JAN PILŻYS
Uniwersytet Szczeciński

# Zarządzanie ochroną informacji w systemach zarządzania kryzysowego[1]

Od maja 2004 roku Polska jest członkiem Unii Europejskiej. Rada Europy, Unia Europejska i poszczególne państwa członkowskie dostrzegły dynamiczny rozwój nowych technologii oraz usług komunikacji i informacji on-line. Ma to wpływ na stosunki społeczne, w tym na zwiększenie możliwości komunikowania się i wymiany informacji na poziomie krajowym i międzynarodowym. Należy jednak zwrócić uwagę zarówno na pozytywne, jak i negatywne skutki rozwoju technologii oraz rozpowszechniania, gromadzenia i przetwarzania informacji (danych) w sieciach i systemach teleinformatycznych[2]. Wszystkie wymienione poczynania muszą odbywać się w granicach obowiązującego prawa.

## Zdefiniowanie pojęcia informacji

Informacja jest pojęciem powszechnie używanym, intuicyjnie wyczuwa się jej istotę, to jednak trudno o ścisłą definicję. Często jest ona utożsamiana z wiadomością[3]. Otrzymać informację, to znaczy dowiedzieć się o czymś, o czym nie wiedziało się przedtem lub dowiedzieć się czegoś więcej o tym, o czym wiedziało się mniej.

Obecnie z łatwością można zdobywać informacje, czytając gazetę, książkę lub przeglądając strony Internetu. Internet to sieć komputerowa łącząca większość ośrodków akademickich świata oraz miliony prywatnych użytkowników, pozwalająca na ni-

[1] Aby swobodnie poruszać się w temacie referatu nieodzowne jest wyjaśnienie podstawowych pojęć związanych z podjętą problematyką: **zarządzanie informacją** – proces, który powinien zagwarantować integralność, poufność i wiarygodność przetwarzanej informacji z udziałem systemu informacyjnego; **system zarządzania kryzysowego** – zespół sił i środków znajdujących się w podsystemie kierowania i wykonawczym systemu, odpowiedzialnych za planowanie działań i reagowanie systemu, co do zaistniałych zagrożeń czasu pokoju, kryzysu i wojny; **zarządzanie kryzysowe** – działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej. Odbywa się przy jednoosobowym kierownictwie sprawowanym przez organy administracji publicznej (wójt, burmistrz, prezydent miasta, starosta, wojewoda, minister, premier rządu), którym jest podporządkowana (lub mogą być) administracja zespolona i niezespolona, różne instytucje i podmioty gospodarcze, na co dzień im nie podlegające; **sytuacja kryzysowa** – sytuacja wpływająca negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków. Definicje opracowano na podstawie: *Ustawa z 17 lipca 2009 r. o zmianie ustawy o zarządzaniu kryzysowym*, „Dziennik Ustaw RP" (dalej – Dz.U.) 2009, nr 131, poz. 1076, art. 2, 3; L. Kiełtyka, R. Kucęba, *Klasyfikacja i funkcjonalność informacji rynkowych oraz integratorów przepływu informacji w strukturach SIR*, w: *Zarządzanie przepływem i ochroną informacji*, Kraków 2007, s. 28; E. Nowak, *Zarządzanie logistyczne w sytuacjach kryzysowych*, Warszawa 2008, s. 74; J. Pilżys, *Zarządzanie kryzysowe*, Szczecin 2007, s. 11–34.

[2] Rekomendacja R (1999) 5 Komitetu Ministrów dla państw członkowskich w sprawie ochrony prywatności w Internecie. Wytyczne w sprawie ochrony osób w zakresie gromadzenia i przetwarzania danych osobowych w „Infostradach". Zob. także J. Kołakowski, J. Cichocki, *UMTS System telefonii komórkowej trzeciej generacji*, Warszawa 2003.

[3] W. Kopaliński, *Słownik wyrazów obcych*, Warszawa 2000, s. 229.

czym nieskrępowaną wymianę informacji, danych i korespondencji wszystkich ich użytkowników[4]. Nie powinno budzić wątpliwości stwierdzenie, że informacje można otrzymywać lub przekazywać. Oznacza to jednocześnie, że musi istnieć „usługodawca i usługobiorca"[5] informacji oraz jej nośnik, którym może być, np. tekst w książce lub na stronach internetowych.

Jeżeli występuje nośnik informacji, to potrzebny jest również odpowiedni kanał informacyjny między usługodawcą i usługobiorcą. Dociekliwy czytelnik z pewnością zapyta o sposób przyjmowania informacji za pomocą tekstu, lecz po chwili zastanowienia sam odpowie, że informację tekstową można odebrać przy pomocy wzroku, czyli za pomocą jednego z naszych receptorów.

Informacja, oddziałując na receptory, powoduje określone zmiany, zmniejszając lub usuwając niewiedzę odbiorcy. Informacja nie musi być nowiną, choć niewątpliwie nowina usuwa albo zmniejsza niewiedzę. Wyjaśnienie tej kwestii można uzyskać, wprowadzając pojęcie informacji dodatniej, zerowej i ujemnej. Informacja dodatnia zwiększa wiedzę o obiektywnej rzeczywistości, zerowa nie zmienia stanu wiedzy tego, kto ją otrzymał, natomiast informacja ujemna jest fałszywa, ponieważ uszczupla stan wiedzy o istniejącej rzeczywistości. Zerową wartość mogą mieć całe informacje bądź tylko niektóre jej fragmenty.

Dotychczasowe rozważania mogą nasunąć pytanie o możliwość pomiaru informacji. Nie wnikając w szczegóły, można odpowiedzieć twierdząco i dodać, że jako kryterium pomiaru informacji przyjmuje się wspomnianą już wartość ilościową oraz wartość użytkową, przy czym wartości ilościowej nie należy utożsamiać z objętością informacji, ale z wartością niewiedzy, jaką dana informacja usuwa.

Jednostką miary wartości ilościowej informacji jest bit, czyli ilość informacji związana z wyborem jednej z dwóch jednakowo prawdopodobnych możliwości.

Rozważając zagadnienie ilości informacji, należy zaznaczyć, że w tym samym określeniu może być zawarta różna ilość informacji, zależnie od objętości zbioru możliwych określeń.

Przez wartość użytkową informacji należy rozumieć jej przydatność (znaczenie, cenność) dla różnych odbiorców. Ta sama informacja może być w niejednakowym stopniu przydatna różnym odbiorcom, a nawet tym samym odbiorcom, lecz w różnym czasie i w różnych warunkach. Wynika to stąd, że wartość użytkowa informacji zależy od: aktualności, dokładności, kompletności, treściwości, komunikatywności, zdolności pojmowania usługobiorców, możliwości wykorzystania, zainteresowań usługobiorców, stopnia prawdziwości itp.

Informacja spóźniona może nie mieć żadnej wartości dla usługobiorcy. Podobnie niewielką wartość może przedstawiać informacja niedokładna, choć jest to relatywne. Niekiedy, zwłaszcza na wyższych szczeblach dowodzenia (kierowania), np. w reagowaniu kryzysowym jednostek ratownictwa, przy współpracy z wojskiem, policją i innymi służbami, szybkość, a zwłaszcza terminowość przekazywania informacji jest jak najbardziej pożądana.

Niekompletna informacja ma zawsze niższą wartość, ponieważ wiąże się z koniecznością zdobywania informacji uzupełniających. Pełniejsza informacja jest lepsza, ponieważ nie wymaga redukcji polegającej na eliminowaniu informacji nieprzydatnych oraz na łączeniu (uogólnieniu) cząstkowych informacji użytecznych, co następuje przy pomocy logicznego rozumowania. Jedna i ta sama informacja może być przekazana z wykorzystaniem różnej liczby sygnałów (znaków).

Zwiększenie treściwości informacji może usprawniać dowodzenie w zarządzaniu kryzysowym, lecz pociąga za sobą zmniejszenie odporności informacji na zakłócenia.

[4] Ibidem, s. 234.
[5] *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną*, Dz.U. 2002, nr 144, poz. 1204.

Jeśli w skondensowanej informacji zmieni się tylko jeden znak, to cała informacja może ulec zasadniczemu zniekształceniu.

Nie rozwijając wszystkich elementów, od których zależy użyteczność informacji, należy jednak zwrócić uwagę, że informacje ze względu na stopień prawdziwości dzielą się na:

– pewne – czyli takie, do których nie ma wątpliwości odnośnie ich prawdziwości, ponieważ zostały uzyskane osobiście lub potwierdzone z kilku źródeł,
– wiarygodne – niepotwierdzone, ale w świetle innych informacji wydają się zgodne z rzeczywistością,
– wątpliwe – często sprzeczne z innymi i budzące uzasadnione zastrzeżenia,
– fałszywe – takie, których niezgodność z rzeczywistością niewątpliwie stwierdzono, zwłaszcza w zestawieniu z informacjami pewnymi.

Wartość informacji, a zwłaszcza ich prawdziwość, wpływa na trafność decyzji, a pośrednio również na wynik naszego działania – sukcesów bądź porażek[6]. Dlatego każdy z nas powinien umieć oceniać informacje i odpowiednio organizować proces ich zbierania. Należy wiedzieć, jakie informacje i w jakich terminach będą potrzebne, jakimi informacjami dysponujemy, a jakie trzeba zdobyć.

Reasumując, informacja jest treścią, która może być przekazywana odpowiednim kanałem od jej nadawcy za pośrednictwem koderów i dekoderów do odbiorcy, oddziałując na jego receptory i powodując określone zmiany; jej miarą jest wartość ilościowa i jakościowa. Jest rodzajem zasobów, który pozwala na zwiększenie naszej wiedzy o nas i otaczającym świecie.

## Ochrona informacji niejawnych

W otoczeniu wewnętrznym, jak i zewnętrznym menedżerowie systemu zarządzania kryzysowego koncentrują się na pozyskaniu jak najwięcej informacji o potencjalnych zagrożeniach, sposobach im przeciwdziałania oraz zasobach systemu, w tym ludzi, sprzętu i materiałów. Odbywać się to może w czasie pokoju, kryzysu i wojny. Pozyskiwanie informacji wiąże się z ich gromadzeniem, przetwarzaniem oraz przesyłaniem do wielu odbiorców. Mogą to być informacje jawne, niejawne, o klauzulach tajności: ściśle tajne, tajne, poufne i zastrzeżone oraz takie, które w swoich zbiorach posiadają dane osobowe. To z kolei powoduje szukanie coraz to nowszych i bezpieczniejszych technik i technologii elektronicznych wchodzących w skład systemów informacyjnych, łączących pracowników pochodzących z różnych instytucji[7]. Jedne informacje są chronione ze względu na zadania, jakie system ma do wykonania, inne ze względu na wymogi przepisów prawa będącego wyrazem potrzeby uporządkowania naszych działań – wyznaczającego granice naszej aktywności informacyjnej. Ochronę wspomnianych informacji regulują ustawy o ochronie informacji niejawnych oraz danych osobowych[8]. Pierwsza z nich nakazuje prowadzenie zwykłych, poszerzonych, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego wobec osób, które mogą mieć lub mają dostęp do tajemnicy służbowej i państwowej[9]. Ponadto

---

[6] A. Austen, A. Frączkiewicz-Wronka, *Statystyka publiczna jako instrument wspomagający podejmowanie racjonalnych decyzji w organizacjach publicznych*, w: *Zarządzanie przepływem*…, s. 91; W. Pszenny, *Zarządzanie kryzysowe w świetle doktryny NATO. Ćwiczenie zgrywające „Bałtyk 2004" nt. „Działanie systemu reagowania kryzysowego w sytuacji zaistnienia rozległych skażeń środowiska morskiego i brzegu morza substancjami ropopochodnymi po katastrofie tankowca",* Mielno–Unieście 2004, s. 22.

[7] Przykładowo: urzędu wojewódzkiego, urzędu morskiego, wydziału zarządzania kryzysowego, Centrum Zarządzania Kryzysowego, policji, straży pożarnej, wojska, straży granicznej, placówek służby zdrowia, straży miejskiej, mediów, zakładów pracy.

[8] *Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych*, Dz.U. 2004, nr 33, poz. 285; *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,* Dz.U. 2010, nr 182, poz. 1228.

[9] Postępowanie sprawdzające ma na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy, m.in. czy sprawdzana osoba nie ma powiązań z wywiadem obcych służb specjalnych, bądź prowadzi działalność

ustawa wprowadziła w zakresie bezpieczeństwa teleinformatycznego oprócz akredytacji obowiązek posiadania certyfikatu systemu i sieci teleinformatycznej do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, na zasadach określonych w ustawie[10]. Każdy mający do czynienia z informacjami niejawnymi powinien zapoznać się z zagrożeniami informacji niejawnych i sposobami przeciwdziałania takim zagrożeniom, jak: podsłuch, wykradanie, fałszowanie, usuwanie danych, podszywanie pod inne osoby i źródła informacji, emisje ujawniające, wirusy komputerowe itp.[11]. Mogą one powodować utratę poufności, integralności i dostępności danych w sieci i systemie teleinformatycznym, np. Centrum Zarządzania Kryzysowego (CZK)[12]. Centrum bazuje na wydzielonej infrastrukturze technicznej, ze ściśle zdefiniowaną liczbą abonamentów i powiązań wspomaganych urządzeniami utajniającymi, o nowoczesnej strukturze i wydolnej przepustowości informacji. Ponadto specyfika sytuacji kryzysowej powoduje, że nie sposób przewidzieć wszystkich uczestników działań antykryzysowych, zakres i miejsce tych działań oraz źródła pozyskiwania informacji. Skłania to do budowania systemu o otwartej strukturze, ściśle powiązanym z Internetem, ale z zachowaniem wysokiego poziomu bezpieczeństwa (na wszystkich poziomach systemu), systemu zdolnego do współpracy z instytucjami państwowymi i ich społecznościami, które mogą nieść pomoc we wszystkich fazach zarządzania kryzysowego (przeciwdziałania, przygotowania, reagowania i odbudowy). Wszystkie wymienione zagrożenia dla informacji stanowiących tajemnicę państwową i służbową mogą być znacznie ograniczone (wyeliminowane) poprzez opracowanie odpowiedniej polityki bezpieczeństwa informacji, która powinna zdefiniować zasady dostępu do zasobów gromadzonych i przetwarzanych przez system, wskazać sposoby ich wyegzekwowania oraz osoby kompetentne i odpowiedzialne za ich bezpieczeństwo[13]. Zapewnienie niedostępności do sieci i systemu osiąga się poprzez wykorzystanie różnych metod: administracyjno-organizacyjnych, programowych, szyfrowych i technicznych. Ważne jest przy tym opracowanie procedur postępowania w sytuacjach kryzysowych na wypadek incydentów bezpieczeństwa informacji, których ujawnienie mogłoby spowodować zagrożenie[14]:

– żywotnych interesów Rzeczypospolitej Polskiej,
– obronności Rzeczypospolitej Polskiej,
– bezpieczeństwa wewnętrznego lub porządku konstytucyjnego Rzeczypospolitej Polskiej,
– bezpieczeństwa sojuszy, układów politycznych, wojskowych i ekonomicznych[15], których Rzeczypospolita Polska jest stroną,
– realizacji celów polityki zagranicznej Rzeczypospolitej Polskiej,
– utrzymania międzynarodowego pokoju i bezpieczeństwa,
– ujawnienia wykonywanych czynności służbowych (operacyjnych) funkcjonariuszy m.in. ABW i AW, SKW i KW, policji, w konsekwencji prowadzących do narażenia na

szpiegowską, terrorystyczna, sabotażową lub inną wymierzoną przeciwko Rzeczypospolitej Polskiej. Zob. *Ustawa o ochronie informacji niejawnych*..., art. 24.1-4 i art. 57.3.

[10] Akredytacją bezpieczeństwa teleinformatycznego – jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych, art. 2. Potwierdzeniem udzielenia akredytacji przez ABW lub SKW jest wydanie przez te instytucje świadectwa akredytacji, Zob. *Ustawa o ochronie informacji niejawnych*..., art. 2 i art. 48.1-6.

[11] M. Kielar, *Bezpieczeństwo informacji w systemie łączności*, „ Zeszyty Naukowe WSO im. gen. J. Bema" 2001, Rok XXXIV (20), s. 158.

[12] Centrum jest jednym z ważniejszych elementów systemu zarządzania kryzysowego – jest „sercem tegoż systemu", które m.in. zapewnia przepływ informacji na potrzeby zarządzania kryzysowego. Zob. *Ustawa z 17 lipca 2009 r. o zmianie ustawy*..., art. 13.2.

[13] Za ochronę informacji niejawnych odpowiada kierownik jednostki organizacyjnej oraz pełnomocnik do spraw ochrony informacji niejawnych. Zob. *Ustawa o ochronie informacji niejawnych*…, art. 14.1-3.

[14] Ibidem, art. 5.1; *Rozporządzenie Prezesa Rady Ministrów z dnia 9 września 2002 r. w sprawie wymiany informacji istotnych dla bezpieczeństwa zewnętrznego i międzynarodowej pozycji Rzeczypospolitej Polskiej*, Dz.U. 2002, nr 150, poz. 1243. Rozporządzenie określa tryb wymiany informacji między organami administracji rządowej w ramach Wspólnoty Informacyjnej Rządu.

[15] *Ustawa z dnia 14 lutego 2003 r. o udostępnianiu informacji gospodarczych*, Dz. U. 2003, nr 50, poz. 424.

szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej[16].

**Ochrona danych osobowych**

Spośród informacji dane osobowe są najpowszechniej prawnie chronione, tzn. dane pracowników wydziałów zarządzania i ochrony ludności, osób wyznaczonych do pracy w zespołach zarządzania kryzysowego, jak i osób z nimi współpracujących. Administrator danych osobowych w wydziale zarządzania kryzysowego, policji czy straży pożarnej powinien znać zagadnienia dotyczące ochrony danych osobowych zawarte w europejskich aktach prawnych, m.in. w konwencji nr 108 Rady Europy z 28 stycznia 1981 r. „O ochronie osób w związku z automatycznym przetwarzaniem danych osobowych", podpisanej przez Polskę w kwietniu 1999 roku i ratyfikowanej w maju 2002. Głównym celem tej konwencji jest zapewnienie każdej osobie fizycznej, bez względu na narodowość lub miejsce zamieszkania, poszanowania praw i podstawowych wolności na terytorium każdej ze stron konwencji, a w szczególności prawa do prywatności w związku z automatycznym przetwarzaniem danych osobowych. Innym bardzo ważnym dokumentem jest dyrektywa 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych.

Dyrektywa, poza tłumaczeniem niektórych pojęć, wprowadziła katalog praw służących osobom, których dane są gromadzone, m.in.: dochodzenie praw na drodze sądowej, zgoda osoby na przetwarzanie danych, której dotyczą, dane mogą być wykorzystywane zgodnie z celem, dla którego zostały zgromadzone, informowanie osoby o zasadach przetwarzania jej danych przed ich zgromadzeniem, możliwości ustalenia informacji dotyczących m.in. treści danych, czy to nie są jej dane wrażliwe (sensystywne), prawo kontroli danych osobowych oraz wniesienia sprzeciwu przeciwko przetwarzaniu danych przez osobę, której one dotyczą. Potwierdzeniem powyższych praw jest Karta Praw Podstawowych[17], która w art. 8 dotyczącym ochrony danych osobowych podaje, że każdy ma prawo do ochrony danych osobowych, dane te muszą być przetwarzane rzetelnie, w określonych celach i za zgodą osoby zainteresowanej lub na innej prawnie uzasadnionej podstawie określonej w ustawie oraz, że każdy ma prawo do dostępu do zebranych danych jego dotyczących i prawo do ich sprostowania. Przestrzeganie tych zasad podlega kontroli niezależnego organu (w Unii – Europejskiego Inspektora Ochrony Danych Osobowych, w Polsce – Głównego Inspektora Ochrony Danych Osobowych).

Powyższe zasady zostały zawarte w Konstytucji RP z roku 1997 w art. 47 i 51:

Art. 47. Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz decydowania o swoim życiu osobistym.

Art. 51.

1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawnienia informacji dotyczących jego osoby.
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

[16] *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*, Dz.U. 2006, nr 104, poz. 709; *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 lutego 2005 r. w sprawie przetwarzania przez Policję danych osobowych w celach wykrywczych lub identyfikacyjnych*, Dz.U. 2005, nr 34, poz. 313.

[17] Katalog podstawowych praw i wolności obywateli Unii Europejskiej zawarty w Karcie Praw Podstawowych UE – projekt został uzgodniony w październiku 2000 r., przyjęty i uroczyście ogłoszony na szczycie UE w Nicei 7 XII 2000 r.; Konwencja nr 108 Rady Europy z 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych.

3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania określa ustawa".

Powyższe dowodzi, że niektóre punkty artykułów Konstytucji Rzeczypospolitej Polskiej są zgodne z ustaleniami Karty Praw Podstawowych UE i zostały wprowadzone do polskiego ustawodawstwa.

Zasady określone w europejskich aktach prawnych są uważane przez projektodawców za zabezpieczenia minimalne. Państwa członkowskie zachowały wolność ustalania silniejszych środków ochrony. Jest to zalecenie, które powinno być dostosowane do wewnętrznego prawa każdego z krajów członkowskich.

W europejskich aktach prawnych (konwencje, dyrektywy, rekomendacje), jak i w krajowych (konstytucja, ustawy, rozporządzenia) z zakresu ochrony danych osobowych do najważniejszych celów zalicza się ujednolicenie przepisów prawnych obowiązujących w państwach członkowskich.

Czym są dane osobowe? W rozumieniu polskiej ustawy z 29 sierpnia 1997 roku o ochronie danych osobowych ...*za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej". Ten sam artykuł w ustępie 2 i 3 wyjaśnia, że ...osobą możliwą do zidentyfikowania jest ta osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań*[18].

Obecnie dane osobowe mogą przybierać formę m.in. podpisu elektronicznego, odcisku linii papilarnych, zarejestrowanego głosu, kodu DNA, wizerunku (geometria twarzy), odczytu tęczówki oka. Każdą z tych informacji można przetworzyć za pomocą komputera i zapisać w zbiorze danych, rozumianym przez ustawę jako zestaw danych o charakterze osobowym i o określonej strukturze, niezależnie od tego, czy zestaw jest rozproszony lub podzielony funkcjonalnie. Mamy tutaj do czynienia z bazą danych, zwaną dalej zbiorem danych zgromadzonych według określonej systematyki lub metody, indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagającym istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji jego zawartości[19].

Wszystkie podmioty wymienione w art. 3 ustawy o ochronie danych osobowych, jeżeli decydują o celach i środkach przetwarzania danych osobowych, nazywane są administratorami danych.

Do najważniejszych obowiązków administratorów danych ustawodawca zaliczył obowiązek zgłoszenia zbioru do rejestracji, poinformowania osoby, której dane są zbierane i odpowiedniego zabezpieczenia zbiorów danych[20].

Administrator danych może przystąpić do przetwarzania danych osobowych wtedy i tylko wtedy, gdy: ...*osoba, której dane dotyczą, wyrazi zgodę, chyba że chodzi o usunięcie dotyczących jej danych. Jest to niezbędne do realizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa*[21].

---

[18] *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, tekst jednolity: Dz.U. 1997, nr 101, poz. 926, ze zm., art. 6.1-3.

[19] *Ustawa z 27 lipca 2001 r. o ochronie baz danych*, Dz.U. 2001, nr 128, poz. 1402, art. 2.1; *Dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z 11 marca 1996 r. w sprawie ochrony prawnej baz danych*. Zob. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:15:31996L0009:PL:PDF

[20] M. Wyrzykowski, *Ochrona danych osobowych*, Warszawa 1999, s. 55.

[21] *Ustawa o ochronie danych osobowych z 29 sierpnia 1997 r. …* , art. 23.1.

Żeby rozporządzać bazą danych, usługodawca[22] (administrator danych) zgłasza zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO), podając: nazwę, charakterystykę administratora danych, opis kategorii osób, których dane będą dotyczyły oraz zakres przetwarzanych danych, sposób ich zbierania oraz udostępniania, opis środków technicznych i organizacyjnych zastosowanych, m.in. do zbierania, przetwarzania i ochrony danych osobowych[23].

Ustawa o ochronie danych osobowych określa prawa osoby do tzw. prywatności, np. prawa do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych (art. 32. ust.1), oprócz tego precyzuje wiele wymagań w stosunku do wszystkich podmiotów (administratorów danych), które danymi takimi dysponują.

Każdy podmiot wyszczególniony w ustawie o ochronie danych osobowych (art. 3) posiada bazę danych osobowych w określonym systemie informatycznym (teleinformatycznym) – rozumianym jako zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji (danych) i narzędzi programowych zastosowanych w celu wykonania jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

Każda z wyszczególnionych operacji (zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie) powinna podlegać zabezpieczeniu[24] poprzez wdrożenie do systemu środków bezpieczeństwa (technicznych i organizacyjnych) zapewniających ochronę danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia, wprowadzono trzy poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym: podstawowy, podwyższony i wysoki[25].

Poziom co najmniej podstawowy stosuje się, gdy w systemie informatycznym nie są przetwarzane dane wrażliwe, o których mowa w art. 27 ustawy o ochronie danych osobowych, oraz żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych, nie jest połączone z siecią publiczną.

Poziom co najmniej podwyższony stosuje się, gdy w systemie informatycznym są przetwarzane dane wrażliwe, o których mowa w art. 27 ustawy o ochronie danych osobowych, oraz żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych, nie jest połączone z siecią publiczną.

Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną. Ustawodawca przewidział środki bezpieczeństwa na każdym poziomie[26]. Na poziomie podstawowym nakazuje: zabezpieczać dane przed: dostępem do systemu osób nieuprawnionych, działaniem obcego oprogramowania, braku prądu, stosować mechanizmy kontroli dostępu do danych, m.in. po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia, wykonywać kopie zapasowe zbiorów danych, zachować szczególną ostroż-

[22] „Usługodawca – osoba fizyczna, osoba prawna albo jednostka organizacyjna nie posiadająca osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową świadczy usługi drogą elektroniczną". Zob. *Ustawa z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną*, Dz.U. 2002, nr 144, poz. 1204.

[23] Zob. *Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych*…, art. 40; *Rozporządzenie Ministerstwa Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych*, Dz.U. 2004, nr 100, poz. 1025.

[24] *Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych*…, art. 36. ust 1; *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.

[25] *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r.* ..., par. 6.

[26] Ibidem, Załącznik do rozporządzenia.

ność podczas transportu, przechowywania i użytkowania komputera z danymi poza obszarem chronionym. Zalecane jest stosowanie środków ochrony kryptograficznej wobec przetwarzanych danych osobowych, pozbawiać urządzenia, dyski lub inne elektroniczne nośniki informacji zapisu danych przeznaczonych do likwidacji, przekazania podmiotowi nieuprawnionemu do przetwarzania danych, naprawy, wyznaczyć sposób, miejsce i okres przechowywania, monitoring zabezpieczeń w tym wykonywanie przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Na podwyższonym poziomie ustawodawca nakazuje: do uwierzytelniania użytkowników używać hasła, które powinno składać się co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne, stosować środki bezpieczeństwa określone na poziomie podstawowym, ponadto, urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. l ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar, o którym mowa w § 4 pkt. l rozporządzenia, zabezpieczać w sposób zapewniający poufność i integralność tych danych.

Na wysokim poziomie ustawodawca nakazuje: chronić system informatyczny służący do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem. W przypadku zastosowania logicznych zabezpieczeń powinny one obejmować: kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych, stosować środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej. Administrator danych powinien stosować na poziomie wysokim środki bezpieczeństwa, określone na poziomie podstawowym, jak i podwyższonym, o ile zasady zawarte w części C załącznika nie stanowią inaczej.

Specyficznym dla pracy w sieci elementem ochrony danych jest regulowanie dostępu do danych. W rozumieniu ustawy o ochronie danych osobowych (art. 37) do systemu informatycznego przetwarzającego dane, mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych i zostały zarejestrowane. Ponadto system powinien posiadać możliwość jednoznacznego wskazania osoby, która określone dane wprowadziła do systemu lub zmieniła, oraz daty wprowadzenia. Upoważnienie powinno mieć formę pisemną. Wynika to z treści art. 39 ust. 1 ustawy stanowiącego, iż w ewidencji osób upoważnionych do przetwarzania danych osobowych, którą prowadzi administrator danych, wskazać należy imię i nazwisko osoby upoważnionej, datę nadania, ustania oraz zakres upoważnienia do przetwarzania danych, a także identyfikator, jeśli dane przetwarzane są w systemie informatycznym. Osoby, które zostały upoważnione do przetwarzania danych, są zobowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

Sytuacja może się skomplikować, gdy dane osobowe, a w szczególności ich zestaw, zbiór może być traktowany jako niejawny, który podlega szczególnej ochronie, gdy: część składających się nań danych ma charakter poufny, do danych można dotrzeć samodzielnie, ale w rezultacie działań bardziej czasochłonnych, niekiedy też kosztownych, istnieje inny jeszcze dysponent danych, który nie udostępnia jednak ich powszechnie[27].

W tej sytuacji administratorzy danych są zwolnieni z obowiązku rejestracji zbioru przez Głównego Inspektora Danych Osobowych (art. 43 par. 1 ustawy o ochronie danych osobowych).

Systemy i sieci teleinformatyczne, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne, podlegają akredytacji bezpie-

[27] J. Barta, R. Markiewicz, *Ochrona danych osobowych. Komentarze*, Kraków 2001, s. 133.

czeństwa teleinformatycznego przez właściwą służbę ochrony państwa oraz otrzymują certyfikat na podstawie[28]:

– zatwierdzonej przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego dokumentacji bezpieczeństwa systemu teleinformatycznego,
– wyników audytu bezpieczeństwa systemu teleinformatycznego przeprowadzonego przez wspomniane służby ochrony państwa,
– zatwierdzonych przez właściwą służbę ochrony państwa dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji, które opracowuje i przekazuje służbie ochrony państwa kierownik jednostki organizacyjnej[29].

Osoby naruszające normy ustalone przepisami ustawy ponoszą odpowiedzialność cywilną za szkody wynikłe z działań lub zaniechań. Odpowiedzialność ta jest wsparta dodatkowo przepisami karnymi – jeżeli ktoś przetwarza dane osobowe niezgodnie z celami utworzenia zbioru lub działa na niekorzyść zbioru (art. 49–54 ustawy o ochronie danych osobowych), może podlegać karze grzywny, ograniczenia wolności albo pozbawienia wolności[30].

* * *

Omówione akty prawne (europejskie i krajowe) określają podstawowe zasady gromadzenia, przetwarzania i przekazywania informacji niejawnych i danych osobowych. Są one gwarantem bezpieczeństwa i obronności państwa oraz ochrony prywatności i intymności człowieka. Ochrona ta w sensie informatycznym stanowi elementarną przesłankę wolności i godności człowieka oraz istnienia demokratycznego państwa prawnego[31].

Bezpieczeństwo pojedynczego człowieka, dobra kondycja rodziny i środowiska przyrodniczego pozwala rozwijać nowoczesną świadomość narodową i społeczną. Człowiek, informacja i komunikacja są tymi elementami życia, które pomagają rozwiązywać sytuacje kryzysowe, konflikty poprzez zebranie i analizowanie potrzebnych informacji (danych), podejmowanie słusznych decyzji, kierowanie zespołami ludzkim i kontrolowanie ich poczynań. Bazy danych istnieją w każdej dziedzinie życia (aktywności) człowieka: od urodzenia do śmierci, od życia zawodowego do emerytury. Problemy tkwią w: nieskuteczności tradycyjnych mechanizmów ochrony prywatności, słabości instrumentów zapobiegawczych, ważności interesów – publicznego czy narodowego, sformułowaniu jednolitej definicji tajności informacji, w tym ochrony poufności danych osobowych. Stąd też wypływają bardzo ważne wnioski: należy robić wszystko, aby nie dopuścić do naruszenia informacji (danych), a mniejszą uwagę poświęcić usunięciu jego skutków, zapobiegaćdominacji informacji nad prywatnością i w konsekwencji nad samym człowiekiem. Konieczne jest poszerzanie wiedzy prawniczej władzy publicznej, w tym osób odpowiedzialnych za zarządzanie kryzysowe.

[28] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*…, art. 48.6 i art. 49.1.
[29] Ibidem, art. 49.1-5; *Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego*, Dz.U. 2005, nr 171, poz. 1433.
[30] Zob. *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny,* Dz.U. z 1997 r., nr 88, poz. 553, Rozdział XXXIII dotyczący przestępstw przeciwko ochronie informacji.
[31] M. Wyrzykowski, *Ochrona danych*..., s. 38.

JAN PILŻYS

## Management of information protection in systems of crisis management

### Summary

We live in a world of new technologies, communication services and online informations. It has an influence on social relations, including increasing the capacity of communication and information exchange at national and international levels. This development brings the advantages and disadvantages, especially in the dissemination, collecting and processing of data in networks and telecommunication systems. These informations may be disclosed or protected by official secret. Anyone with such informations should secure them against eavesdropping, stealing, falsification, destruction of data, disclose issues, computer viruses, fire, electrical disturbance, water, atmospheric discharges, etc. All of these can cause the loss of confidentiality, integrity and availability of data in networks and telecommunication systems. The way to secure informations is to use safer techniques and electronic technologies. Thats why managers (agents for the protection of classified informations, personal data) are needed, defined as the organizers of specific activities, responsible for the development and use of resources at their disposal to protect informations. Thats why the knowledge of the law is needed which should help to develop information security policies, including procedures to be followed in emergency situations in case of information security incidents.