AUTOR
mgr Lidia Więcaszek-Kuczyńska
lidiakuczynska@neostrada.pl

WYBRANE REGULACJE PRAWNE W OBSZARZE ZAGROŻEŃ BEZPIECZEŃSTWA INFORMACYJNEGO. CZĘŚĆ II

Wstęp

Celem niniejszego opracowania, będącego kontynuacją artykułu na temat regulacji prawnych w obszarze zagrożeń bezpieczeństwa informacyjnego (zob., ZN Obronność 3(11)/2014), jest przedstawienie wybranych przepisów prawa szczególnie istotnych w praktyce organizacji będącej przedsiębiorstwem działającym we współczesnej rzeczywistości gospodarczej.

W części pierwszej przybliżono pojęcia i definicje z zakresu problematyki zagrożeń bezpieczeństwa informacyjnego oraz nakreślano ramy prawno-karnej ochrony informacji, część druga opracowania przedstawia swoiste unormowania w obszarze bezpieczeństwa informacyjnego, które wydają się mieć zasadnicze znaczenie dla dzisiejszej organizacji.

Wybrane akty prawne w obszarze zagrożeń bezpieczeństwa informacyjnego

Za J. Koniecznym można stwierdzić, *iż prawo polskie chroni sporą liczbę tajemnic*[1]*,* ale za regulacje prawne najbardziej istotne dla menadżera w jego codziennej pracy powinno się uznać: przepisy o ochronie informacji niejawnych zawarte w *Ustawie o ochronie informacji niejawnych*, regulacje dotyczące tajemnicy przedsiębiorstwa zawarte w *Ustawie o zwalczaniu nieuczciwej konkurencji* oraz zapisy *Ustawy o ochronie danych osobowych*[2].

[1] Ze względu na rodzaj podmiotu lub dziedzinę gospodarki, do której odnosi się chroniona informacja możemy wyszczególnić: tajemnicę przedsiębiorstwa, tajemnicę handlową, bankową, publicznego obrotu papierami wartościowymi, zamówień publicznych, tajemnicę statystyczną, tajemnicę skarbową, tajemnicę czynności operacyjno-rozpoznawczych, lekarską i wiele innych, których szczegółowe omówienie wykracza poza ramy niniejszego opracowania. Zob., J. Konieczny, *Wprowadzenie do bezpieczeństwa biznesu*, Konsalnet, Warszawa, 2004, s. 171.

[2] Tamże, s. 171.

W Polsce aktualnie ponad dwieście aktów prawnych[3] odnosi się do ochrony informacji, a dla każdego obszaru działania przedsiębiorstwa[4] można rozpoznać klika lub kilkanaście przepisów prawnych obejmujących zapisy odnoszące się szczególnie do bezpieczeństwa informacji[5].

Jedną z kluczowych ustaw regulujących obszar bezpieczeństwa informacyjnego jest *Ustawa o ochronie danych osobowych*[6].

Koncepcja ochrony danych osobowych jest w polskim ustawodawstwie relatywnie nowa, gdyż w krajach Europy Zachodniej pierwsze regulacje tego obszaru zostały wprowadzone już po II wojnie światowej, ale zasadnicze znaczenie w tym zakresie ma *Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 o ochronie osób w związku z automatycznym przetwarzaniem danych o charakterze osobowym*[7].

Ustawa o ochronie danych osobowych formułuje między innymi odpowiedzialność osoby administrującej zbiorem danych oraz penalizuje, jako czyn zabroniony, niezabezpieczenie danych.

Art. 50 ust. 1 *Ustawy o ochronie danych osobowych* określa odpowiedzialność osoby administrującej zbiorem danych, która, będąc obowiązana do ochrony danych osobowych, udostępnia je lub umożliwia dostęp do nich osobom nieuprawnionym. Podlega ona karze grzywny, ograniczenia wolności lub pozbawienia wolności. Przepis stanowi, że sprawcą czynu może być zarówno kierownik jednostki, jak i administrator bezpieczeństwa informacji, a także inny pracownik danej jednostki, który jest odpowiedzialny za ochronę danych;

Art. 52 *Ustawy o ochronie danych osobowych* penalizuje jako czyn zabroniony samo niezabezpieczenie danych, bez względu na ich uszkodzenie, zniszczenie czy kradzież, niezależnie od tego, czy dane te zostały ukradzione, uszkodzone lub zniszczone[8].

[3] Por., M. Taradejna, R. Taradejna, *Dostęp do informacji publicznej, a prawna ochrona informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego*, Adam Marszałek, Toruń, 2003, s. 304-319.

[4] Jako przykład może posłużyć obowiązująca podmioty prowadzące księgi rachunkowe *Ustawa o rachunkowości*, której cały rozdział ósmy dotyczy zagadnienia ochrony danych, w tym szczegółowo reguluje tematykę przechowywania danych, ich przetwarzania i udostępniania. Zob., *Ustawa z 29.09.1994 r. o rachunkowości*, Dz. U. z 2009 r., nr 152, poz. 1223 z póz. zm.

[5] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, AON, Warszawa, 2010, s. 6.

[6] *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, Dz. U. z 1997 r., nr 133, poz. 883.

[7] A. M. Dereń, *Prawna ochrona informacji w krajowym ustawodawstwie*. *Wybrane zagadnienia*, Zeszyt 2008, OPO, Bydgoszcz, 2001, s. 13.

[8] *Ustawa z dnia 29 sierpnia 1997 r. o ochronie....* Por., A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczpospolitej*, Oficyna Wydawnicza ABRYS, Kraków, 2000, s. 122-123.

W poniżej zaprezentowanej tabeli 1 przedstawiono zestawienie aktów wykonawczych do *Ustawy o ochronie danych osobowych*, których wielość wskazuje na szeroki zakres regulacji w tym obszarze:

Tabela 1.

Akty wykonawcze do *Ustawy o ochronie danych osobowych*

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 1997 r., nr 133, poz. 883)		
Akty wykonawcze		
Adres publikacyjny	Status	Tytuł
M.P. z 2010 r., nr 53, poz. 719	Obowiązujący	Uchwała Senatu Rzeczypospolitej Polskiej z dnia 22 lipca 2010 r. w sprawie wyrażenia zgody na powołanie Generalnego Inspektora Ochrony Danych Osobowych
M.P. z 2010 r., nr 53, poz. 715	Obowiązujący	Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 25 czerwca 2010 r. w sprawie powołania Generalnego Inspektora Ochrony Danych Osobowych
M.P. z 2006 r., nr 47, poz. 494	Obowiązujący	Uchwała Senatu Rzeczypospolitej Polskiej z dnia 6 lipca 2006 r. w sprawie wyrażenia zgody na powołanie Generalnego Inspektora Ochrony Danych Osobowych
M.P. z 2006 r., nr 47, poz. 493	Obowiązujący	Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 23 czerwca 2006 r. w sprawie powołania Generalnego Inspektora Ochrony Danych Osobowych
Dz. U. z 2011 r., nr 225, poz. 1350	Obowiązujący	Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych
Dz. U. z 2011 r., nr 103, poz. 601	Obowiązujący	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 maja 2011 r. zmieniające rozporządzenie w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych
Dz. U. z 2008 r., nr 229, poz. 1536	Obowiązujący	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych

Dz. U. z 2004 r., nr 100, poz. 1024	Obowiązujący	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. z 2004 r., nr 94, poz. 923	Obowiązujący	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych

Źródło: opracowanie własne na podstawie: http://isip.sejm.gov.pl/DetailsServlet?id=WDU19971330883 [dostęp: 24.05.2014].

Dostęp do szczególnych informacji, tzw. informacji niejawnych[9], reguluje *Ustawa o ochronie informacji niejawnych*[10] opierająca *dostęp do informacji niejawnych na dwóch podstawowych zasadach:*

- *zasadzie ograniczonego dostępu do informacji stanowiących tajemnice państwową lub służbową (ang. „need to know" – wiedzieć tylko tyle, ile jest to konieczne),*
- *konieczności przeprowadzenia postępowania sprawdzającego (…) w celu ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy*[11].

Znajomość przepisów o ochronie informacji niejawnych jest niezwykle pomocna w praktyce biznesowej także przedsiębiorstw komercyjnych[12], niewymienionych w art. 1 *Ustawy o ochronie informacji niejawnych*[13], jako bezwzględnie zobligowanych do ich stosowania, gdyż ustawa ta dostarcza wielu wytycznych co do szeroko *rozumianej metodyki ochrony informacji, a nie ma lepszych wzorców niż te, które służą zabezpieczeniu tajemnicy państwowej*[14]*.*

Ustawa o ochronie informacji niejawnych (zwana dalej UOIN) zasadniczo reguluje tylko podstawowe aspekty ochrony informacji niejawnych,

[9] (…) *informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania*. Zob., *Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych,* Dz. U. z 2010 r., nr 182, poz. 1228, art. 1.1.

[10] Tamże.

[11] M. Wrzosek, *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną,* AON, Warszawa, 2010*,* s. 153.

[12] Szerzej: J. Konieczny, *Wprowadzenie...*, s. 170-187.

[13] Zob., *Ustawa z 5 sierpnia 2010 r. o ochronie*…, art. 1 ust. 2.

[14] J. Konieczny, *Wprowadzenie…*, s. 171.

gdyż wiele szczegółowych rozwiązań z tego obszaru znajduje się w aktach wykonawczych wydanych na jej podstawie.

Zasady ochrony informacji niejawnych zawarte w UOIN kodyfikują:

- klasyfikowanie informacji niejawnych;
- organizowanie ochrony informacji niejawnych;
- przetwarzanie informacji niejawnych;
- postępowanie sprawdzające prowadzone w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwane dalej odpowiednio „postępowaniem sprawdzającym" lub „kontrolnym postępowaniem sprawdzającym";
- postępowanie prowadzone w celu ustalenia czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych, zwane dalej „postępowaniem bezpieczeństwa przemysłowego";
- organizację kontroli stanu zabezpieczenia informacji niejawnych;
- ochronę informacji niejawnych w systemach teleinformatycznych;
- stosowanie środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych[15].

Wymienione poniżej poszczególne artykuły UOIN obligują właściwe organy Państwa do uściślenia zasad ochrony informacji niejawnych m.in.[16]:

- Art. 6 ust. 9: delegacja dla Prezesa Rady Ministrów do określenia w drodze rozporządzenia sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także tryb i sposób zmiany lub znoszenia nadanej klauzuli, zrealizowana Rozporządzeniem Rady Ministrów z dnia 22 grudnia 2011 r.
- Art. 11 ust. 6: delegacja dla Prezesa Rady Ministrów do określenia w drodze rozporządzenia zakresu, trybu i sposobu współdziałania Szefa ABW i Szefa SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa przez Szefa ABW, zrealizowana Rozporządzeniem Prezesa Rady Ministrów z dnia 4 października 2011 r.
- Art. 12 ust. 6: delegacja dla Prezesa Rady Ministrów do określenia w drodze rozporządzenia:

1) sposobu przygotowania oraz zakresu i trybu przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych;

2) trybu uzgadniania terminu kontroli, w tym czynności, o których mowa w ust. 1 pkt 1-5 i 8, wykonywanych w stosunku do Kancelarii Sejmu, Kancelarii Senatu oraz Kancelarii Prezydenta Rzeczypospolitej Polskiej;

3) zadań funkcjonariuszy ABW oraz funkcjonariuszy lub żołnierzy SKW nadzorujących i wykonujących czynności kontrolne;

4) sposobu dokumentowania czynności kontrolnych oraz sporządzania protokołu kontroli, wystąpienia pokontrolnego i informacji o wynikach

[15] Zob. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie*..., art. 1.

[16] *Ustawa z 5 sierpnia 2010 r. o ochronie*…; por., B. Iwaszko, *Ochrona informacji niejawnych w praktyce,* Presscom Sp. z o.o., Wrocław, 2012, s. 18-19.

kontroli, zrealizowana Rozporządzeniem Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r.

- Art. 13 ust. 4: delegacja dla Prezesa Rady Ministrów do określenia w drodze rozporządzenia:

1) szczegółowego zakresu, warunków, sposobu i trybu przekazywania przez kierowników jednostek organizacyjnych służbom i instytucjom uprawnionym doprowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego informacji, o których mowa w ust. 1 i 3, oraz udostępniania im dokumentów niezbędnych dla celów tych postępowań;

2) szczegółowego zakresu, warunków, sposobów i trybu udzielania przez Centralne Biuro Antykorupcyjne (zwane dalej „CBA"), Policję, Straż Graniczną, Żandarmerię Wojskową oraz organy kontroli skarbowej niezbędnej pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego przy wykonywaniu czynności w ramach tych postępowań, zrealizowana *Rozporządzeniem Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie przekazywania informacji*.

- Art. 18: delegacja dla Ministra Obrony Narodowej do określenia w drodze rozporządzenia:

1) szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych jemu podległych lub przez niego nadzorowanych;

2) szczególnych wymagań dotyczących stosowania środków bezpieczeństwa fizycznego przeznaczonych do ochrony informacji niejawnych;

3) miejsca i roli Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych oraz pełnomocników ochrony kierowników bezpośrednio nadrzędnych jednostek organizacyjnych w resortowym systemie ochrony informacji niejawnych;

4) zakresu, trybu i sposobu współdziałania pełnomocników ochrony w zakresie ochrony informacji niejawnych z SKW;

5) rodzajów, szczegółowych celów oraz sposób organizacji szkoleń w zakresie ochrony informacji niejawnych;

6) zakresu stosowania środków bezpieczeństwa fizycznego oraz kryteriów tworzenia stref ochronnych;

7) trybu opracowywania oraz niezbędne elementy planów ochrony informacji niejawnych, w tym postępowanie z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne" w razie wprowadzenia stanu nadzwyczajnego, a także sposób nadzorowania ich realizacji, zrealizowana *Rozporządzeniem MON z dnia 2 listopada 2011 r.*

- Art. 20 ust. 2: delegacja dla Prezesa Rady Ministrów do określenia w drodze rozporządzenia:

1) wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych;

2) sposobu rozliczania kosztów szkolenia, o których mowa w art. 19 ust. 4, zrealizowana *Rozporządzeniem Prezesa Rady Ministrów z dnia 28 grudnia 2010 r.*

- Art. 29 ust. 6: delegacja dla Prezesa Rady Ministrów do określenia w drodze rozporządzenia wzorów:

1) poświadczenia bezpieczeństwa;

2) poświadczeń bezpieczeństwa organizacji międzynarodowych, zrealizowana *Rozporządzeniem Prezesa Rady Ministrów z dnia 28 grudnia 2010*, poz. 1752.

- Art. 30 ust. 8: delegacja dla Prezesa Rady Ministrów do określenia w drodze rozporządzenia wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa, zrealizowana *Rozporządzeniem Prezesa Rady Ministrów z dnia 28 grudnia 2010 r*.
- Art. 33 ust. 12: Prezes Rady Ministrów określi, w drodze rozporządzenia, wzór decyzji o cofnięciu poświadczenia bezpieczeństwa, zrealizowano *Rozporządzeniem Prezesa Rady Ministrów z dnia 28 grudnia 2010 r.*
- Art. 47 ust. 1: Rada Ministrów określi w drodze rozporządzenia:

1) podstawowe kryteria i sposób określania poziomu zagrożeń oraz dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń;

2) wymagania w zakresie organizacji i funkcjonowania kancelarii tajnych;

3) rodzaje zagrożeń, które należy uwzględnić przy określaniu poziomu zagrożeń;

4) podstawowe elementy, które powinien zawierać plan ochrony informacji niejawnych;

5) zakres stosowania środków bezpieczeństwa fizycznego;

6) kryteria tworzenia stref ochronnych;

7) strukturę organizacyjną kancelarii tajnej, z uwzględnieniem możliwości tworzenia jej oddziałów;

8) podstawowe zadania kierownika kancelarii;

9) sposób i tryb przetwarzania informacji niejawnych;

10) wzór karty zapoznania się z dokumentem;

11) wzory dzienników ewidencji zrealizowano Rozporządzeniem z dnia 7 grudnia 2011 r.

Tabela 2 przedstawia zestawienie aktów wykonawczych do UOIN, których mnogość wskazuje na szeroki i złożony zakres obszaru podlegającego regulacjom.

Tabela 2.

Akty wykonawcze do UOIN

Dz. U. z 2010 r., nr 182, poz. 1228 *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*		
Akty wykonawcze		
Adres publikacyjny	Status	Tytuł
M.P. z 2013 r., nr 0, poz. 639	Obowiązujący	Zarządzenie nr 46 Prezesa Rady Ministrów z dnia 30 lipca 2013 r. w sprawie sposobu przeprowadzania przez Prezesa Rady Ministrów kontroli postępowań zrealizowanych przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego
Dz. U. z 2013 r., nr 0, poz. 1660	Obowiązujący	Rozporządzenie Ministra Obrony Narodowej z dnia 19 grudnia 2013 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych
Dz. U. z 2013 r., nr 0, poz. 11	Obowiązujący	Rozporządzenie Rady Ministrów z dnia 21 grudnia 2012 r. zmieniające rozporządzenie w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych
Dz. U. z 2012 r., nr 0, poz. 683	Obowiązujący	Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych
Dz. U. z 2011 r., nr 271, poz. 1603	Obowiązujący	Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne
Dz. U. z 2011 r., nr 220, poz. 1302	Obowiązujący	Rozporządzenie Prezesa Rady Ministrów z dnia 4 października 2011 r. w sprawie współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa

		Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa
Dz. U. z 2011 r., nr 159, poz. 949	Obowiązujący	Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego
Dz. U. z 2011 r., nr 159, poz. 948	Obowiązujący	Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego
Dz. U. z 2011 r., nr 156, poz. 926	Obowiązujący	Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego
Dz. U. z 2011 r., nr 93, poz. 541	Obowiązujący	Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych
Dz. U. z 2011 r., nr 86, poz. 470	Obowiązujący	Rozporządzenie Rady Ministrów z dnia 5 kwietnia 2011 r. w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego
Dz. U. z 2011 r., nr 67, poz. 356	Obowiązujący	Rozporządzenie Prezesa Rady Ministrów z dnia 22 marca 2011 r. w sprawie wysokości i trybu zwrotu zryczałtowanych kosztów ponoszonych przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego za przeprowadzenie sprawdzenia przedsiębiorcy oraz postępowań sprawdzających

Dz. U. z 2010 r., nr 258, poz. 1754	Obowiązujący	Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa
Dz. U. z 2010 r., nr 258, poz. 1753	Obowiązujący	Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa
Dz. U. z 2010 r., nr 258, poz. 1752	Obowiązujący	Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa
Dz. U. z 2010 r., nr 258, poz. 1750	Obowiązujący	Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego

Źródło: opracowanie własne na podstawie: http://isap.sejm.gov.pl/RelatedServlet?id=WDU20101821228&type=9&isNew=true [dostęp: 24.05.2014].

Podejmując próbę przedstawienia wybranych przepisów prawa w obszarze zagrożeń bezpieczeństwa informacyjnego, należy również zaznaczyć szczególną rolę regulacji zawartych w *Ustawie o zwalczaniu nieuczciwej konkurencji*[17].

Art. 11 powyższej ustawy stanowi, iż czynem nieuczciwej konkurencji jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża lub narusza interes przedsiębiorcy.

Zgodnie z literą prawa, *przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności*[18].

[17] *Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji,* Dz. U. z 2003 r., nr 153, poz. 1503.

[18] Tamże, art. 11, ust. 4.

Informacja uznana za tajemnicę przedsiębiorstwa to informacja charakteryzująca się brakiem publicznej jawności, która nie może zostać ujawniona nikomu spoza określonego zbioru osób stanowiących np. pracowników organizacji. Są nią zwykle wiadomości o charakterze technicznym, jak np.: plany techniczne, technologiczne, wiadomości o charakterze handlowym i marketingowym – listy klientów, cenniki, metody kontroli jakości towarów, wzory użytkowe, dane o wielkości produkcji i sprzedaży, know-how. Zatem zakres pojęcia tajemnicy jest szeroki, nie może być ona jednak wykorzystywana przeciwko wymiarowi sprawiedliwości i sąd lub prokurator są umocowani do zwolnienia osoby z obowiązku zachowania tajemnicy[19].

Czyn nieuczciwej konkurencji, jakim jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji, podlega karze: *kto, wbrew ciążącemu na nim obowiązkowi w stosunku do przedsiębiorcy, ujawnia innej osobie lub wykorzystuje we własnej działalności gospodarczej informację stanowiącą tajemnicę przedsiębiorstwa, jeżeli wyrządza to poważną szkodę przedsiębiorcy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Tej karze podlega również ten, kto, uzyskawszy bezprawnie informację stanowiącą tajemnicę przedsiębiorstwa, ujawnia ją innej osobie lub wykorzystuje we własnej działalności gospodarczej*[20].

Powyższe ustawy wraz z towarzyszącymi im aktami prawnymi ustanawiają dla podmiotu wyraźne obowiązki w obszarze bezpieczeństwa informacyjnego, dotyczące poufności i spójności pewnych informacji, *aby organizacja nie była przejrzysta i przeźroczysta dla konkurentów*[21]. W świetle powyższego, każdy podmiot gospodarczy powinien opracować swe wewnętrzne regulacje i zasady dotyczące systemów przeciwdziałających zagrożeniom utraty informacji.

Podsumowanie

Gwałtowny postęp cywilizacyjny, powstanie zbiorów olbrzymich zasobów informacji oraz rozwój środków komunikowania, jako zjawiska charakterystyczne dla czasów nam współczesnych[22], niosą szczególne zagrożenia dla bezpieczeństwa informacyjnego, a katalog tych zagrożeń jest katalogiem otwartym, gdyż wraz z rozwojem społeczeństwa informacyjnego pojawiają się nowe możliwości i wyzwania.

[19] J. Konieczny, *Wprowadzenie...*, s. 182.
[20] *Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu…*, art. 23 pkt 1 i 2.
[21] J. Konieczny, *Wprowadzenie…*, s. 6.
[22] M. Wrzosek, *Współczesne zagrożenia w obszarze bezpieczeństwa europejskiego,* Wydawnictwo Menedżerskie PTM, Warszawa, 2013, s. 179.

Wielorakość regulacji prawnych[23] w obszarze zagrożeń bezpieczeństwa informacyjnego wskazuje, iż we współczesnej organizacji jednym z najważniejszych zagrożeń bezpieczeństwa informacyjnego jest możliwość niekontrolowanego dostępu i ujawnienia informacji stanowiącej tajemnicę[24], a zagwarantowanie ochrony takiej informacji to szczególnie istotne wyzwanie, przed jakim stoją menedżerowie.

Za kluczowe akty prawne regulujące problematykę zagrożeń bezpieczeństwa informacyjnego w polskim systemie legislacyjnym należy uznać ustawę o ochronie informacji niejawnych i ustawę o ochronie danych osobowych, a prawo dostępu do informacji oraz jego ograniczenia wynikają bezpośrednio z Konstytucji Rzeczypospolitej Polskiej.

Bez wątpienia, przedsiębiorstwo w odpowiedzi na zagrożenia bezpieczeństwa informacyjnego, w celu ochrony szczególnego rodzaju aktywów, jakim jest informacja, powinno wykorzystać obowiązujące w jego kraju prawo, a także opracować dodatkowe formalne procedury, *gdyż ustrzeżenie informacji przed penetracją konkurentów jest jednym z podstawowych elementów utrzymania przewagi konkurencyjnej*[25].

Bibliografia

1. Dereń A. M., *Prawna ochrona informacji w krajowym ustawodawstwie*. *Wybrane zagadnienia*, Zeszyt 2008, OPO, Bydgoszcz, 2001.

2. Iwaszko B. *Ochrona informacji niejawnych w praktyce*, Presscom Sp. z o.o., Wrocław, 2012.

3. Konieczny J., *Wprowadzenie do bezpieczeństwa biznesu*, Konsalnet, Warszawa, 2004.

4. Liderman K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa, 2012.

[23] Za autorami M. i R. Taradejna jako akty prawne regulujące obszar ochrony informacji należy wymienić także m.in.: *Ustawę z dnia 23 kwietnia 1964 r. – Kodeks Cywilny*, *Ustawę z dnia 15 lutego 1962 r. o obywatelstwie polskim*, *Ustawę z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczpospolitej Polskiej*, *Ustawę z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych*, *Ustawę z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych, Ustawę z dnia 26 czerwca 1974 r. – Kodeks Pracy, Ustawę z dnia 10 czerwca 1994 r. o zamówieniach publicznych, Ustawę z dnia 29 czerwca 1995 r. o statystyce publicznej, Ustawę z dnia 29 września 1994 r. o rachunkowości, Ustawę o zawodzie lekarza, Prawo bankowe, Ustawę z dnia 26 maja 1982 r. o adwokaturze, Ustawę z dnia 20 czerwca 1985 r. o prokuraturze, Ustawę z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Ustawę z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji*. Zob. M. Taradejna, R. Taradejna, *Dostęp do informacji publicznej, a prawna ochrona informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego*, Adam Marszałek, Toruń, 2003, s. 332-333.

[24] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa, 2012, s. 61.

[25] Tamże, s. 170.

5. Nowak A., Scheffs W., *Zarządzanie bezpieczeństwem informacyjnym*, AON, Warszawa, 2010.

6. Taradejna M., Taradejna R., *Dostęp do informacji publicznej a prawna ochrona informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego*, Adam Marszałek, Toruń, 2003.

7. *Ustawa z 29 września 1994 r. o rachunkowości*, Dz. U. z 2009 r., nr 152, poz. 1223.

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

9. *Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji*, Dz. U. z 2003 r., nr 153, poz. 1503.

10. *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, Dz. U. z 1997 r., nr 133, poz. 883.

11. Wrzosek M., *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, AON, Warszawa, 2010.

12. Wrzosek M., *Współczesne zagrożenia w obszarze bezpieczeństwa europejskiego*, Wydawnictwo Menedżerskie PTM, Warszawa, 2013.

13. Żebrowski A., Kwiatkowski W., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza ABRYS, Kraków, 2000.

Źródła internetowe

1. http://isap.sejm.gov.pl.
2. http://isip.sejm.gov.pl.
3. http://www.iniejawna.pl.

SELECTED LEGAL REGULATIONS CONCERNING INFORMATION SECURITY THREATS. PART TWO

Abstract: Nowadays over two hundred acts of law refer to information protection. For each area of a company's operation, one can find several legal regulations that include regulations concerning information security in particular.

The most essential acts of law that deal with information security threat problems in the Polish legislative system include the Law on Protection of Classified Information and the Law on Personal Data Protection, marking a crucial role of regulations contained in the Act on Combating Unfair Competition.