potrzeba państwa czy społeczności międzynarodowej.

Dążenie do zapewnienia bezpieczeństwa zbiorowego zyskało na znaczeniu po I wojnie światowej, niemniej jednak na jego rozwój zdecydowany wpływ miały doświadczenia II wojny światowej. Tragiczna w skutkach przyczyniała się bowiem do podjęcia zdecydowanych działań zmierzających do zapewnienia bezpieczeństwa zbiorowego przez budowę międzynarodowej organizacji rządowej, która miała je zapewnić. Konsekwencją tych działań było powstanie w 1945 roku Organizacji Narodów Zjednoczonych (ONZ).

Pojęcie „bezpieczeństwo" jest nierozerwalnie związane z zagrożeniami. Jak podkreśla J. Kuniowski, bezpieczeństwo ma ścisły związek z zagrożeniami, czyli sytuacjami, w których istnieje prawdopodobieństwo wystąpienia stanu niebezpiecznego dla człowieka (J. Kuniowski, *Bezpieczeństwo i zagrożenia współczesnego człowieka* (w:) *Bezpieczeństwo człowieka a proces transformacji systemowej*, J. Dębowski, E. Jarmocha, A. Świderski, Akademia Podlaska, Siedlce 2006, s. 93). Te zaś ulegają ciągłej ewolucji, o czym świadczy chociażby powstanie cyberprzestrzeni, w której funkcjonuje wiele nowych, nieznanych dotąd zagrożeń. To zaś przyczyniło się do redefinicji terminu „bezpieczeństwo". Cechą charakterystyczną współczesnych zagrożeń jest ich globalny zasięg. Terroryzm, międzynarodowa przestępczość gospodarcza, handel ludźmi to tylko niektóre przykłady zagrożeń, z którymi pojedyncze państwo nie jest w stanie sobie poradzić. Skuteczna walka wymaga zaangażowania większej liczby podmiotów, a w niektórych sytuacjach także całej społeczności międzynarodowej. Także zagrożenia

naturalne jak susze, powodzie, huragany chociaż występują lokalnie, w coraz szerszym zakresie dotyczą całej społeczności międzynarodowej, zwłaszcza w przypadku walki z nimi.

Jak zostało zauważone, rozwój społeczeństwa informacyjnego, a przede wszystkim powstanie Internetu, przyczynił się do powstania nowych zagrożeń, w tym chociażby wzrostu bezrobocia czy zagrożeń naturalnych, które w swych skutkach są coraz bardziej niszczycielskie i zmuszają niejednokrotnie ludność do przesiedleń. Innym realnym zagrożeniem, które w ostatnich latach zdominowało opinię publiczną, jest terroryzm. Zagrożenie to zyskało na znaczeniu po 2001 roku. Terroryzm rozprzestrzenia się bardzo szybko, nie powinien więc dziwić fakt, że występuje wiele różnych jego odmian. Czynnikami determinującymi jego rozwój są m.in. poszerzająca się dysproporcja pomiędzy państwami rozwiniętymi, rozwijającymi się a najmniej rozwiniętymi, różnice kulturowe oraz religijne. Cechą charakterystyczną terroryzmu jest dążenie do rozgłosu i sławy sprawców ataków. Te najczęściej przeprowadzane są w dużym skupisku ludzi, tak by swym zasięgiem objęły jak największą liczbę ofiar.

Nie ulega wątpliwości, że Internet to przestrzeń szczególnie podatna na zagrożenia. Ich cechą charakterystyczną jest skala, na jaką przestępstwa te są popełniane, krótki czas niezbędny do ich popełnienia oraz ogromna skala zniszczeń. Cyberzagrożenia przybierają różną postać w zależności od tego, jaki cel podmiot przeprowadzający atak chce osiągnąć. Problematyka zagrożeń w cyberprzestrzeni szczegółowiej zostanie opisana w kolejnych rozdziałach.

Na rozwój społeczeństwa informacyjnego warto jednak patrzeć szerszej, nowoczesne rozwiązania technologiczne, poza zagrożeniami przyczyniają się także bowiem do ułatwienia i przyspieszenia pracy człowieka, o czym świadczy chociażby rozwój robotyki.

1. Bezpieczeństwo jednostki

Kolejne dekady po utworzeniu ONZ doprowadziły do powstania licznych i nowych form współpracy zarówno o charakterze globalnym, jak i regionalnym, których podstawowym celem stało się dążenie do zapewnienia bezpieczeństwa. Cały czas jednak skupiano się na bezpieczeństwie w skali globalnej, nie koncentrując się na bezpieczeństwie poszczególnych osób fizycznych. Koncepcja bezpieczeństwa jednostki (*human security*), skupiając się ściśle na osobie fizycznej i jej najbliższym otoczeniu, zaczęła rozwijać się znacznie później. Po raz pierwszy pojęcie to zostało wykorzystane w 1994 roku w raporcie ONZ do spraw rozwoju (A. Czubaj, *Miejsce jednostki we współczesnym pojmowaniu bezpieczeństwa*, *O bezpieczeństwie obronności*, nr 1 (2) 2016 Siedlce, s. 61). W dokumencie podkreślono, że koncepcja ta znajduje odniesienie do wszystkich ludzi, niezależnie od miejsca, w którym się znajdują. W ocenie autorów raportu działanie zmierzające do zapewnienia bezpieczeństwa powinny mieć przede wszystkim wymiar prewencyjny, a nie interwencyjny (A. Czubaj, *Miejsce jednostki we współczesnym*

pojmowaniu bezpieczeństwa, *O bezpieczeństwie obronności*, nr 1 (2) 2016 Siedlce, s. 61). W literaturze przedmiotu *human security* dzieli się na dwie podstawowe szkoły: japońską oraz kanadyjską (A. Urbanek, *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, Słupsk 2013, s. 41–43). Koncepcja japońska oparta jest na założeniu *freedom for want*, kanadyjska zaś na podejściu *freedom for fear*.

Rozwój nowoczesnych rozwiązań technologicznych przyczynia się niewątpliwie do przyspieszenia i ułatwienia naszego życia, niemniej jednak wpływa także na rozwój nowych, nieznanych dotąd zagrożeń.

2. Bezpieczeństwo danych osobowych

Chociaż problematyka bezpieczeństwa jednostki jest stosunkowo młoda, zarówno na płaszczyźnie międzynarodowej, jak i krajowej funkcjonują przepisy, które ją regulują. Najistotniejszym z nich wydaje się art. 12 Powszechnej Deklaracji Praw Człowieka wskazujący, że „nie wolno ingerować samowolnie w czyjekolwiek życie prywatne, rodzinne, domowe ani w jego korespondencję, ani też uwłaczać jego honorowi lub dobremu imieniu. Każdy człowiek ma prawo do ochrony prawnej przeciwko takiej ingerencji lub uwłaczaniu" (Powszechna Deklaracja Praw Człowieka, przyjęta w Paryżu 10 grudnia 1948 r.). Standardy wypracowane w tym dokumencie zostały następnie powtórzone w art. 17 Międzynarodowego Paktu Praw Osobistych i Politycznych (MPPOiP) – Art. 17 Międzynarodowego Paktu Praw Osobistych i Politycznych (Dz.U. z 1977 r. nr 38 poz. 167), Nowy Jork, 16 grudnia 1966 r.

Dokumentem, który wywarł znaczący wpływ na rozwój przyszłego kształtu praw dotyczących wolności jednostki, była zawarta w 1950 roku przez państwa członkowskie Rady Europy Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności (EKPC) – Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie 4 listopada 1950 r., zmieniona następnie Protokołem nr 3, 5, 8 oraz uzupełniona Protokołem nr 2, Dz.U. z 1993 r. nr 61 poz. 284. Konwencja ta, po uzyskaniu niezbędnych dziesięciu ratyfikacji, weszła w życie 3 września 1953 r. Powyższe dokumenty odnosiły się do prawa jednostki do prywatności, uznając je za fundamentalne prawo przysługujące każdemu człowiekowi.

Niemniej jednak żaden z nich nie odnosi się bezpośrednio do prawa jednostki do ochrony danych osobowych. Dopiero wejście w życie Konwencji 108, następnie dyrektywy 95/46/WE zmieniły ten stan rzeczy w sposób zasadniczy. Oba dokumenty w całości zostały poświęcone mechanizmom prawnym gwarantującym bezpieczne przetwarzanie danych osobowych. O ile Konwencja 108 w ogólny sposób odnosi się do standardów, jakim powinien odpowiadać ten proces, o tyle dyrektywa 95/46/WE stała się drogowskazem, w jaki sposób państwa powinny kształtować ustawodawstwa krajowe. W tym celu zostały zobowiązane do implementacji dyrektywy. Potrzeba zapewnienia bezpieczeństwa wynikała

przede wszystkim z rozwoju zagrożeń, na które jesteśmy narażeni każdego dnia. Niestety w momencie przygotowania tekstu dyrektywy nie zdawano sobie sprawy, że rozwój technologiczny będzie tak dynamicznie się rozwijać, w związku z tym wiele zagrożeń nie zostało zidentyfikowanych, a co za tym idzie − nie wprowadzono mechanizmów prawnych gwarantujących bezpieczeństwo w tych obszarach.

Współcześnie bezpieczeństwo nie jest rozumiane wyłącznie w kategoriach wojskowych, politycznych czy gospodarczych. Coraz częściej dotyczy także funkcjonowania jednostki w cyberprzestrzeni.

Z raportu opublikowanego przez Deloitte w 2016 roku wynika, że najbardziej narażoną grupą internautów na ataki byli klienci banków głównie poprzez kampanie typu *phishing* oraz ataki *skimming* (M. Ludwiszewski, *Cyberbezpieczeństwo 2016, podsumowanie Deloitte*). Nowym, rosnącym w siłę zagrożeniem są rozwijające się także ataki na placówki służby zdrowia czy podmioty sektora motoryzacyjnego. Warto zwrócić uwagę, że zupełnie inny jest motyw działania hakerów w tych obszarach. Nakierowani są przede wszystkim na wymuszeniu okupu, wiedząc, że dane wrażliwe pacjentów dotyczące ich stanu zdrowia to cenne źródło wiedzy, które może stać się łakomym kąskiem dla wielu podmiotów (M. Ludwiszewski, *Cyberbezpieczeństwo 2016, podsumowanie Deloitte*). Z tego też powodu placówki medyczne często decydują się na płacenie okupów. Branża motoryzacyjna narażona jest na ataki obejmujące system otwierania pojazdu.

W dobie rozwoju społeczeństwa informacyjnego niezwykle trudno jest zapewnić bezpieczeństwo danych osobowych. Wynika to bowiem z faktu, że informacja o osobie jest dobrem równie cennym jak pieniądz. Każdego dnia powstają nowe, innowacyjne zabezpieczenia, które następnego dnia są łamane przez hakerów. Warto także pamiętać, iż najsłabszym ogniem jest człowiek, pomimo stosowania innowacyjnych rozwiązań bardzo często powodem wystąpienia incydentu jest działanie lub zaniechanie człowieka. Dobrze mieć również świadomość, że często nieświadomie sami narażamy się na naruszenie naszego prawa do prywatności, bezmyślnie umieszczając nasze dane na różnych portalach, mając złudne poczucie anonimowości. Tymczasem łączenie różnych informacji na nasz temat stanowi narzędzie do naruszenia prywatności.

Chociaż świadomość użytkowników wirtualnego świata stopniowo rośnie, nadal duża ich część uważa, że cyberzagrożenia ich nie dotyczą. Wielu administratorów nadal nie widzi potrzeby, by angażować środki finansowe w celu wprowadzenia lub poprawy systemów bezpieczeństwa. Jeżeli już decydują się na kroki w tym kierunku, często są to jednak najtańsze i najprostsze rozwiązania.

3. Bezpieczeństwo danych osobowych w ustawie o ochronie danych osobowych

Ustawa o ochronie danych osobowych (uodo), której kształt w dużej mierze wynikał z obowiązku dostosowania polskiego prawa do standardów Unii Europejskiej, wprost wskazuje w rozdziale 5, że administrator danych zobowiązany jest zapewnić środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36 uodo).

Bezpieczeństwo danych osobowych rozpatrywane jest na bazie trzech podstawowych cech: poufność, integralność i dostępność danych osobowych. Poufność danych zapewnia to, że jedynie uprawnione jednostki będą mieć dostęp do danych osobowych, integralność danych zapewnia ich spójność, a dostępność gwarantuje, że dostęp do danych osobowych mają wyłącznie upoważnione do tego osoby (Definicja zgodna z normą ISO/IEC 27001).

Aby zapewnić właściwy poziom bezpieczeństwa proporcjonalny do zagrożeń, ustawodawca nałożył na administratorów danych obowiązek prowadzenia odpowiedniej dokumentacji opisującej sposób przetwarzania danych osobowych (rozporządzenie ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. nr 100, poz. 1024).

Działania podejmowane w celu zapewnienia bezpieczeństwa danych osobowych mają przede wszystkim zapewnić ich ochronę przed wszelkimi działaniami niepożądanymi. W związku z tym, aby zapewnić właściwy proces przetwarzania danych osobowych, ustawodawca określił minimalne standardy, jakie powinny być wprowadzone w każdej jednostce organizacyjnej za pośrednictwem odpowiedniej dokumentacji.

Dodatkowo w § 7 rozporządzenia ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. nr 100, poz. 1024) określone zostały standardy, jakim powinna odpowiadać dokumentacja opisująca sposób przetwarzania danych osobowych, uwzględniając rodzaj przetwarzanych danych. W dokumentacji powinny zostać ujęte także mechanizmy, które pozwolą zabezpieczać dane osobowe przed możliwymi do wystąpienia zagrożeniami. Te zaś zostały określone według trzech poziomów: podstawowy, podwyższony oraz

wysoki. Wdrożenie odpowiedniej dokumentacji nie jest jednak wystarczające, aby zapewnić bezpieczeństwo danych osobowych w jednostce organizacyjnej. Warto uświadomić sobie, że bezpieczeństwo danych jest wypadkową wielu różnych procesów, w tym m.in. nadawania upoważnień do przetwarzania danych osobowych, prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, nadawania uprawnień do przetwarzania danych osobowych w systemach informatycznych.

Ważne jest także, by dokumentacja przygotowana przez administratora danych była właściwie wdrożona oraz by pracownicy zapoznali się z jej treścią. Każdy pracownik powinien także zostać przeszkolony w zakresie procedur ochrony danych osobowych funkcjonujących w jednostce organizacyjnej, a szkolenia te powinny być cyklicznie powtarzane i rozszerzane o nowe zagadnienia. W praktyce bowiem okazuje się, że zagadnienia takie jak sposób niszczenia dokumentów, częstotliwość zmiany haseł dostępu, stosowanie legalnych licencjonowanych programów antywirusowych to kwestie nadal bagatelizowane przez wielu administratorów danych.

4. Bezpieczeństwo danych osobowych w ogólnym rozporządzeniu o ochronie danych

Rozpoczęcie stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, rodo) nie zmieni w sposób diametralny standardów dotyczących bezpieczeństwa danych osobowych. Niemniej jednak każdy administrator danych zobowiązany będzie do zweryfikowania stworzonych procedur pod kątem tego rozporządzenia.

Rozporządzenie ogólne w dużej mierze oparte jest na analizie ryzyka. Oznacza to, że każdy administrator będzie musiał ocenić możliwe do wystąpienia zagrożenia oraz zastosować odpowiednie środki techniczne i organizacyjne już na etapie projektowania procesu przetwarzania danych osobowych. Zgodnie z artykułem 32 ust. 2 rodo: „oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych". Co za tym idzie − administrator danych zobowiązany będzie wdrożyć środki techniczne i organizacyjne proporcjonalne do możliwego do wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych.

Rozpoczęcie stosowania rozporządzenia ogólnego w wielu obszarach nakłada na administratorów nowe obowiązki, w tym m.in.: obowiązek informowania organu nadzorczego oraz osoby, której dane dotyczą, o powstałych naruszeniach, czy prowadzenia rejestru czynności przetwarzania danych. Z

jednej strony ogólne rozporządzenie o ochronie danych rozszerza obowiązki podmiotów przetwarzających dane osobowe, z drugiej zaś nie ma szczegółowych wytycznych odnośnie do ich wdrożenia.

Każdy administrator będzie musiał prowadzić rejestr czynności przetwarzania danych, który musi udostępnić na żądanie organu nadzorczego. Ponadto, jeżeli dany rodzaj przetwarzania (w szczególności z użyciem nowych technologii) może powodować ze względu na swój charakter, cel i zakres z dużym prawdopodobieństwem wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania danych powinien dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (art. 35 rodo).

Niedostosowanie się do wymogów rozporządzenia ogólnego może nieść za sobą daleko idące skutki. Do najpoważniejszych należy zaliczyć: utratę kontroli nad danymi, ograniczenie praw, dyskryminację, kradzież tożsamości, naruszenie dobrego imienia, nieuprawnione odwrócenie pseudonimizacji, naruszenie poufności danych osobowych chronionych tajemnicą zawodową. Poza tymi szkodami coraz częściej dochodzi także do szkody o charakterze majątkowym (motyw 75 preambuły rozporządzenia ogólnego).

Dodatkowo, administrator, który nie zapewni bezpieczeństwa przetwarzanych danych osobowych, musi liczyć się z narażeniem się na odpowiedzialność finansową.

Z raportu przedstawionego przez Security Trends w 2015 roku wynika, że wśród 81% ankietowanych wiedza na temat potencjalnych zagrożeń nie jest adekwatna do tempa rozwoju i upowszechniania technologii. Najczęściej popełnianymi błędami w tym obszarze są: przekazywanie niezabezpieczonych danych pomiędzy domeną prywatną a służbową, wykorzystywanie serwisów społecznościowych do prywatnej komunikacji czy podatność na socjotechniki (Raport Security Trends z 2015 roku). 81% użytkowników końcowych nie przestrzega zasad bezpieczeństwa. Z raportu wynika także, że 67% firm posiada własne zespoły odpowiedzialne za reagowanie na incydenty, a 7% korzysta z usług podmiotów zewnętrznych (Raport Security Trends z 2015 roku). 25% połączeń do polskich witryn internetowych pochodziło w 2015 roku z tabletów i smartfonów (Raport Security Trends z 2015 roku).

Autor:
Agnieszka Stępień

Stopka redakcyjna

Redaktor:	Wioleta Szczygielska
ISBN:	978-83-269-6984-3
E-book nr:	2HH0658
Wydawnictwo:	Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł