Cywilizacja i Polityka
2022, nr 20, s. 213–230
https://doi.org/10.15804/cip202212
ISSN 1732-5641

Mateusz Żoch
Uniwersytet Mikołaja Kopernika

Normy prawne ochrony informacji

Legal standards for information protection

Słowa kluczowe: normy prawne, ochrona informacji
Keywords: legal standards, information protection

Streszczenie

Informacja jest ważnym elementem życia człowieka i towarzyszy mu w jego codziennym życiu. Od dawnych czasów przyczyniała się do rozwoju cywilizacji. Wraz z rozwojem technologii jej udział w życiu człowieka tylko się zwiększył. Dzięki współczesnym technologiom każdy człowiek ma prawie nieograniczony dostęp do informacji. Na przykład dzięki Internetowi informacja w mgnieniu oka może zostać przesłana z jednego miejsca na świecie do drugiego. Tak łatwy dostęp do informacji ułatwia podejmowanie decyzji biznesowych oraz życiowych. Jednak nie każda informacja wytworzona na przykład przez firmę lub instytucje państwową powinna być łatwo dostępna dla każdego. Spowodowało to konieczność stosowania środków ochrony informacji, które zapewnią jej bezpieczeństwo. Konieczność ochrony informacji doprowadziła do powstania norm prawnych, które regulują jej ochronę.

Abstract

Information is an important element of human life and accompanies him in his everyday life. It has contributed to the development of civilization since ancient times. With the development of technology, its share in human life has only increased. Thanks to modern technologies, everyone has almost unlimited access to information. For example, thanks to the Internet, information can be sent from one place in the world to another in the blink of an eye. Such easy access to information makes it

easier to make business and life decisions. However, not every piece of information produced, for example, by a company or state institution, should be easily accessible to everyone. This resulted in the need to use information protection measures that will ensure its security. The need to protect information has led to the creation of legal standards that regulate its protection.

Informacja posiada wiele definicji i może być rozpatrywana na wielu płaszczyznach. Zdefiniowana może być jako każda otrzymana wiadomość bez względu na to kto ją przekazał ani do kogo. Nieważna jest również jej treść, forma czy znaczenie[1]. Może być również przedstawiona jako zachodzący między co najmniej dwoma podmiotami stosunek złożony ze znaczenia i nośnika, który służy do przekazania sygnału od jednego podmiotu do drugiego. W znaczeniu podmiotowym informacja jest zbiorem czynności służących do tworzenia, przetwarzania, przechowywania, pozyskiwania oraz odbierania i udostępniania treści, które dotyczą określonego obiektu[2].

Informacja zawsze dotyczy czegoś konkretnego, istniejącego w rzeczywistości. Jest ona również zasobem, który nigdy się nie wyczerpie, ponieważ nawet pozyskanie jej przez wielu odbiorców nie wpływa na jej występowanie. Informacja powinna również jak najdokładniej odzwierciedlać rzeczywistość, ponieważ im dokładniejsza jest informacja, tym bardziej wzrasta jej wartość.

Encyklopedyczna definicja informacji brzmi: „Informacja – obiekt abstrakcyjny, który może być w postaci zakodowanej zapisywany (na nośnikach informacji), przesyłany, przetwarzany za pomocą programów komputerowych i używany do sterowania urządzeniami”[3]. Jest to definicja bardzo uproszczona i nieoddająca złożoności pojęcia. Skupia się głównie na informacji ściśle związanej z systemami informatycznymi.

W naukach z zakresu bezpieczeństwa stworzona i przyjęta została definicja brzmiąca: „Informacja – wiedza uzyskiwana w drodze interpretacji danych, która w ustalonym kontekście ma określone znaczenie i dotyczy obiektów, takich jak fakty, zdarzenia, przedmioty, zjawiska, procesy i idee: także nieprzetworzone dane każdego rodzaju, które mogą być wykorzystane do opracowań wywiadowczych

[1] W. Roman, *Podstawy zarządzania informacją,* Toruń 2012, s. 17.

[2] J. Ratajewski, *Wstęp do informacji naukowej,* Katowice 1973, s. 8–9.

[3] *Encyklopedia PWN*, https://encyklopedia.pwn.pl/haslo/informacja;3914687.html [dostęp: 2.11.2022].

(rozpoznawczych)"[4]. Definicja zawiera część ogólną oraz część specjalistyczną, która wykorzystana może być tylko w sytuacjach związanych z bezpieczeństwem lub w dziedzinach pośrednich. Jest to jednak definicja zawierająca podstawowy błąd, który eliminuje ją z poważnych rozważań naukowych: informacja to nie jest to samo co wiedza.

Prowadząc rozważania nad informacją należy znać różnice między danymi, informacją i wiedzą. Dane przedstawiają fakty, które nie mają znaczenia i celu oraz przenoszone są jako komunikat. Informacja jest zbiorem danych zawartych w komunikacie, aby zbiór danych stał się informacją potrzebny jest odbiorca, który je zinterpretuje, a dane będą miały dla niego znaczenie i wniosą coś nowego do jego świadomości. Wiedza z kolei tworzona jest z informacji, które odbiorca sprawdził i zweryfikował[5].

Informację określić można jako dobro ekonomiczne, ponieważ we współczesnym świecie traktowana jest jako towar poprzez przenoszenie praw własności lub uprawnień do czasowego korzystania z jednego podmiotu na inny. Może być jednak również dobrem publicznym w zakresie dostępnym każdemu użytkownikowi i w nieograniczony sposób. Jako przykład można przytoczyć informację w administracji publicznej, która dotyczyć może obowiązującego systemu podatkowego, stosowania ulg oraz sposobów prowadzenia księgowości. Informacja jest również dobrem niewyczerpalnym, ponieważ nie zużywa się w trakcie jej wykorzystywania[6].

Zagrożenia i środki ochrony informacji

Ze względu na mnogość występujących rodzajów informacji występuje również wiele jej zagrożeń, które mogą wpłynąć na jej kształt, zmienić jej znaczenie, a nawet doprowadzić do jej fizycznego zniszczenia. Można je podzielić na wiele sposobów.

Jednym z najprostszych kryteriów podziału jest podział na zagrożenia wewnętrzne i zewnętrzne. Wewnętrzne to te związane z systemem i użytkownikami, a zewnętrzne to te niezależne od użytkowników i systemu. Przykładami zagrożeń

[4] B. Zdrodowski (red.), *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2008, s. 51.

[5] M. Grabowski A. Zając, *Dane, informacja, wiedza – próba definicji*, https://www.uci.agh.edu.pl/uczelnia/tad/APSI/cwiczenia/Dane_informacje_wiedza.pdf [dostęp: 2.11.2022].

[6] R. Kurek, *Informacja jako dobro publiczne a nadzór nad działalnością zakładów ubezpieczeń*, https://piu.org.pl/public/upload/ibrowser/WU/WU4_2010/kurek.pdf [dostęp: 3.11.2022].

zewnętrznych są zdarzenia naturalne takie, jak na przykład powódź czy pożar, czyli takie którym trudno zapobiec i ciężko je przewidzieć. Przykładem takiego zagrożenia może być również awaria lub uszkodzenie nośnika informacji powstałe niezależnie od użytkownika[7].

Kolejną kategorią podziału zagrożeń dla informacji są zagrożenia spowodowane przez użytkownika informacji w sposób umyślny lub też nieumyślny. Zagrożeniom nieumyślnym ciężko jest zapobiegać. Są one często spowodowane błędami lub zaniedbaniami popełnianymi przez użytkowników informacji, aby im zapobiegać należy ich szkolić i dbać o to, żeby dostęp do wrażliwych informacji miały tylko osoby odpowiednio przeszkolone. Zagrożenia umyślne mogą pochodzić zarówno z wewnątrz, jak i z zewnątrz, aby uchronić się przed nimi należy również ograniczyć dostęp do wrażliwych informacji oraz zadbać o zabezpieczenia fizyczne lub specjalne oprogramowanie[8].

Istotnym zagrożeniem dla informacji jest sama jej ilość. Zarówno zbyt mała, jak i zbyt duża ilość informacji uniemożliwi nam podjęcie prawidłowej decyzji. Gdy informacji jest zbyt mało niemożliwe jest po prostu rozważenie wszystkich możliwości czy konsekwencji, które może przynieść nasza decyzja. Z kolei zbyt duża ilość informacji sprawi, że powstanie szum informacyjny, z którego ciężko nam będzie wybrać przydatne informacje[9]. Obie sytuacje mogą być wywołane w sposób umyślny, ponieważ nasz dostęp do informacji może być ograniczany na różne sposoby jak na przykład uniemożliwienie nam dostępu do pewnych źródeł informacji, ale możemy również zostać „zasypani" dużą ilością nic nieznaczących informacji, których celem jest stworzenie natłoku informacji, w którym znikną przydatne dla nas informacje.

W dzisiejszych czasach coraz częściej można natknąć się na instytucje, firmy, organizacje lub osoby, których głównym zajęciem jest manipulowanie przekazem informacji. Mogą to być na przykład ośrodki medialne powiązane z ugrupowaniami politycznymi, które wykorzystują techniki manipulacyjne oraz dezinformację, aby w ten sposób osiągać korzyści polityczne lub materialne[10].

Powszechne występowanie i wykorzystywanie informacji sprawia, że jej zagrożenia mogą dotknąć nie tylko firmy czy instytucje państwowe, ale również

[7] D. Fleszer, *Wokół problematyki bezpieczeństwa informacji*, „Roczniki Administracji i Prawa" 2018, nr XVII (1), s. 192–193.

[8] J. Madej, *Polityka bezpieczeństwa i system ochrony informacji w przedsiębiorstwie,* „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie" 2002, nr 604, s. 140.

[9] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2005, s. 86.

[10] Ibidem, s. 116.

każdego człowieka bezpośrednio. Dlatego właśnie niezbędne jest systemowe unormowanie ochrony informacji oraz zapewnienie bezpiecznego dostępu do informacji. Do osiągnięcia całkowitego bezpieczeństwa informacji należy wykorzystywać wszelkie dostępne środki. Powinny być one oparte na następujących zasadach ochrony informacji:

- racjonalności – zgodnie z nią wszelkie podejmowane działania ochronne powinny być uzależnione od możliwości wystąpienia zagrożenia, ponieważ nie każda informacja narażona jest na takie same zagrożenia;
- adekwatności – podejmowane środki ochrony powinny być stosowane proporcjonalnie do zagrożenia;
- nieprzewidywalności – potencjalny napastnik nie powinien być w stanie przewidzieć reakcji na jego atak;
- stałej gotowości – zagrożenia mogą wystąpić w każdej chwili, dlatego powinniśmy być w każdej chwili gotowi do reakcji;
- najsłabszego ogniwa – system bezpieczeństwa jest tak silny, jak jego najsłabsze ogniwo[11].

Zastosowane środki ochrony informacji muszą być dopasowane do sposobu w jaki jest ona utrwalona na nośniku oraz formy fizycznej nośnika. Powinny one prowadzić do zachowania poufności, spójności oraz dostępności informacji. Każdy tworzący system bezpieczeństwa informacji powinien samodzielnie ocenić, która z tych cech jest dla niego najważniejsza. Banki skupiają się na zachowaniu poufności, ponieważ wyciek informacji może zniszczyć ich reputację, instytucje naukowe skupiają się na spójności, ponieważ nie mogą sobie pozwolić na jakiekolwiek błędy w swojej działalności, a firmy usługowe koncentrują się na dostępności informacji, aby nie ponieść strat materialnych z powodu braku dostępu do informacji[12].

Środki ochrony informacji możemy podzielić na:

- prawne – akty prawa zarówno krajowego, jak i również akty prawa międzynarodowego;
- organizacyjno-administracyjne – opracowanie i wprowadzenie przepisów wewnętrznych odnośnie nadzoru, kontroli i procedur awaryjnych związanych z obiegiem dokumentacji, przemieszczaniem się ludzi oraz kontroli przeciwpożarowej;

[11] W. Roman, *Podstawy zarządzania*..., s. 204.

[12] J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001,* Poznań 2009, s. 12.

- programowo-sprzętowe – dotyczą bezpośrednio systemów teleinformatycznych, zapewniają nieprzerwany i bezpieczny przepływ informacji między poszczególnymi elementami tych systemów;
- fizyczne – najprostsza kategoria środków ochrony polegająca na fizycznym zabezpieczeniu informacji, np. szafy, sejfy[13].

Środki ochrony powinny zostać dobrane w sposób dopasowany do potencjalnych zagrożeń oraz ich faktycznej oceny, ponieważ zastosowanie nieodpowiednich środków ochrony lub ich zbyt dużej ilości może doprowadzić do niewydolności systemu.

Ochrona informacji w przepisach Unii Europejskiej

Unia Europejska jako wspólnota państw posiada własną osobowość prawną, a w związku z tym również swój własny system prawny, który różni się od międzynarodowego systemu prawnego. Swoją działalnością UE wpływa na prawa jej państw członkowskich w sposób pośredni oraz bezpośredni. Jej prawa stają się prawami jej członków. Unijne akty prawne możemy podzielić na:

- rozporządzenia – z powodu ogólnego i bezpośredniego zastosowania są w całości respektowane przez podmioty, których dotyczą i powinny być stosowane we wszystkich państwach członkowskich;
- dyrektywy – skierowane są do poszczególnych państw członkowskich, które muszą osiągnąć określony cel poprzez wydanie krajowego aktu wykonawczego, który dostosuje prawo krajowe do określonych celów;
- decyzje – służą regulowaniu konkretnych sytuacji w państwach członkowskich, mogą być skierowane do państwa, ale również do osoby fizycznej lub prawnej;
- zalecenia i opinie – nie przyznają żadnych praw, są wskazówkami dotyczącymi prawa UE[14].

Prawne środki ochrony informacji UE można znaleźć w różnych aktach prawnych. Najważniejszym z nich jest Karta Praw Podstawowych Unii Europejskiej. Zawarty w niej art. 8 gwarantuje każdemu prawo do ochrony jego danych osobowych. Zgodnie z tym artykułem powinny one być one przetwarzane w sposób

[13] J. Madej, *Polityka bezpieczeństwa*..., s. 144.

[14] Oficjalna strona internetowa Parlamentu Europejskiego, https://www.europarl.europa.eu/factsheets/pl/sheet/6/sources-and-scope-of-european-union-law [dostęp: 3.11.2022].

rzetelny i tylko w celach określonych za zgodą osoby zainteresowanej. Artykuł ten zapewnia również dostęp do danych każdego, którego dane dotyczą[15].

Kolejny akt prawny zawierający środki ochrony informacji to rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. Powszechnie nazywane jest RODO, jest to skrót od Rozporządzenie o Ochronie Danych Osobowych. Dotyczy ono ochrony osób fizycznych w związku z przetwarzaniem i swobodnym przepływem danych osobowych. Rozporządzenie zapewnia ochronę obywateli UE przed naruszeniami prywatności. Została w nim wprowadzona możliwość zwrócenia się do administratora danych o ich wykasowanie. Przepisy zawarte w rozporządzeniu dotyczą wszystkich przedsiębiorstw działających na terenie Unii nawet jeśli ich siedziba znajduje się poza jej granicami. W przypadku wystąpienia naruszeń przepisów mogą zostać zastosowane ostrzeżenia lub kary finansowe[16].

Innym aktem prawnym UE dotyczącym ochrony informacji jest dyrektywa Parlamentu Europejskiego i Rady UE 2016/680 z dnia 27 kwietnia 2016 r. Dotyczy ona ochrony informacji przetwarzanych przez organy zwalczające i zapobiegające przestępczości. Ma na celu ochronę wykorzystywanych przez nie informacji oraz ułatwienie współpracy między nimi[17].

Środki ochrony informacji niejawnych zawarte są w oddzielnych dokumentach od tych dotyczących ochrony danych osobowych. Jednym z takich dokumentów jest Decyzja Rady z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE[18]. Określa ona podstawowe zasady oraz minimalne normy bezpieczeństwa, które służyć mają ochronie informacji. Zawarte w niej normy i zasady obowiązują Radę Unii Europejskiej oraz jej Sekretariat Generalny, ale również państwa członkowskie Unii Europejskiej, gdy wykorzystują one informacje niejawne UE. Decyzja wprowadza podział informacji niejawnych na cztery kategorie. Najniższą kategorią jest EU Restricted. Nieuprawnione ujawnienie informacji oznaczonych tą kategorią miałoby niekorzystny wpływ na interesy państw członkowskich, nawet całej UE. Kolejną

[15] Karta Praw Podstawowych Unii Europejskiej, 2012/C 326/02, art. 8, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:12012P/TXT&from=PL [dostęp: 3.11.2022].

[16] Rozporządzenie Parlamentu Europejskiego i Rady UE, 2016/679, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679&from=PL [dostęp: 3.11.2022].

[17] Dyrektywa Parlamentu Europejskiego i Rady UE, 2016/680, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L0680&from=PL [dostęp: 3.11.2022].

[18] Decyzja Rady z dnia 23 września 2013 r., 2013/488/UE, s. 2, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32013D0488&from=HR [dostęp: 3.11.2022].

kategorią jest EU Confidential, gdyby informacje objęte tą kategorią zostały ujawnione w sposób nieuprawniony to mogłyby wyrządzić szkodę dla podstawowych interesów UE lub państw członkowskich. Następną kategorią jest EU Secret. Objęte są nią informacje, których ujawnienie poważnie zaszkodziłoby interesom państw członkowskich lub UE. Ostatnią kategorią i zarazem oznaczającą najważniejsze spośród informacji niejawnych jest EU Top Secret. Kategoria ta obejmuje informacje, które w przypadku ujawnienia wyrządziłyby poważną szkodę interesom UE lub państw członkowskich.

Ochrona informacji w przepisach państwowych

W polskim systemie prawnym zgodnie z Konstytucją Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r.[19] występują następujące źródła prawa:

- Konstytucja – akt normatywny, czyli taki, w którym zawarte zostały normy prawne, najważniejszy akt prawny w Polsce;
- ustawy – akty normatywne, wydawane przez Sejm i Senat, ogłaszane w Dzienniku Ustaw, mogą obejmować prawa i obowiązki obywateli, przepisy podatkowe, przepisy prawa karnego i zagadnienia gospodarki finansowej państwa;
- ratyfikowane umowy międzynarodowe – umowy międzynarodowe przyjęte przez Prezydenta RP za zgodą Sejmu, są źródłami powszechnie obowiązującego prawa;
- rozporządzenia – akty wykonawcze ustaw, mogą być podstawą egzekwowania praw i obowiązków jednostek.

Najważniejszym aktem prawa, w którym zawarta jest ochrona informacji jest Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych[20]. Uchwalona została w celu dostosowania polskich przepisów do unijnego rozporządzenia o ochronie danych osobowych z kwietnia 2016 r. Jej głównym zadaniem jest utworzenie jednolitego systemu ochrony danych osobowych z tym występującym w innych państwach UE.

Ustawa wprowadza nowy organ odpowiedzialny za nadzorowanie ochrony danych osobowych, jest nim Prezes Urzędu Ochrony Danych Osobowych i zastępuje on Generalnego Inspektora Ochrony Danych. Prezes Urzędu Ochrony Danych Osobowych powoływany i odwoływany jest przez Sejm RP za zgodą Senatu RP.

[19] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. Nr 78, poz. 483 ze zm.
[20] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2018, poz. 1000 ze zm.

Kandydować na to stanowisko może osoba posiadająca obywatelstwo polskie, wyższe wykształcenie, nieposzlakowaną opinię, ale również posiada wiedzę prawniczą i doświadczenie w zakresie ochrony danych osobowych, nie była nigdy prawomocnie skazana za umyślne przestępstwo lub umyślne przestępstwo skarbowe oraz korzysta z pełni praw publicznych. Prezes UODO powoływany jest na czteroletnią kadencję i może powołać do trzech zastępców, a jako jego organ opiniodawczo-doradczy działa Rada do Spraw Ochrony Danych Osobowych. Prezes posiada uprawnienia do skierowania do organów państwowych, samorządu terytorialnego, podmiotów niepublicznych prowadzących zadania publicznych oraz osób fizycznych i prawnych wystąpienia, które zapewni skuteczną ochronę danych osobowych. Kolejnym uprawnieniem Prezesa jest występowanie z wnioskami do odpowiednich organów o podjęcie inicjatywy ustawodawczej, zmianę lub wydanie aktów prawnych z zakresu ochrony danych osobowych. Ustawa zobowiązuje Prezesa do publikacji w Biuletynie Informacji Publicznej zatwierdzonych kodeksów postępowania oraz ich zmian, klauzul umownych dotyczących podmiotów przetwarzających dane osobowe, rekomendacji, w których określone są środki organizacyjne oraz techniczne stosowane jako zapewnienie bezpieczeństwa przetwarzania danych osobowych[21].

Nowością w systemie ochrony danych osobowych wprowadzoną w ustawie są kodeksy postępowań. Są to tak zwane kodeksy dobrych praktyk. Mają one pomóc we właściwym stosowaniu przepisów zawartych w unijnym rozporządzeniu o Ochronie Danych Osobowych. Kodeksy tworzone przez zrzeszenia lub inne podmioty reprezentujące administratorów lub podmioty przetwarzające dane osobowe powinny uwzględniać specyfikę różnych sektorów, w których przetwarzane są informacje oraz specyfikę średnich i małych przedsiębiorstw. Kodeksy muszą przed przekazaniem ich do zatwierdzenia przez Prezesa UODO przejść konsultacje, następnie informacja o konsultacjach i ich wyniku przekazywane są do Prezesa celem ich zatwierdzenia. Ustawa umożliwia udzielenie akredytacji podmiotom posiadającym odpowiedni poziom wiedzy w dziedzinie kodeksu. Akredytacja pozwala podmiotowi monitorowanie przestrzegania kodeksu. Wykaz podmiotów akredytowanych powinien być udostępniony w Biuletynie Informacji Publicznej Urzędu Ochrony Danych Osobowych[22].

Kolejną nowością wprowadzoną przez ustawę jest certyfikacja. Dokonywana jest ona przez Prezesa UODO lub podmiot certyfikujący, który posiada akredyta-

[21] Ibidem, s. 5–26.
[22] Ibidem, s. 13–15.

cję Polskiego Centrum Akredytacji, na wniosek podmiotu przetwarzającego lub administratora. Wniosek o certyfikację rozpatrzony powinien zostać w ciągu trzech miesięcy od daty złożenia. Kryteria certyfikacji, wysokość opłat z nią związanych oraz publiczny wykaz podmiotów posiadających certyfikację, ale również takich, którym certyfikacja została cofnięta powinien być dostępny na stronie BIP Urzędu Ochrony Danych Osobowych. Ustawa przyznaje również Prezesowi UODO możliwość przeprowadzenia kontroli zarówno w podmiocie starającym się o certyfikację, jak i w podmiocie, który certyfikację już otrzymał, w celu sprawdzenia czy podmiot spełnia kryteria certyfikacji[23].

Ustawa o ochronie danych osobowych wprowadza również obowiązek powołania przez jednostki sektora finansów publicznych, Narodowy Bank Polski oraz instytuty badawcze Inspektora Ochrony Danych Osobowych. Informacja zawierająca imię i nazwisko oraz numer telefonu lub adres e-mail powinna zostać zamieszczona na stronie internetowej wymienionych podmiotów lub w przypadku, gdy podmiot nie posiada strony internetowej powinna zostać zamieszczona w ogólnie dostępnym miejscu w miejscu prowadzenia działalności. Po wyznaczeniu Inspektora podmiot zobowiązany jest do powiadomienia o tym w ciągu czternastu dni Prezesa UODO[24].

Ustawa udzieliła każdemu podmiotowi danych prawo do skutecznego środka ochrony przed sądem w przypadku stwierdzenia naruszenia przysługujących mu praw dotyczących ochrony danych osobowych. Ustawa doprecyzowuje, że do takich roszczeń stosowane są przepisy Kodeksu cywilnego, a organem rozpatrującym takie roszczenia jest Sąd Okręgowy[25].

Ochrona informacji to jednak nie tylko ochrona danych osobowych, ale również ochrona informacji niejawnych. Najważniejszym aktem w polskim systemie prawnym dotyczącym ochrony informacji niejawnych jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[26]. Jest ona podstawowym aktem prawnym regulującym ochronę informacji niejawnych w Polsce.

W ustawie dokonano klasyfikacji informacji niejawnych według zagrożeń, które mogłyby wystąpić w sytuacji ujawnienia takiej informacji. Najniższym poziomem w tej klasyfikacji informacji niejawnych jest informacja zastrzeżona, czyli taka, której ujawnienie źle wpłynęłoby na wykonywane przez organy władzy

[23] Ibidem, s. 9–13.

[24] Ibidem, s. 6–8.

[25] Ibidem, s. 37–39.

[26] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. 2010, nr 182, poz. 1228 ze zm.

publicznej zadania. Kolejną klauzulą tajności informacji zawartą w ustawie jest informacja poufna. Informacja taka w przypadku ujawnienia niosłaby za sobą szkody dla Rzeczpospolitej Polskiej poprzez utrudnienia prowadzenia polityki zagranicznej, czy zagrożenie stabilności systemu finansowego, co wpłynęłoby niekorzystnie na gospodarkę państwa. Następną kategorią informacji niejawnych jest informacja tajna. W przypadku jej ujawnienia wystąpiłyby poważne szkody na przykład zakłócenie działalności Sił Zbrojnych czy pogorszenie stosunków z innymi państwami. Ostatnią i najwyższą klauzulą tajności informacji zdefiniowaną w tej ustawie jest informacja ściśle tajna. Ujawnienie takiej informacji niosłoby bardzo poważne szkody dla państwa, na przykład zagrożenie bezpieczeństwa wewnętrznego lub nawet niepodległości[27].

Kolejnym aspektem ochrony informacji niejawnych zawartym w ustawie jest organizacja tej ochrony. Ustawa powierza ochronę informacji Agencji Bezpieczeństwa Wewnętrznego oraz Służbie Kontrwywiadu Wojskowego. Precyzuje również zadania, które dotyczą ochrony informacji niejawnych. Do zadań tych należy doradzanie oraz przeprowadzanie szkoleń z zakresu ochrony informacji niejawnych, przeprowadzanie postępowań mających na celu sprawdzenie, kontrolę lub bezpieczeństwo przemysłowe, zapewnienie bezpieczeństwa informacjom niejawnym wymienianym między RP a innymi państwami lub z organizacjami międzynarodowymi oraz kontrola przestrzegania przepisów ochrony informacji niejawnych[28].

Ustawa o ochronie informacji niejawnych reguluje również zasady dostępu do informacji niejawnych. Do informacji zakwalifikowanych jako poufne dostęp otrzymać można po uzyskaniu poświadczenia bezpieczeństwa oraz odbyciu szkolenia z zakresu ochrony informacji. Informacje zastrzeżone dostępne są dla osób, które odbyły szkolenie dotyczące ochrony informacji oraz w przypadku, gdy osoba, która nie posiada poświadczenia bezpieczeństwa otrzymała pisemne upoważnienie od kierownika jednostki organizacyjnej. Dostęp do informacji tajnych i ściśle tajnych wymaga posiadania odpowiedniego poświadczenia bezpieczeństwa, które wydawane jest po przeprowadzeniu postępowania sprawdzającego pozwalającego sprawdzić, czy osoba poddawana postępowaniu daje rękojmię zachowania tajemnicy[29].

Kolejnym aktem prawnym normującym ochronę informacji w polskim systemie prawnym jest umowa między stronami Traktatu Północnoatlantyckiego

[27] Ibidem, s. 5–9.
[28] Ibidem, s. 9–17.
[29] Ibidem, s. 19–34.

o ochronie informacji[30]. Jest to ratyfikowana umowa międzynarodowa zawarta w celu unormowania warunków ochrony informacji niejawnych przekazywanych pomiędzy państwami członkowskimi Traktatu Północnoatlantyckiego. Zgodnie z tą umową państwa członkowskie zapewnią ochronę informacjom niejawnym wytworzonym przez NATO lub przekazanym NATO przez państwo członkowskie oraz informacje określone jako niejawne, a przekazywane pomiędzy państwami z powodu kontraktu, projektu lub programu NATO. Zawarte w umowie zapisy gwarantują utrzymanie odpowiedniej klauzuli tajności przekazywanych informacji, ale również gwarantują, że przekazane informacje wykorzystane zostaną tylko w celach określonych przez Traktat Północnoatlantycki oraz, że informacje nie zostaną przekazane do podmiotu spoza Traktatu, jeśli zgody na to nie wyrazi podmiot, który zastrzegł informację[31].

Umowa zawiera również zobowiązanie wobec państw członkowskich Traktatu dotyczące zapewnienia, że dostęp do przekazywanych informacji niejawnych otrzymają tylko osoby, które zostały odpowiednio sprawdzone. Sprawdzenie ma na celu zweryfikowanie czy osoba dopuszczona nie stworzy zagrożenia dla bezpieczeństwa informacji. Strony Traktatu Północnoatlantyckiego zgodnie z umową mają ze sobą współpracować, aby stosowane były procedury sprawdzania satysfakcjonujące każdą ze Stron[32].

Innym krajowym aktem prawnym dotyczącym ochrony informacji obowiązującym w Polsce jest ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[33]. Reguluje ona zasady i warunki przetwarzania danych osobowych przez odpowiednie organy do „rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych"[34]. Oznacza to, że zobowiązane do przestrzegania przepisów zawartych w tej ustawie zobowiązane są tylko organy zajmujące się zapobieganiem i zwalczaniem przestępczości, takie jak Policja, Straż Graniczna oraz Sądy i Prokuratura, ale również Państwowa Straż Rybacka i komornik egzekwujący kary, które zasądzono w postępowaniu karnym. W ustawie zawarte są sposoby zabezpieczania danych osobowych, tryby współpracy z organami innych państw Unii

[30] Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji z dnia 6 marca 1997 r., Dz.U. 2000, nr 64, poz. 740 ze zm.

[31] Ibidem, s. 3951–3952.

[32] Ibidem, s. 3952–3953.

[33] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, Dz.U. 2019, poz. 125 ze zm.

[34] Ibidem, s. 1.

Europejskiej oraz prawa osób, których dane przetwarzane są przez organy, które ustawa obowiązuje.

Ochrona informacji w przepisach wewnętrznych

Prawne środki ochrony informacji to nie tylko przepisy krajowe czy międzynarodowe, ale również przepisy wewnętrzne tworzone w różnych instytucjach czy przedsiębiorstwach.

Przykładem dokumentu dotyczącego ochrony informacji w przedsiębiorstwie lub instytucji jest Polityka Bezpieczeństwa Informacji. Jest to dokument zdefiniowany w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[35] jako „zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z planem ich wdrożenia i egzekwowania"[36]. Oznacza to, że Polityka Bezpieczeństwa Informacji to zbiór dokumentów, który określa zasady i metody ochrony informacji. Dokumenty muszą być spójne, aby tworzyć jedną całość, na której oparty jest cały system ochrony informacji w instytucji lub przedsiębiorstwie. Polityka Bezpieczeństwa Informacji nie posiada unormowanej struktury. W normie krajowej ISO dotyczącej technik informatycznych, technik bezpieczeństwa oraz praktycznych zasad zarządzania bezpieczeństwem informacji[37] zawarto jedynie jakie minimum ma znajdować się w PBI. Musi w niej zostać zdefiniowane bezpieczeństwo informacji oraz sprecyzowane mają być jego cele i znaczenie, zdefiniować należy również obowiązki z zakresu bezpieczeństwa informacji, w tym te dotyczące zgłaszania przypadków naruszenia bezpieczeństwa informacji. PBI powinna również zawierać oświadczenie, w którym zawarte są intencje kierownictwa instytucji oraz wyjaśnienie czym jest sama Polityka i wskazanie, które zasady i wymagania mają szczególne znaczenie dla instytucji. Norma ISO wskazuje również, że Politykę Bezpieczeństwa Informacji należy udostępnić użytkownikom w taki sposób, aby była łatwo

[35] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2012, poz. 526.

[36] Ibidem, s. 2.

[37] Polski Komitet Normalizacyjny, PN-ISO/IEC 17799:2007, Katalog Polskich Norm [dostęp: 3.11.2022].

dostępna w całej instytucji lub przedsiębiorstwie we właściwej i zrozumiałej dla czytelnika formie[38].

Opracowując Politykę Bezpieczeństwa Informacji należy zwrócić uwagę na obowiązujące przepisy, ponieważ musi ona być zgodna z prawem. Należy również wziąć pod uwagę takie czynniki, jak charakter i struktura instytucji, zachodzące w niej procesy oraz specyfikę jej funkcjonowania. Dokument ten powinien obejmować każdego pracownika instytucji oraz powinien być ciągle aktualizowany. Wszystko to sprawia, że Polityka Bezpieczeństwa Informacji powinna być tworzona indywidualnie dla każdej instytucji czy przedsiębiorstwa, ponieważ nie jest możliwe stworzenie dokumentu, który spełni wymagania wszystkich instytucji czy przedsiębiorstw[39].

Kolejnym dokumentem wewnętrznym instytucji, w którym zawarte są środki ochrony informacji jest Instrukcja Zarządzania Systemami Informatycznymi. Jest to dokument, który tak jak Polityka Bezpieczeństwa powinien znajdować się w dokumentacji każdej instytucji czy przedsiębiorstwa. Od czasu wejścia w życie unijnego rozporządzenia o Ochronie Danych Osobowych taka instrukcja nie jest prawnie wymagana. Jednak pomimo to powinna być wprowadzona w każdej instytucji czy przedsiębiorstwie przetwarzającym dane osobowe. Instrukcja powinna być znana każdemu pracownikowi, który pracuje z systemem informatycznym. Struktura Instrukcji określona została w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 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[40]. Rozporządzenie to nie jest już obowiązującym aktem prawnym, ponieważ zostało uchylone, jednak dalej jest źródłem informacji dotyczących Instrukcji. Zgodnie z tym rozporządzeniem Instrukcja Zarządzania Systemami Informatycznymi powinna zawierać procedury, podczas których nadawane są uprawnienia do przetwarzania danych, procedury tworzenia kopi zapasowych, sposób, okres i miejsce przechowywania nośników informacji,

[38] M. Kowalewski, A. Ołtarzewska, *Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności – Państwowego Instytutu Badawczego,* „Telekomunikacja i Techniki Informacyjne" 2007, nr 3–4, s. 4–5.

[39] Ibidem, s. 7–8.

[40] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 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. 2004, nr 100, poz. 1024.

kopii zapasowych systemu lub danych. Instrukcja powinna także zawierać informacje jakie środki i metody wykorzystywane są do zabezpieczenia systemu, sposób w jaki system odnotowuje operacje, które użytkownik przeprowadza na danych oraz procedury określające rozpoczęcie i zakończenie pracy użytkowników w systemie[41].

Środki prawne ochrony informacji w instytucji lub przedsiębiorstwie mogą być określone również w Regulaminie Organizacyjnym danej instytucji. Jest to dokument, w którym opisana jest struktura instytucji. Dokument ten obowiązkowy jest tylko w niektórych instytucjach, na przykład w jednostkach budżetowych sektora publicznego oraz jednostkach samorządu terytorialnego[42]. W Regulaminie zawarte są zadania i obowiązki na poszczególnych stanowiskach w danej instytucji. Na przykład w Regulaminie Organizacyjnym Urzędu Gminy w Kruklankach[43] opisana jest struktura Pionu Ochrony Informacji Niejawnych. Pion ten tworzą trzy stanowiska pracy: Pełnomocnik do spraw Ochrony Informacji Niejawnych, Administrator systemu teleinformatycznego oraz Inspektor ds. ewidencjonowania materiałów niejawnych. Osoby na tych stanowiskach odpowiedzialne są za zapewnienie ochrony informacji niejawnych, systemów teleinformatycznych oraz nadzór nad obiegiem informacji niejawnych w urzędzie[44].

Oprócz Pionu Ochrony Informacji Niejawnych w urzędzie istnieje również stanowisko Inspektora Ochrony Danych. Do jego zadań należy opracowywanie i aktualizowanie dokumentów opisujących przetwarzanie danych osobowych oraz bezpieczeństwo informacji. Prowadzi on również rejestry zbiorów danych przetwarzanych w urzędzie, na bieżąco monitoruje przestrzeganie przepisów dotyczących ochrony informacji w jednostce, prowadzi szkolenia wewnętrzne w zakresie ochrony danych osobowych oraz rozpatruje skargi osób fizycznych dotyczące naruszeń praw z zakresu przetwarzania danych osobowych[45].

Z kolei w Miejskim Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. w Lubinie wdrożono System Zarządzania Bezpieczeństwa Informacji stanowiący część całościowego systemu zarządzania „opartą na podejściu wynikającym z ryzyka biznesowego, odnoszącą się do ustanawiania, wdrażania, eksploatacji,

[41] Ibidem, s. 7021.

[42] *Regulamin organizacyjny*, [w:] *Encyklopedia Zarządzania*, https://mfiles.pl/pl/index.php/Regulamin_organizacyjny [dostęp: 3.11.2022].

[43] Regulamin Organizacyjny Urzędu Gminy w Kruklankach, https://bipkruklanki.warmia.mazury.pl/5005/regulamin-organizacyjny.html [dostęp: 3.11.2022].

[44] Ibidem, s. 17–18.

[45] Ibidem, s. 18–19.

monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji"[46]. Podejście do bezpieczeństwa informacji oparto na trzech podstawowych zasadach, z których pierwsza to reguła poufności informacji oznaczająca pewność, że informacja jest udostępniana jedynie osobom upoważnionym, druga to reguła integralności informacji oznaczająca zapewnienie jej dokładności i kompletności oraz właściwych metod jej przetwarzania, a trzecia to reguła dostępności informacji polegająca na dostępie do informacji przez osoby upoważnione, gdy istnieje taka potrzeba[47].

Zakończenie

Jak widać system prawny ochrony informacji jest rozbudowany i obejmuje praktycznie wszystkie najważniejsze aspekty jej występowania. Nie świadczy to jednak o pełnym bezpieczeństwie informacji. Same normy prawne nie zapewnią informacji wystarczającej ochrony. Konieczne jest również ich respektowanie oraz wprowadzanie innych koniecznych środków ochrony informacji, bez których informacja nie będzie w pełni bezpieczna.

Normy prawne powinny być także stale aktualizowane i dopasowywane do stale zmieniającego się środowiska informacyjnego, ponieważ technologie wciąż się rozwijają, co powoduje, że cały czas pojawiają się nowe zagrożenia oraz sposoby szkodzenia informacji.

Bibliografia

Akty prawne

Decyzja Rady z dnia 23 września 2013 r., 2013/488/UE, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32013D0488&from=HR.

Dyrektywa Parlamentu Europejskiego i Rady UE, 2016/680, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L0680&from=PL.

Karta Praw Podstawowych Unii Europejskiej, 2012/C 326/02, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:12012P/TXT&from=PL.

Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. Nr 78, poz. 483 ze zm.

[46] Polityka bezpieczeństwa informacji, https://mpwik.lubin.pl/pdf/Polityka-bezpieczenstwa-informacji.pdf [dostęp: 3.11.2022].

[47] Ibidem.

Polski Komitet Normalizacyjny, PN-ISO/IEC 17799:2007, Katalog Polskich Norm.

Regulamin Organizacyjny Urzędu Gminy w Kruklankach, https://bipkruklanki.warmia.mazury.pl/5005/regulamin-organizacyjny.html.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 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. 2004, nr 100, poz. 1024.

Rozporządzenie Parlamentu Europejskiego i Rady UE, 2016/679, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679&from=PL.

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2012, poz. 526.

Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji z dnia 6 marca 1997 r., Dz.U. 2000, nr 64, poz. 740 ze zm.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2018, poz. 1000 ze zm.

Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, Dz.U. 2019, poz. 125 ze zm.

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. 2010, nr 182, poz. 1228.

Druki zwarte i czasopisma

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń, 2005.

Fleszer D., *Wokół problematyki bezpieczeństwa informacji*, „Roczniki Administracji i Prawa" 2018, nr XVII (1).

Grabowski M., Zając A., *Dane, informacja, wiedza – próba definicji*, https://www.uci.agh.edu.pl/uczelnia/tad/APSI/cwiczenia/Dane_informacje_wiedza.pdf.

Kowalewski M., Ołtarzewska A., *Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności – Państwowego Instytutu Badawczego*, „Telekomunikacja i Techniki Informacyjne" 2007, nr 3–4.

Kurek R., *Informacja jako dobro publiczne a nadzór nad działalnością zakładów ubezpieczeń*, https://piu.org.pl/public/upload/ibrowser/WU/WU4_2010/kurek.pdf.

Łuczak J., Tyburski M., *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Poznań 2009.

Madej J., *Polityka bezpieczeństwa i system ochrony informacji w przedsiębiorstwie*, „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie" 2002, nr 604.

Ratajewski J., *Wstęp do informacji naukowej*, Katowice 1973.

Roman W., *Podstawy zarządzania informacją*, Toruń 2012.

Zdrodowski B. (red.), *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2008.

Netografia

www.encyklopedia.pwn.pl

www.mfiled.pl

www.europarl.europa.eu

www.mpwik.lubin.pl