PRAWNE ASPEKTY INFORMACJI CHRONIONYCH

Redakcja naukowa

Mariusz Kubiak

Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
2020

dr hab. Mariusz KUBIAK, prof. uczelni
(redakcja naukowa)
ORCID: 0000-0002- 6757-5509

Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych, Instytut Nauk o Bezpieczeństwie

Recenzenci:

dr hab. Sławomir Zalewski, prof. uczelni
Szkoła Wyższa im. Pawła Włodkowica w Płocku

kmdr dr hab. Bartłomiej Pączek, prof. uczelni
Akademia Marynarki Wojennej, Gdynia

ISBN 978-83-66541-34-4

Wydawnictwo Naukowe UPH

Wydawnictwo Naukowe
Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach
www.wydawnictwo-naukowe.uph.edu.pl
08-110 Siedlce, ul. Żytnia 17/19, tel. 25 643 15 20
Ark. wyd. 11.7. Ark. druk. 14.5

Projekt okładki, druk i oprawa: Mazowieckie Centrum Poligrafii

Spis treści

Wstęp 5

Część pierwsza

Włodzimierz Fehler
Bariery informacyjne jako czynnik kształtujący współczesne bezpieczeństwo informacyjne 11

Robert Zapart
Perspektywa politycznego wykorzystywania informacji niejawnych w komunikowaniu publicznym 31

Waldemar Krztoń
Zarządzanie informacją – zarys problemu 47

Stanisław Topolewski
Zagrożenia dla bezpieczeństwa informacji 63

Tomasz Stefaniuk
Bezpieczeństwo informacji w świadczeniu pracy zdalnej 93

Część druga

Maria Hapunik
Zakres uprawnień służb państwowych do przetwarzania informacji w celu zapobiegania przestępstwom i ich zwalczania na przykładzie Policji 117

Jowita Sobczak
Obowiązek zgłaszania naruszeń ochrony danych osobowych w jednostkach organizacyjnych 131

Monika Kopczyńska
Przetwarzanie danych osobowych w Straży Granicznej 153

Joanna Tyburska
Zasada jawności dostępu do informacji publicznej – postępowanie egzekucyjne a prywatność osoby fizycznej 171

Artur Gajowniczek
Wybrane aspekty funkcjonowania Krajowego Systemu Cyberbezpieczeństwa w jednostkach samorządu terytorialnego na przykładzie województwa mazowieckiego 185

Urszula Adamczyk
Prawo do prywatności i ochrony danych osobowych w Rzeczypospolitej Polskiej 209

Wstęp

W dziejach cywilizacji ludzkiej informacja od zawsze była wyjątkowo cenionym dobrem niematerialnym. Dzięki jej specyficznemu charakterowi i posiadanym atrybutom, między innymi jako nośnika wiedzy, odgrywała i nadal odgrywa wręcz fundamentalną rolę zarówno w życiu państw, społeczeństw, jak i poszczególnych ludzi. Dlatego też zawsze starano się zapewnić jej ochronę, traktując zwykle w kategoriach wyłącznej przynależności do podmiotów, które ją stworzyły bądź pozyskały, będąc jej właścicielami (dysponentami). Tę ochronę miały zapewnić odpowiednie przepisy prawa stojące na straży jej bezpieczeństwa, bowiem to prawo w państwach demokratycznych stanowi ważny filar regulacji i porządku życia zbiorowego. Jego kreowanie, przestrzeganie i konsekwentne egzekwowanie w znacznej mierze świadczy o jakości życia społecznego oraz poziomie rozwoju państwa prawa i społeczeństwa obywatelskiego. Podjęte w monografii zagadnienia badawcze, zarówno teoretyczne, jak i typowo praktyczne, wpisują się we wszechstronne działania zmierzające do zapewnienia informacji odpowiedniej ochrony i statusu prawnego we współczesnych, jakże zmiennych uwarunkowaniach.

Monografia składa się z dwóch części. W części pierwszej zawarte są zagadnienia natury bardziej ogólnej i teoretycznej, zaś w drugiej, kwestie bardziej szczegółowe i pragmatyczne.

Część pierwszą monografii otwiera rozdział **Włodzimierza Fehlera** pt. *Bariery informacyjne jako czynnik kształtujący współczesne bezpieczeństwo informacyjne.* Autor już we wstępie na wielu przykładach z literatury przedmiotu ukazuje wielość i różnorodność definicyjną oraz znaczenie terminu informacja oraz społeczeństwo informacyjne. Następnie wskazuje na rosnące znaczenie informacyjnych aspektów bezpieczeństwa, a w tym kontekście na czynniki, które to utrudniają, czyli bariery informacyjne. W zakończeniu podkreśla, że aby zwiększyć

poziom bezpieczeństwa informacyjnego konieczne jest identyfikowanie, poznawanie i usuwanie istniejących barier oraz obszarów ich występowania.

Robert Zapart w materiale zatytułowanym *Perspektywa politycznego wykorzystywania informacji niejawnych w komunikowaniu publicznym* prezentuje zagadnienia dotyczące jawności i ograniczenia informacji z perspektywy demokratycznego państwa prawa. Zaznacza przy tym rolę komunikowania jako metody realizacji celów i interesów politycznych oraz informacji niejawnych w bieżącym przekazie publicznym.

W opracowaniu *Zarządzanie informacją – zarys problemu* **Waldemar Krztoń** podejmuje problemy związane z naturą informacji, pojęciem zarządzania oraz istotą zarządzania informacją. W konkluzjach podkreśla, że „Zapewnienie informacji dla organizacji związane jest przede wszystkim z podejmowaniem decyzji oraz stworzeniem takich warunków, aby realizowane funkcje zarządzania zapewniały osiągnięcie przez organizację założonych celów".

Stanisław Topolewski analizuje zagadnienie: *Zagrożenia dla bezpieczeństwa informacji.* W swoich rozważaniach rozpatruje problem potrzeby ochrony informacji, charakteryzuje pojęcie zagrożenia i dokonuje klasyfikacji zagrożeń dla bezpieczeństwa informacji. W dalszej części wskazuje na wybrane obszary zagrożeń dla przetwarzanych informacji: w systemach i sieciach teleinformatycznych, cyberprzestrzeni i dla infrastruktury krytycznej. Część końcową rozdziału poświęca przedsięwzięciom zmierzającym do przeciwdziałania zagrożeniom.

Problem *Bezpieczeństwa informacji w świadczeniu pracy zdalnej* rozważa **Tomasz Stefaniuk**. Rozdział składa się z trzech części. W części pierwszej autor przedstawia istotę i miejsce pracy zdalnej we współczesnym świecie. W drugiej – zagrożenia dla bezpieczeństwa informacji w pracy zdalnej oraz ich następstwa, a w trzeciej – ochronę informacji w organizacji pracy zdalnej.

Część drugą książki otwiera rozdział **Marii Hapunik** *Zakres uprawnień służb państwowych do przetwarzania informacji w celu zapobiegania i zwalczania przestępstw na przykładzie Policji*, w którym autorka podejmuje tematykę dotyczącą ochrony danych osobowych w czynnościach służbowych podejmowanych i realizowanych przez polską Policję.

Obowiązek zgłaszania naruszeń ochrony danych osobowych w jednostkach organizacyjnych omawia **Jowita Sobczak**. Przybliża pojęcie naruszeń

ochrony danych osobowych i wskazuje na obowiązek ich zgłaszania organowi nadzorczemu oraz zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony jej danych osobowych. Analizuje to zagadnienie w oparciu o przykłady najczęściej występujących naruszeń danych osobowych w jednostkach organizacyjnych.

Monika Kopczyńska przedmiotem swoich dociekań uczyniła *Przetwarzanie danych osobowych w Straży Granicznej.* Autorka w części wstępnej rozdziału przybliża wybrane aspekty działalności Straży Granicznej, by w kolejnych przedmiotem swych badań uczynić dane osobowe przetwarzane w tej formacji mundurowej.

Joanna Tyburska koncentruje swą uwagę badawczą na zagadnieniu: *Zasada jawności dostępu do informacji publicznej – postępowanie egzekucyjne a prywatność osoby fizycznej.* Autorka wprowadza czytelnika w problematykę danych osobowych, po czym zwraca uwagę na kolizję wartości konstytucyjnych w postaci dostępu do informacji publicznej i prywatności osoby fizycznej. W dalszej części rozpatruje problematykę postępowania windykacyjnego w aspekcie przetwarzania danych zgodnie z RODO.

Artur Gajowniczek prezentuje *Wybrane aspekty funkcjonowania Krajowego Systemu Cyberbezpieczeństwa w jednostkach samorządu terytorialnego na przykładzie województwa mazowieckiego*. Autor analizuje ten niezwykle istotny z punktu widzenia bezpieczeństwa przetwarzanych informacji temat na podstawie uzyskanych wyników badań własnych.

Urszula Adamczyk poświęciła swoje rozważania kwestii fundamentów ochrony prywatności w RP. Jej tekst pt. *Prawo do prywatności i ochrony danych osobowych w Rzeczypospolitej Polskiej* dotyka najważniejszych prawnych i organizacyjnych podstaw zapewnienia ochrony danych osobowych i prywatności w Polsce.

Redaktor opracowania wyraża nadzieję, że niniejsza publikacja przybliży wszystkim zainteresowanym Czytelnikom problematykę zagadnień dotyczących prawnych uwarunkowań bezpieczeństwa informacji oraz stanie się pomocnym materiałem dydaktycznym dla studentów różnych kierunków studiów, a zwłaszcza – bezpieczeństwa narodowego oraz bezpieczeństwa wewnętrznego.

Mariusz Kubiak

Część pierwsza

WŁODZIMIERZ FEHLER
ORCID: 0000-0002-0927-4337
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych

Bariery informacyjne jako czynnik kształtujący współczesne bezpieczeństwo informacyjne

Procesy informowania oparte na wytwarzaniu, zdobywaniu, przekazywaniu, odbieraniu, gromadzeniu i wykorzystywaniu informacji towarzyszą rodzajowi ludzkiemu od początków jego istnienia. Od zawsze bowiem człowiek starał się, stosując środki i instrumenty dostępne mu na danym etapie rozwoju, przekazywać innym swoje odczucia, wrażenia, doświadczenia, poglądy, stanowiska i decyzje. Jednocześnie dążył także do skutecznego odbioru i gromadzenia informacji, które przekazać mogli mu inni ludzie oraz otoczenie. Czynił tak zarówno po to, by rozwiązywać bieżące problemy, jak i po to, by budować w oparciu o pozyskiwane informacje wiedzę decydującą o jego losie w dłuższej perspektywie. Można zatem stwierdzić, że potrzeba ekspresji i komunikowania się z innymi ludźmi stała się jednym z ważniejszych mechanizmów rozwoju cywilizacyjnego. Opierając się na wynikach badań amerykańskiego matematyka Claude'a E. Shannona[1], twórcy ilościowej teorii informacji, należy podkreślić, że informacje stanowią nie tylko

[1]Claude Elwood Shannon (1916–2001) – amerykański matematyk i inżynier, jeden z kreatorów teorii informacji. Związany z prestiżowym Massachusetts Institute of Technology (MIT), gdzie od roku 1958 był profesorem. Pracował także w Laboratoriach Bella – ośrodku badawczym, w którym powstało m.in. ogniwo fotowoltaiczne, tranzystor, laser oraz fotokomórka. Istotne przedmioty jego zainteresowań stanowiły również kod binarny oraz sztuczna inteligencja. Najbardziej znane dzieło C.E. Shannona to opublikowana w 1948 r. *Matematyczna teoria komunikacji* (A Mathematical Theory of Communication). Jej treści stworzyły podwaliny pod teorię informacji i kodowania.

podstawę budowania wiedzy, ale wpływają także na jej wykorzystywanie. Dzieje się tak m.in. dlatego, że kształtują one sposoby postrzegania i interpretacji zjawisk zachodzących w otaczającym człowieka środowisku oraz w nim samym. W rezultacie umożliwiają dostosowywanie się do zmiennej rzeczywistości oraz pozwalają na jej przekształcanie tak, aby stawała się ona jak najbardziej przyjazna. Informacja, która zawsze odgrywała ważną rolę w funkcjonowaniu ludzkości, z czasem uzyskała rangę zasobu o znaczeniu strategicznym. Współczesne społeczeństwo, charakteryzujące się dużą dynamiką rozwoju, nie tylko wytwarza coraz więcej informacji, ale także coraz więcej ich potrzebuje. Tego, czym jest informacja, jak dotychczas nie udało się ująć w ścisłe i powszechnie akceptowane definicje. Jak celnie zauważa Marcin Koszowy, termin ten występuje w wielu kontekstach[2]. Nieprzypadkowo zatem francuski matematyk René Thom[3] określił pojęcie informacji (ze względu na jej szczególną zdolność do zmiany znaczenia pod wpływem otoczenia i kontekstu) mianem „semantycznego kameleona”[4]. Zgodnie ze słownikowym ujęciem informacja to: „powiadomienie o czymś, zakomunikowanie czegoś, wiadomość, wskazówka, pouczenie”[5]. Tadeusz Kifner stwierdza, że „informacja jest elementem wiedzy, faktem, wiadomością, komunikatem lub wskazówką gromadzoną, komunikowaną lub przekazywaną komuś za pomocą jakiegoś kodu lub języka”[6]. Jerzy Seidler reprezentuje pogląd mówiący o tym, że „informacją można nazwać to wszystko, co jest użytkowane do bardziej sprawnego wyboru działań prowadzących do realizacji pewnego celu”[7]. Nieco inaczej widzi istotę informacji Elżbieta Niedzielska, która zauważa, że jest ona „tym co, w jakiś sposób, porządkuje rzeczy, fakty, zjawiska, procesy itp., a mówiąc dokładniej – tym czymś, co danym (nie przetworzonej, »surowej« liczbie, tekstowi, obrazowi, dźwiękom) przydaje ostatecznie treści znaczeniowej, wzbogacając naszą wiedzę o przedmiocie

[2] Zob. M. Koszowy, *Informacja – nowe pojęcie filozoficzne?*, [w:] *Internet i nowe technologie – ku społeczeństwu przyszłości*, red. T. Zasępa, R. Chmura, Częstochowa 2003, s. 39.

[3] René Thom (1923-2002) – francuski matematyk, członek Francuskiej Akademii Nauk, autor prac z topologii algebraicznej i różniczkowej (przestrzeń Thoma), twórca teorii katastrof, która przyniosła mu największy rozgłos.

[4] Zob. Z. Tworak, *W stronę jednolitej teorii informacji. Propozycja Marka Burgina*, „Studia Metodologiczne” 2015, nr 35 (4), s. 84.

[5] *Uniwersalny słownik języka polskiego*, red. S. Dubisz, Warszawa 2003, t. 1, s. 1212.

[6] T. Kifner, *Polityka bezpieczeństwa i ochrony informacji*, Gliwice 1999, s. 14.

[7] J. Seidler, *Nauka o informacji*, Warszawa 1983, s. 69.

rozważań”[8]. W ramach zamknięcia tego fragmentu rozważań – do dalszego wykorzystania przyjęto definicję autorstwa Piotra Sienkiewicza określającą informację jako „zbiór faktów, zdarzeń, cech itp. określonych obiektów (rzeczy, procesów, systemów) zawarty w wiadomości (komunikacie), tak ujęty i podany w takiej postaci (formie), że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działanie umysłowe lub fizyczne”[9]. Należy zauważyć, że ujęcie to podkreśla znaczenie informacji wynikające z tego, iż jest ona zasobem pozwalającym na systematyczne zmniejszanie niepewności przez pogłębianie wiedzy o otaczającym człowieka świecie i o nim samym. Warto w tym miejscu zauważyć, że na bazie nieustannego wzrostu roli informacji w początkach lat 60. XX w. w Japonii zrodziła się idea społeczeństwa informacyjnego[10], która zresztą bardzo szybko się zmaterializowała, m.in. dzięki dynamicznemu rozwojowi komputeryzacji oraz powstałemu w USA Internetowi[11]. Jak zauważa Marian Golka, powstanie społeczeństwa informacyjnego można potraktować „jako pewną wersję »dojrzałości dziejów«, jako coś, do czego świat powoli zmierzał poprzez kolejne wynalazki komunikacyjne: od sygnałów za pomocą chemii ciała i komunikowania niewerbalnego, poprzez mowę i rozmowę, pismo i druk, do nowych mediów związanych z cyfrową obróbką danych. Jest tu ukryte myślenie teleologiczne – taki cel musiał »przyświecać« rozwojowi cywilizacji ludzkiej, cel, którym miałaby być poprawa warunków działalności człowieka”[12]. Społeczeństwo informacyjne, które

[8] E. Niedzielska, *Podstawowe pojęcia informatyki*, [w:] *Informatyka ekonomiczna*, red. E. Niedzielska, Wrocław 1998, s. 14.

[9] P. Sienkiewicz, *Ewaluacja informacji w społeczeństwie informacyjnym*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego – Ekonomiczne Problemy Usług” 2011, nr 67, s. 127.

[10] Termin „społeczeństwo informacyjne” (jap. *johoka shakai* – społeczeństwo komunikujące się przez komputery), wprowadził do obiegu naukowego japoński etnolog Tadao Umesao, publikując w 1963 r. artykuł o ewolucyjnej teorii społeczeństwa opartego na przetwarzaniu informacji. Następnie pojęcie to spopularyzował japoński teoretyk mediów Kenichi Koyama, stosując je w wydanej w 1968 r. pracy *Introduction to Information Theory* (*Wprowadzenie do teorii informacji,* Tokyo 1968). Wspomnieć należy także o zasługach kolejnego Japończyka Yoneji Masudy, który dokonał szczegółowego opisu zmian zachodzących w obrębie społeczeństwa opartego na sektorze informacji i telekomunikacji, publikując w 1981 r. książkę *The Information Society as Post-industrial Society* (Tokyo 1981).

[11] Pierwsza wersja sieci o nazwie Arpanet została zaprezentowana w 1969 r. i łączyła komputery z uniwersytetów w Los Angeles, Stanford, Santa Barbara oraz Utah.

[12] M. Golka, *Czym jest społeczeństwo informacyjne*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny” 2005, z. 4, s. 262.

charakteryzuje się wysokim stopniem wykorzystania informacji w codziennym życiu przez większą część ludzkiej populacji, a także umiejętnością jej odbioru, przekazu i szybkiej wymiany bez względu na odległość, jest jednocześnie kolejnym etapem w rozwoju społecznym, który nastąpił po erze agrarnej i industrialnej[13].

Na grunt europejski problematykę społeczeństwa informacyjnego jako pierwsi wprowadzili francuscy socjologowie Alain Minc i Simon Nora, którzy zawarli odniesienia do tej kwestii w przekazanym w 1978 r. prezydentowi Francji Giscardowi d'Estaing raporcie zatytułowanym *L'lnformatisation de la Societe*. Fundamentalne zasługi w dziedzinie rozwoju społeczeństwa informacyjnego w Europie trzeba przypisać jednak Martinowi Bangemannowi[14] sprawującemu w latach 1993-99 funkcję komisarza Unii Europejskiej ds. Polityki Przemysłowej, Technologii Informatycznych i Telekomunikacji. W grudniu 1993 r. stanął on na czele grupy roboczej, której zadaniem było przygotowanie ekspertyzy mającej odpowiedzieć na to, jakie działania należy podjąć, aby skutecznie budować społeczeństwo informacyjne na obszarze UE. W rezultacie prac wspomnianego zespołu ekspertów powstał raport zatytułowany *Europa i globalne społeczeństwo informacyjne: zalecenia dla Rady Europy* (*Europe and the Global Information Society: recommendations to the European Council*). Został on przedstawiony Radzie Europejskiej w czerwcu 1994 r. i od tego czasu znany jest jako raport Bangemanna. Twórcy tego dokumentu apelowali do kierowniczych gremiów UE o rozpoczęcie działań umożliwiających tworzenie nowych, dynamicznie rozwijających się sektorów gospodarki oraz podjęcie wspólnych kroków na rzecz takiego ujednolicenia przepisów prawnych, aby umożliwić powstanie konkurencyjnego ogólnoeuropejskiego rynku usług informacyjnych. Raport Bangemanna wskazywał dwa podstawowe obszary, w których należałoby rozpocząć budowę europejskiego społeczeństwa informacyjnego. Pierwszy – to rozwijanie świadomości społecznej, ze

[13] Zob. P. Aftański, *Społeczeństwo informacyjne – nowy wymiar informacji*, „Dydaktyka Informatyki" 2011, nr 6, s. 67.

[14] Martin Bangemann (ur. 1934 r.) – niemiecki polityk, który w latach 1985-1988 był szefem Wolnej Partii Demokratycznej (FDP). Od 1973 r. do 1984 r. w różnych rolach zasiadał w Parlamencie Europejskim (m.in. w latach 1976-1979 był wiceprzewodniczącym, a od 1979 r. do 1984 r. przewodniczącym Grupy Liberalno-Demokratycznej). W okresie lat 1984-1988 wchodził w skład rządu RFN jako minister gospodarki. W latach 1989-1995 był komisarzem UE ds. rynku wewnętrznego i spraw przemysłowych, następnie w latach 1995-1999 komisarzem ds. polityki przemysłowej, technologii informatycznych i telekomunikacji.

szczególnym naciskiem na sektor małych i średnich przedsiębiorstw, administrację państwową oraz młode pokolenie obywateli UE. Drugi – to wprowadzanie nowatorskich rozwiązań technologicznych w odniesieniu do systemów telekomunikacji, sieci przesyłu informacji (telefonicznych, satelitarnych i kablowych) oraz budowa europejskiej infrastruktury szerokopasmowej, pozwalającej na połączenie wszystkich tych sieci. Jednocześnie autorzy raportu zaproponowali podjęcie dziesięciu inicjatyw w zakresie zastosowania nowoczesnych technologii informacyjnych w takich dziedzinach jak: telepraca, nauka na odległość, sieci dla uniwersytetów i centrów badawczych, usługi telematyczne dla małych i średnich przedsiębiorstw, zarządzanie ruchem drogowym, kontrola ruchu powietrznego, sieci opieki zdrowotnej, elektroniczne przetargi, ogólnoeuropejska sieć administracji publicznej, miejskie autostrady informacji[15]. We wspomnianym dokumencie podkreślono, że infrastruktury informacyjne są tworami bez granic w środowisku otwartego rynku, w związku z czym społeczeństwo informacyjne posiada globalne rozmiary[16]. W odpowiedzi na przywoływany raport UE podjęła szereg kolejnych prac eksperckich ukierunkowanych na przeanalizowanie możliwości związanych z rozwojem społeczeństwa informacyjnego oraz przyjęła plany działań, które dzięki ich skutecznej realizacji pozwoliły na wprowadzenie państw Unii w erę społeczeństwa informacyjnego. Można powiedzieć, że pojęcie „społeczeństwo informacyjne" w ostatnich dekadach stało się określeniem kluczowym, służącym do objaśniania szeregu przeobrażeń społecznych. Jeżeli chodzi o jego istotę, to literatura przedmiotu obfituje w bardzo wiele definicji tego terminu. W większości z nich społeczeństwo informacyjne jest traktowane jako konstrukt, którego najważniejsze składniki niezbędne do sprawnego funkcjonowania to: produkcja, gromadzenie i obieg informacji. Dla członków takiego społeczeństwa komputer, Internet oraz techniki cyfrowe stanowią jeden z najważniejszych elementów życia i pracy[17]. Według P. Sienkiewicza społeczeństwo informacyjne to

[15] Zob. A. Demczuk, *Od raportu Bangemanna do Strategii Europa 2020. Rozwój społeczeństwa informacyjnego w polityce Unii Europejskiej – bilans 15 lat*, „Annales Uniwersitas Mariae Curie-Skłodowska", Lublin 2016, Vol. XXIII, s. 30.

[16] Zob. J. Małkowski, *Społeczeństwo informacyjne w Unii Europejskiej*, s. 9, https://alebank.pl/wp-content/plugins/lc-edocsviewer/stream.php?hash=Sav2/y/9k5RG39IpDDgXqS7RSdSWQBLZv3QQsLgl2qO79OleSAsY5M9I2gVn4M5mfDy7eNXRwFME6Pl/C6cdTzZF/25Q9L3AzsvPZa8i6UQ= [dostęp 29.03.2020].

[17] Zob. M. Golka, *Czym jest społeczeństwo informacyjne*, dz. cyt., s. 254.

„system społeczny, ukształtowany w procesie informacji, w którym systemy informacyjne i zasoby informacyjne determinują społeczną strukturę zatrudnienia, wzrost zamożności społeczeństwa (dochodu narodowego) oraz stanowią podstawę orientacji cywilizacyjnej”[18]. W optyce Kazimierza Krzysztofka i Marka S. Szczepańskiego społeczeństwo informacyjne to takie „społeczeństwo, w którym informacje intensywnie wykorzystuje się w życiu społecznym, kulturalnym, ekonomicznym i politycznym. Bogate środki komunikacji i przetwarzania informacji są tu podstawą tworzenia większości dochodu narodowego i stanowią źródło utrzymania dla większości ludzi”[19]. W opracowaniu *ePolska. Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006 s*połeczeństwo informacyjne zdefiniowano jako „system społeczeństwa kształtujący się w krajach o wysokim stopniu rozwoju technologicznego, gdzie zarządzanie informacją, jej jakość, szybkość przepływu są zasadniczymi czynnikami konkurencyjności zarówno w przemyśle, jak i w usługach, a stopień rozwoju wymaga stosowania nowych technik gromadzenia, przetwarzania, przekazywania i użytkowania informacji”[20]. Zważywszy na potrzeby prowadzonych rozważań, za najbardziej adekwatną do dalszych rozważań przyjęto definicję Tomasza Gobana-Klasa głoszącą, że „społeczeństwo informacyjne to społeczeństwo, które nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz także środki te są podstawą tworzenia dochodu narodowego i dostarczają źródła utrzymania większości społeczeństwa”[21]. Do elementarnych cech społeczeństwa informacyjnego za Agnieszką Pawłowską zaliczyć należy jego wielowarstwowość, na którą składa się:

- substrat technologiczny (infrastruktura informatyczna, urządzenia służące do gromadzenia, przetwarzania, przechowywania i udostępniania

[18] P. Sienkiewicz, *Teorie rozwoju społeczeństwa informacyjnego*, [w:] *Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego. Dylematy cywilizacyjno-kulturowe*, red. L.H. Haber, Kraków 2002, s. 506-507.

[19] K. Krzysztofek, M.S. Szczepański, *Zrozumieć rozwój: od społeczeństw tradycyjnych do informacyjnych*, Katowice 2005, s. 170.

[20] ePolska. Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006, Warszawa 2001, s. 69, http://www.cyfrowyurzad.pl/gfx/cyfrowyurzad/files/iza/epolska.pdf [dostęp 29.03.2020].

[21] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne. Szanse, zagrożenia, wyzwania*, Kraków 1999, s. 53.

informacji, kanały transmisji danych wraz z możliwościami łączenia ich w rozmaitych konfiguracjach);
- substrat ekonomiczny (gałęzie produkcji i usług zajmujące się wytwarzaniem informacji, technik informacyjnych oraz ich dystrybucją);
- substrat społeczny (odsetek osób korzystających w pracy, szkole i domu z nowoczesnych technologii informacyjnych);
- substrat kulturowy (kultura informacyjna obejmująca postrzeganie informacji jako dobra strategicznego i towaru, odpowiedni poziom kultury informatycznej związanej z umiejętnościami posługiwania się urządzeniami informatycznymi)[22].

Cechy charakterystyczne społeczeństwa informacyjnego to przede wszystkim:
- wysoki poziom korzystania z informacji przez większość obywateli i organizacji;
- posługiwanie się jednorodnymi lub kompatybilnymi technologiami informacyjnymi na użytek własny, społeczny, w edukacji i działalności zawodowej;
- zdolność do przekazywania, odbierania oraz szybkiej wymiany danych bez względu na odległość[23].

W związku z dynamicznym rozwojem społeczeństwa informacyjnego, w którym informacja stanowi kluczowy produkt i zasób, gwałtownie zaczęło rosnąć także znaczenie informacyjnych aspektów bezpieczeństwa. W rezultacie bezpieczeństwo informacyjne stało się jednym z kluczowych, wyodrębnianych przy użyciu kryterium przedmiotowego, wymiarów bezpieczeństwa. Należy przy tym zauważyć, że w kwestii pojmowania jego istoty bardzo często przyjmowana jest postawa ekskluzywna, ograniczająca się tylko do ochrony informacji niejawnych oraz cyberprzestrzeni i zachodzących w niej procesów. Dostrzegając rosnącą rolę i rangę technologii informatycznych, nie można jednak w myśleniu i działaniu na rzecz bezpieczeństwa pomijać tradycyjnej „klasycznej" części infosfery, która cały czas funkcjonuje i jako taka musi być uwzględniana. Na

[22] Zob. A. Pawłowska, *Zasoby informacyjne w administracji publicznej w Polsce. Problemy zarządzania*, Lublin 2002, s. 23-39.
[23] Zob. M. Nowina-Konopka, *Istota i rozwój społeczeństwa informacyjnego*, [w:] *Społeczeństwo informacyjne. Istota, rozwój wyzwania*, red. M. Witkowska, K. Cholawo-Sosnowska, Warszawa 2006, s. 15.

gruncie krytycznej analizy istniejących przykładów ujęć (często mało adekwatnych) istoty bezpieczeństwa informacyjnego[24] należy stwierdzić, iż poprawna, odpowiadająca współczesnej roli informacji oraz dynamicznemu rozwojowi społeczeństwa informacyjnego charakterystyka istoty bezpieczeństwa informacyjnego nie znalazła właściwego zobrazowania. W ramach działań prowadzących do zmiany takiego stanu rzeczy, opierając się na wnioskach z przeprowadzonych badań oraz uwzględniając aktualny stan funkcjonowania społeczeństwa informacyjnego, uzasadnionym jest przyjęcie poglądu wskazującego, że bezpieczeństwo informacyjne to proces i ciąg stanów, w ramach których zapewniane są – zgodne ze standardami demokratycznego państwa prawa – swoboda wytwarzania, dostępu, gromadzenia, przetwarzania i przepływu odpowiedniej ilości, wysokiej jakości informacji (osiąganej przez merytoryczną selekcję) połączona z racjonalnym, prawnym i zwyczajowym wyodrębnianiem takich ich kategorii, które podlegają szczególnej ochronie bądź reglamentacji ze względu na bezpieczeństwo podmiotów, których one dotyczą[25]. Zważywszy na kluczowe znaczenie dla tak rozumianego bezpieczeństwa informacyjnego swobody dostępu i przepływu informacji, bardzo istotną staje się kwestia czynników, które je utrudniają, czyli barier informacyjnych. W ujęciu jednego z polskich fachowych słowników bariera informacyjna to „przeszkoda utrudniająca lub uniemożliwiająca korzystanie z informacji bądź rozpowszechnianie informacji"[26]. Z kolei niemiecki *Lexikon Information und Dokumentation* wskazuje, że „bariera informacyjna to przeszkoda, która zakłóca proces przepływu informacji od jej twórcy do użytkownika. Może oddziaływać na użytkownika informacji niezależnie od jego świadomości (bariery obiektywne) lub poprzez tę świadomość (bariery subiektywne). Bariera informacyjna powoduje, że istniejące informacje nie są wykorzystywane z dwóch powodów:

1) ponieważ użytkownik nie wie o ich istnieniu lub nie korzysta ze znanych źródeł informacji;

[24] Szerzej na ten temat: zob. W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne w XXI wieku*, red. M. Kubiak, S. Topolewski, Siedlce-Warszawa 2016.
[25] *Leksykon bezpieczeństwa wewnętrznego*, red. W. Fehler, J.J. Piątek, R. Podgórzańska, Szczecin 2017, s. 74.
[26] *Słownik terminologiczny informacji naukowej*, red. M. Dembowska i in., Wrocław-Warszawa 1979, s. 28.

2) ponieważ użytkownik ma utrudniony dostęp do tych źródeł, z różnych przyczyn”[27].

Według niemieckiego badacza Heinza Engelberta z Uniwersytetu Humboldta w Berlinie bariery informacyjne to „zjawiska obiektywnej rzeczywistości, które zakłócają proces swobodnego przepływu informacji od jej twórcy do adresata (użytkownika)”[28]. Marzena Świgoń z kolei uważa, że „bariery informacyjne (information barriers), nazywane także barierami w dostępie do wiedzy i informacji, są to przeszkody i ograniczenia, które utrudniają lub uniemożliwiają korzystanie i rozpowszechnianie wiedzy i informacji, czyli ich przepływ od nadawcy do odbiorcy”[29]. Przywołana badaczka wskazuje także, iż najwcześniej – bo w latach siedemdziesiątych XX wieku – termin ten pojawił się w piśmiennictwie rosyjskim, a później w niemieckim[30]. Opierając się na przedstawionych przykładach, można przyjąć do dalszego wykorzystania ujęcie, zgodnie z którym bariera informacyjna to względnie trwały rodzaj przeszkody, która utrudnia, ogranicza lub uniemożliwia pozyskiwanie, przekazywanie, dostarczanie i wykorzystywanie informacji.

Zagadnieniami identyfikacji istoty i klasyfikacji barier informacyjnych występujących w różnych aspektach ludzkiej aktywności zajmują się m.in. Dietrich E. Haag i Thomas D. Wilson. Pierwszy z wymienionych badaczy jest postrzegany jako prekursor prac nad barierami informacyjnymi. Marianna Banacka zwraca uwagę na fakt, że w latach osiemdziesiątych XX wieku skonstruował on szczegółową klasyfikację, w której zawarł listę kilkudziesięciu utrudnień[31]. Wspomniana badaczka przywołuje także czteroskładnikową klasyfikację barier T.D. Wilsona zawierającą bariery:

1) związane z osobą użytkownika;
2) interpersonalne;
3) środowiskowe;

[27] *Lexikon Information und Dokumentation*, red. S. Rückl, G. Schmoll, Lipsk 1984, s. 187.
[28] M. Świgoń, *Bariery informacyjne w środowisku naukowym*. *Badania pilotażowe*, „Przegląd Biblioteczny” 2003, z. 4, s. 38.
[29] M. Świgoń, *Bariery informacyjne*, [w:] *Nauka o informacji*, red. W. Babik, Warszawa 2016, s. 457.
[30] Tamże.
[31] Zob. M. Banacka, *Współczesne bariery w dostępie do informacji. Kilka uwag w związku z ich typologiami i rodzajami*, s. 2, http://e-pedagogiczna.edu.pl/upload/file/dokumenty/jarocin1.pdf [dostęp 1.04.2020].

4) związane ze źródłami informacji[32].

Jeżeli chodzi o innych znawców problematyki, to do najbardziej rozpoznawalnych z racji posiadanego dorobku zaliczyć można Elżbietę B. Zybert, Jolantę Sobielgę, Marię Próchnicką i Marzenę Świgoń. Każda z nich sformułowała własną klasyfikację barier informacyjnych. M. Próchnicka przyjęła, że istnieją dwie grupy barier:

- o charakterze zewnętrznym, względnie niezależne od użytkownika informacji (np. czasowe i ekonomiczne);
- o charakterze wewnętrznym, wynikające z niedostatecznego przygotowania użytkowników do odbioru informacji oraz deficytu umiejętności selekcji źródeł informacji[33].

Z kolei E.B. Zybert, która badała środowiska osób niedostosowanych społecznie, wskazuje na bariery:

- środowiskowe (rodzinne, szkolne, rówieśnicze);
- psychologiczne (np. atmosfera w pracy);
- intelektualne (brak umiejętności czytania i pisania, ograniczone formy wypowiedzi słownej, obniżenie ogólnego poziomu inteligencji, nieświadomość istnienia ciekawych książek)[34].

Inną, interesującą propozycję klasyfikacji barier informacyjnych przedstawiła J. Sobielga, która, nawiązując do uwarunkowań zewnętrznych użytkowania informacji oraz predyspozycji użytkownika w tym zakresie, podzieliła je na:

- przeszkody fizyczne związane z identyfikacją i wyszukiwaniem (pozyskiwaniem) oraz wykorzystaniem informacji;
- ograniczenia występujące ze strony podmiotów współpracujących z poszukującymi informacji w procesie ich użytkowania;
- przeszkody wynikające z niedostatecznych umiejętności użytkowników, ujawniające się w procesie korzystania z informacji;

[32] Zob. tamże.

[33] Zob. M. Próchnicka, *Informacja a umysł*, Kraków 1991, s. 169.

[34] Zob. E.B. Zybert, *Bariery w dostępie do książki i biblioteki w środowisku niedostosowanych społecznie*, „Poradnik Bibliotekarza" 1992, nr 7/8, s. 11.

- procesy i stany psychiczne użytkownika informacji blokujące efektywne jej wykorzystanie[35].

Z kolei w klasyfikacji sporządzonej przez M. Świgoń, mającej bardzo rozbudowany i stosunkowo wyczerpujący charakter, występują cztery grupy barier informacyjnych:

- związane z czynnikami indywidualnymi;
- interpersonalne;
- środowiskowe;
- związane ze źródłem informacji.

W ramach pierwszej grupy, która łączy się z intelektualnymi, edukacyjnymi i psychologicznymi czynnikami charakteryzującymi użytkownika informacji, przywoływana badaczka wskazuje na istnienie barier:

- nieświadomości – wynikających z braku potrzeb informacyjnych;
- terminologicznych – związanych z trudnościami w odbiorze informacji specjalistycznych;
- nieznajomości lub słabej znajomości języków obcych;
- deficytu kwalifikacji potrzebnych do poszukiwania i pozyskiwania informacji;
- braku motywacji i zaangażowania w poszukiwanie informacji;
- oporu przed korzystaniem z nowoczesnych technologii informacyjnych oraz usługami podmiotów oferujących zbiory informacji.

Druga grupa barier (interpersonalnych), zgodnie z poglądami M. Świgoń, może pojawić się wówczas, gdy źródłem informacji jest inna osoba lub jeżeli interakcja interpersonalna jest niezbędna do uzyskania dostępu do źródła informacji[36]. Podstawowe bariery w tej grupie to:

- opór psychiczny poszukujących/użytkujących informację przed zadawaniem pytań: specjalistom z danej dziedziny, współpracownikom, personelowi obsługującemu zbiory informacji;

[35] Zob. J. Sobielga, *Psychologiczne aspekty barier informacyjnych – badania wśród studentów*, „Praktyka i Teoria Informacji Naukowej i Technicznej" 1997, nr 4, s. 14.

[36] M. Świgoń zwraca uwagę, że mogą to być bariery występujące zarówno po stronie osób poszukujących informacji, jak i po stronie osób udzielających informacji.

- brak wsparcia ze strony osób będących bezpośrednim lub pośrednim źródłem informacji (np. ekspertów, współpracowników/kolegów, bibliotekarzy).

Trzecia, środowiskowa grupa barier, wiąże się z bliższym lub dalszym otoczeniem użytkowników informacji, czyli z warunkami zewnętrznymi, na które nie posiadają oni wpływu lub wpływ ten mają ograniczony. Ten zbiór barier to:

- bariery prawne – związane z ochroną tajemnic, praw własności intelektualnej i przemysłowej, ochroną danych osobowych czy ochroną archiwaliów;
- bariery finansowe – niedobór lub brak środków finansowych koniecznych do zdobycia dostępu do informacji (np. konieczność wnoszenia opłat za: udział w konferencjach naukowych i szkoleniach, dostęp do baz danych, dostęp do Internetu, dostęp do płatnych archiwów prasowych itp.);
- bariery geograficzne – utrudniające nawiązywanie współpracy międzynarodowej lub korzystanie ze zbiorów i zasobów, których nie poddano digitalizacji;
- bariery polityczne – wynikające z aktualnej sytuacji politycznej (krajowej międzynarodowej);
- bariery kulturowe – związane z różnicami w kulturach państw i narodów;
- bariery organizacyjne – związane z kulturą organizacji, atmosferą i relacjami pomiędzy pracownikami, a także przepływem wiedzy pomiędzy organizacjami i instytucjami (np. światem nauki a podmiotami gospodarczymi).

Czwartą grupę tworzą bariery wiążące się ze źródłami informacji, takie jak:

- bariera nadmiaru informacji i niedoboru wiedzy w nich zawartej;
- bariera niskiej jakości informacji i wiedzy (informacje nierzetelne, niewiarygodne, przestarzałe);
- bariera dominacji języka angielskiego w międzynarodowej komunikacji naukowej;
- bariera opóźnień w zakresie upubliczniania informacji;
- bariera dostępu do informacji niepublikowanych;
- bariera niedoskonałości narzędzi wyszukiwawczych;

- bariera niesprawności w działalności organizacji i instytucji gromadzących i udostępniających zasoby informacyjne[37].

Opierając się na dokonanym przeglądzie stanowisk dotyczących podziału barier informacyjnych w syntetycznym ujęciu, można wskazać na istnienie kilku ogólnych ich typów, które w różnych (często wzajemnie przenikających się) konfiguracjach oddziaływają na bezpieczeństwo informacyjne, obniżając jego poziom szczególnie w aspektach: dostępności, swobody przekazu i użyteczności informacji. Lista tych barier obejmuje:

- bariery przestrzenne;
- bariery techniczno-technologiczne;
- bariery ekonomiczne;
- bariery społeczno-edukacyjne;
- bariery temporalne;
- bariery psychologiczne;
- bariery zdrowotne;
- bariery językowe;
- bariery terminologiczne;
- bariery administracyjne.

Jeżeli chodzi o bariery przestrzenne związane z brakiem możliwości i znacznymi ograniczeniami w zakresie przekazu informacji na dłuższą odległość[38], to przez wiele stuleci należały one do kluczowych. Jednak, dzięki wszechstronnemu postępowi w dziedzinie środków komunikacji i przesyłu informacji osiągniętemu w XIX i XX stuleciu, bariery te zostały przełamane i w zasadzie[39] odeszły do

[37] Zob. M. Świgoń, *Bariery informacyjne*, [w:] *Nauka o informacji*, dz. cyt., s. 460-462.

[38] Warto w tym miejscu wspomnieć np. o jednym z osiągnięć cywilizacji inkaskiej, w ramach której stworzono system kurierski oparty na posłańcach pieszych zwanych chasci, dla których wzdłuż dróg pobudowano specjalne stacje. Przesyłanie wiadomości i drobnych przesyłek odbywało się na zasadzie sztafety. Kiedy jeden biegacz docierał do stacji, drugi przejmował przesyłkę lub wiadomość i natychmiast ruszał w drogę. Sztafeta chasci była tak sprawna, że informacje z Cuzco do Quito, które dzieli prawie 3 tys. km, docierały w czasie mniej więcej 6 dni. Pamiętać należy również o afrykańskim języku bębnów szczelinowych (tam-tamów), za pomocą których niepiśmienne plemiona afrykańskie w epoce przedkolonialnej komunikowały się na odległościach przekraczających setki kilometrów. Wtedy nikt na świecie nie potrafił przesyłać złożonych informacji tak szybko.

[39] Pamiętać jednak należy, że bariery przestrzenne ujawniają się w sytuacjach, kiedy rezygnujemy z pośredniego przekazu i chcemy (lub musimy) poszukiwać informacji bezpośrednio u źródeł znajdujących się np. w geograficznie odległych czy trudno dostępnych miejscach.

historii. Obecnie niemal każda informacja może być natychmiast przekazana pomiędzy najbardziej nawet oddalonymi punktami na kuli ziemskiej. Dotyczy to przede wszystkim informacji bieżących. W przypadku barier techniczno-technologicznych należy wskazać na dwie ich grupy. Pierwsza – wiąże się z technicznym i infrastrukturalnym upośledzeniem niektórych państw (obszarów geograficznych) oraz warstw społecznych w zakresie dostępu do najnowszych rozwiązań w sferze informacyjnej. Druga – to nienadążanie rozwoju techniki, technologii i organizacji w zakresie korzystania z informacji za lawinowym jej przyrostem. Istnienie barier ekonomicznych łączy się z bezpośrednimi kosztami finansowymi, jakie trzeba ponieść w związku z poszukiwaniem informacji i ich przetwarzaniem, co nie wszyscy są w stanie w odpowiednim wymiarze udźwignąć. Istotne są także bariery społeczno-edukacyjne powstające na gruncie niedostatków w zakresie wykształcenia, braku aspiracji rozwojowych, deficytów wiedzy ogólnej (z których może wynikać niemożność zrozumienia czy odpowiedniej interpretacji posiadanych informacji), zdolności i motywacji do poszukiwania i przyswajania treści informacji. W ramach tej grupy barier istnieje także bariera obejmująca brak orientacji w odniesieniu do istnienia informacji mogących zaspokoić potrzeby informacyjne.

Bariery temporalne wynikają z ograniczonego czasu na pozyskiwanie informacji – a także braku czasu na jej odpowiednie przyswojenie czy interpretację. Bariery psychologiczne są związane z różnego rodzaju nieuzasadnionymi merytorycznie tendencyjnymi opiniami i uprzedzeniami w odniesieniu do źródeł informacji (autorów, środków przekazu, książek, tytułów prasowych uznawanych z założenia np. za obrazoburcze, radykalne, antypaństwowe, antynarodowe). Do barier psychologicznych należy także pasywna postawa wobec wyszukiwania informacji i niechęć do podejmowania wysiłku intelektualnego. Bariery zdrowotne wiążą się z różnymi formami niesprawności oraz schorzeń (fizycznych i psychicznych) generujących problemy z dostępem do informacji oraz z jej przetwarzaniem i przyswajaniem. Kolejna bardzo istotna i stosunkowo rzadko charakteryzowana grupa przeszkód to bariery językowe. Ich istnienie wiąże się przede wszystkim z faktem, że mieszkańcy kuli ziemskiej posługują się różnymi językami, których – jak się szacuje – jest obecnie ok. 7 tysięcy (przy czym w ciągu ostatnich 500 lat

wymarło ich ok. 9 tys.)[40]. Próby zniwelowania tej przeszkody poprzez tworzenie języków sztucznych nie powiodły się[41]. Pewnym pomostem przerzucanym nad tymi barierami jest postępujące upowszechnianie się tzw. języków konferencyjnych (j. angielski, j. francuski, j. niemiecki). Duży postęp odnotowuje się także w zakresie różnych form translacji przy użyciu nowoczesnych technik komputerowych. Mimo to posługiwanie się małą liczbą języków znacznie ogranicza swobodę przepływu i dostępu do zgromadzonych przez różne narody informacji. Bariery językowe nie sprzyjają także wzajemnemu poznawaniu i zrozumieniu w szerszym ujęciu, czyli poznaniu kultur, religii, podstaw stylu życia, zwyczajów. Bardzo widocznymi negatywnymi skutkami istnienia barier językowych jest wynikająca z braków informacyjnych wrogość, nieuzasadnione odrzucenie, błędne interpretowanie zachowań, mylne odczytywanie innych przekazów. Konsekwencją istnienia barier językowych jest również podatność na manipulacje pośredników informacyjnych, z których część ma skłonności do tendencyjnego opisywania oraz charakteryzowania ludzi i zjawisk z obcych językowo obszarów. Blisko spokrewnione z barierami językowymi są bariery terminologiczne, polegające na trudności w zrozumieniu poszczególnych informacji z powodu używania hermetycznej, nieznanej odbiorcom terminologii. Jest rzeczą oczywistą i zrozumiałą, że każda dziedzina wiedzy posiada swój specyficzny język i siatkę pojęciową, z której korzystają jej przedstawiciele. Problem tkwi w tym, że często reprezentanci niektórych zawodów (np. lekarze, prawnicy, inżynierowie, bankowcy) nie chcą lub nie potrafią w sposób czytelny i zrozumiały komunikować się ze swoimi pacjentami, klientami, interesantami czy partnerami w różnych przedsięwzięciach i dostarczać potrzebnych im informacji w sposób zrozumiały. Bariery terminologiczne powodują, że odbiorcy niektórych informacji (np. pacjenci, klienci banków czy firm ubezpieczeniowych) stają się ofiarami nieczytelnych dla nich diagnoz czy podstępnie

[40] Zob. O. Woźniak, *Skąd się wzięły języki i po co nam ich tyle*, „Gazeta Wyborcza" z 2 maja 2018 r., https://wyborcza.pl/7,75400,23344459,skad-sie-wziely-jezyki.html [dostęp 1.04.2020].

[41] Najbardziej rozpoznawalne języki sztuczne to: wolapik (autor: John Martin Schleyer – Niemcy), esperanto (autor: Ludwik Zamenhof – Polska), occidental (autor: Edgar de Wahl – Estonia), Basic English (autor: Charles Kay Ogden – Anglia), interlingua (autor: International Auxiliary Language Association), logan (autor: James Cooke Brown – USA), europanto (autor: Diego Marani – Włochy), slovio (autor: Mark Hučko – Słowacja/Szwajcaria). Szerzej na ten temat: zob. N. Soldecka, *8 najciekawszych sztucznych języków*, https://menway.interia.pl/obyczaje/nauka/news-8-najciekawszych-sztucznych-jezykow,nId,451587#utm_source=paste&utm_medium=paste&utm_campaign=chrome [dostęp 1.04.2020].

sformułowanych umów, generujących np. zawyżone koszty. Bariery terminologiczne to także posługiwanie się ograniczonym zasobem słów, słownictwem prymitywnym oraz zwulgaryzowanym. Do barier terminologicznych zaliczyć możemy również rozległe deformacje językowe o charakterze polityczno-poprawnościowym, reklamowym, populistyczno-prostackim. Swoistą barierą terminologiczną jest coraz częściej pojawiający się w różnych opracowaniach pseudonaukowy język, oparty na pustosłowiu nasyconym fasadowo-rozbudowaną frazeologią, który przy zachowaniu pozorów naukowości nie niesie jednak żadnych istotnych i sensownych przekazów merytorycznych.

Bariery administracyjne wiążą się z różnego rodzaju regulacjami ograniczającymi dostęp do informacji i swobodę jej dystrybucji. Szczególnie dotkliwe rodzaje barier administracyjnych to cenzura oraz nieuzasadnione ograniczanie jawności informacji. Cenzura, czyli administracyjne określanie tego, jakie treści mogą być rozpowszechniane, ma bogatą tradycję i wiele odmian. Może mieć charakter religijny (np. znany z przeszłości Indeks ksiąg zakazanych) czy obyczajowy, obejmujący np. zakaz pokazywania określonych scen w filmach[42]. Cenzura bardzo często ma również charakter polityczny. Stosują ją państwa niedemokratyczne w szczególności po to, aby: umacniać autorytet przywódców, budować jedność narodu, mobilizować do realizacji celów wskazywanych przez władzę, prowadzić skuteczną indoktrynację. W warunkach działania cenzury szerokie kręgi społeczeństwa otrzymują informacje niepełne, często spreparowane i poprzez to budujące fałszywy obraz rzeczywistości. Cenzura, ingerując w różne formy komunikowania się i przekazywania informacji (m.in. w prasę, film, literaturę, Internet), czyni z nich instrumenty ideologicznej obróbki, ograniczając funkcje informacyjne i kulturotwórcze. Jednym z negatywnych efektów obowiązywania cenzury jest fałszowanie historii poprzez pomijanie w oficjalnie dostępnych źródłach informacji i faktów niewygodnych dla władz lub też przedstawianie ich w sposób zniekształcony bądź całkowicie fałszywy. Cenzura pozbawia także możliwości działania czwartą władzę, czyli media. W warunkach braku wolności słowa nie da się

[42] Przykładem takich działań jest tzw. Kodeks Haysa od nazwiska W.H. Haysa, który w latach 1922–45 przewodniczył amerykańskiemu związkowi producentów i dystrybutorów filmowych (MPPD). Był on jednym z inicjatorów i autorów zbioru drobiazgowych przepisów obyczajowej cenzury filmowej, ogłoszonego w 1931 i zaostrzonego w 1935 r. Kodeks ten, rygorystycznie określający co wolno pokazywać na ekranie, obowiązywał aż do 1966 r.

bowiem skutecznie realizować misji informowania społeczeństwa, w której mieści się również ukazywanie zła, nieprawidłowości oraz ocenianie skuteczności i racjonalności działań rządzących. Kolejnym skutkiem funkcjonowania cenzury politycznej jest uniformizowanie poglądów wynikające z braku możliwości swobody ich wymiany, prowadzenia polemik i wygłaszania nonkonformistycznych wypowiedzi. Chociaż działania cenzorskie coraz trudniej jest stosować we współczesnym świecie, to jednak tego typu bariera nadal ujawnia swą destrukcyjną siłę w wielu państwach (np. w Chinach, Korei Północnej czy na Białorusi) i nie można jej traktować jako zjawiska historycznego. Do barier administracyjnych należy zaliczyć także ograniczanie dostępu do informacji poprzez nieuzasadnione określanie jej jako poufnej czy tajnej oraz utrudnianie dostępu przez przedstawicieli władz (państwowych, samorządowych) do informacji o charakterze publicznym.

Reasumując, należy stwierdzić, że każdy z użytkowników informacji, mimo imponującego postępu w niwelowaniu barier informacyjnych, staje (i to dość często) w obliczu różnych ich odmian utrudniających mu funkcjonowanie. W świetle teorii i praktyki bezpieczeństwa informacyjnego widać, że bariery informacyjne są zjawiskiem stale obecnym w procesach kształtowania przestrzeni informacyjnej jednostek, organizacji i społeczeństw. W tym kontekście, dostrzegając wpisanie problematyki tych barier w obszar zainteresowania badawczego ekologii informacji (zajmującej się wzajemnymi oddziaływaniami człowieka na informację i odwrotnie, a także relacjami informacyjnymi między ludźmi w prywatnej i publicznej przestrzeni informacyjnej) za niezbędne należy uznać także (zważywszy na znaczenie informacyjnego wymiaru bezpieczeństwa) zintensyfikowanie zainteresowania tą problematyką na gruncie nauk o bezpieczeństwie. Należy podkreślić, że towarzyszące człowiekowi różne bariery informacyjne w niesprzyjających okolicznościach i przy kumulacji ich wystąpienia mogą prowadzić do znacznego obniżenia poziomu bezpieczeństwa informacyjnego, którego fundamentem jest dostęp do wysokiej jakości informacji oraz swoboda jej transferu. W takiej sytuacji infosfera tak dla jednostek, jak i dla podmiotów zbiorowych, może przyjmować kształt środowiska nieprzyjaznego czy nawet wrogiego. Aby ograniczyć ilość i zasięg takich sytuacji i skutecznie obniżać towarzyszący im stres informacyjny oraz poczucie zagrożenia dla bezpieczeństwa informacyjnego, obok usuwania istniejących barier (co realizowane jest w zróżnicowanym tempie w różnych obszarach i w odniesieniu do różnych środowisk) konieczne jest także ich

identyfikowanie i poznawanie. Dotyczy to zarówno samych barier, jak i miejsc ich występowania oraz wyrządzanych przez te bariery szkód. Takie działanie pozwoli na: wypracowywanie sposobów zapobiegania i przełamywania barier informacyjnych, minimalizowanie skutków istnienia tych, których przełamać w danym momencie nie można oraz blokowanie powstawania nowych. Jednym z narzędzi takiego działania jest stałe budowanie i uzupełnianie kompetencji informacyjnych. Tylko bowiem ich odpowiedni zasób zapewni zainteresowanym podmiotom w sposób względnie trwały status pełnoprawnego i bezpiecznego uczestnictwa we współczesnym społeczeństwie informacyjnym.

Bibliografia

Aftański P., *Społeczeństwo informacyjne – nowy wymiar informacji*, „Dydaktyka Informatyki" 2011, nr 6.

Banacka M., *Współczesne bariery w dostępie do informacji. Kilka uwag w związku z ich typologiami i rodzajami*, http://e-pedagogiczna.edu.pl/upload/file/dokumenty/jarocin1.pdf.

Demczuk A., *Od raportu Bangemanna do Strategii Europa 2020. Rozwój społeczeństwa informacyjnego w polityce Unii Europejskiej – bilans 15 lat*, „Annales Uniwersitas Mariae Curie-Skłodowska", Lublin 2016, Vol. XXIII.

ePolska. Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006, Warszawa 2001, http://www.cyfrowyurzad.pl/gfx/cyfrowyurzad/files/iza/epolska.pdf.

Fehler W., *O pojęciu bezpieczeństwa informacyjnego,* [w:] *Bezpieczeństwo informacyjne w XXI wieku*, red. M. Kubiak, S. Topolewski, Siedlce-Warszawa 2016.

Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne. Szanse, zagrożenia, wyzwania*, Kraków 1999.

Golka M., *Czym jest społeczeństwo informacyjne*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2005, z. 4.

Kenichi K., *Introduction to Information Theory*, Tokyo 1968.

Kifner T., *Polityka bezpieczeństwa i ochrony informacji*, Gliwice 1999.

Koszowy M., *Informacja – nowe pojęcie filozoficzne?*, [w:] *Internet i nowe technologie – ku społeczeństwu przyszłości*, red. T. Zasępa, R. Chmura, Częstochowa 2003.

Krzysztofek K., Szczepański M.S., *Zrozumieć rozwój: od społeczeństw tradycyjnych do informacyjnych,* Katowice 2005.

Leksykon bezpieczeństwa wewnętrznego, red. W. Fehler, J.J. Piątek, R. Podgórzańska, Szczecin 2017.

Lexikon Information und Dokumentation, red. S. Rückl, G. Schmoll, Lipsk 1984.

Małkowski J., *Społeczeństwo informacyjne w Unii Europejskiej*, https://alebank.pl/wp-content/plugins/lc-edocsviewer/stream.php?hash=Sav2/y/9k5RG39IpDDgXqS7RSdSWQBLZv3QQsLgl2qO79OleSAsY5M9I2gVn4M5mfDy7eNXRwFME6Pl/C6cdTzZF/25Q9L3AzsvPZa8i6UQ=.

Masuda Y., *The Information Society as Post-industrial Society*, Tokyo 1981.

Niedzielska E., *Podstawowe pojęcia informatyki*, [w:] *Informatyka ekonomiczna*, red. E. Niedzielska, Wrocław 1998.

Nowina-Konopka M., *Istota i rozwój społeczeństwa informacyjnego,* [w:] *Społeczeństwo informacyjne. Istota, rozwój, wyzwania*, red. M. Witkowska, K. Cholawo-Sosnowska, Warszawa 2006.

Pawłowska A., *Zasoby informacyjne w administracji publicznej w Polsce. Problemy zarządzania,* Lublin 2002.

Próchnicka M., *Informacja a umysł*, Kraków 1991.

Seidler J., *Nauka o informacji*, Warszawa 1983.

Sienkiewicz P., *Ewaluacja informacji w społeczeństwie informacyjnym*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego – Ekonomiczne Problemy Usług" 2011, nr 67.

Sienkiewicz P., *Teorie rozwoju społeczeństwa informacyjnego,* [w:] *Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego. Dylematy cywilizacyjno-kulturowe*, red. L.H. Haber, Kraków 2002.

Słownik terminologiczny informacji naukowej, red. M. Dembowska i in., Wrocław-Warszawa 1979.

Sobielga J., *Psychologiczne aspekty barier informacyjnych – badania wśród studentów*, „Praktyka i Teoria Informacji Naukowej i Technicznej" 1997, nr 4.

Soldecka N., *8 najciekawszych sztucznych języków*, https://menway.interia.pl/ obyczaje/nauka/news-8-najciekawszych-sztucznych-jezykow,nId,451587#utm_source=paste&utm_medium=paste&utm_campaign=chrome.

Świgoń M., *Bariery informacyjne,* [w:] *Nauka o informacji*, red. W. Babik, Warszawa 2016.

Świgoń M., *Bariery informacyjne w środowisku naukowym*. *Badania pilotażowe*, „Przegląd Biblioteczny" 2003, z. 4.

Tworak Z., *W stronę jednolitej teorii informacji. Propozycja Marka Burgina*, „Studia Metodologiczne" 2015, nr 35 (4).

Uniwersalny słownik języka polskiego, red. S. Dubisz, Warszawa 2003, t 1.

Woźniak O., *Skąd się wzięły języki i po co nam ich tyle*, „Gazeta Wyborcza" z 2 maja 2018 r., https://wyborcza.pl/7,75400,23344459,skad-sie-wziely-jezyki.html.

Zybert E.B., *Bariery w dostępie do książki i biblioteki w środowisku niedostosowanych społecznie.* „Poradnik Bibliotekarza" 1992, nr 7/8.

Information barriers as a factor shaping contemporary information security

Summary: The study presents a reflection on the nature and classification of information barriers. The analysis is conducted in the context of the relationship between information barriers and information security. On the broad theoretical background, including the characterization of the essence of information, comprehension and features of the information society, the increasing importance of information security has been pointed out. The section that follows reviews definitions related to the understanding of the term 'information barrier'. The next fragment of the analysis concerns the classification of information barriers present in the literature and ends with the presentation of the author's version. The summary postulates the need to intensify research on information barriers in the field of security sciences. Including these barriers in the scope of securitology's interest is associated with the need to ensure an adequate level of information security based on the freedom of access and exchange of high quality information. An important argument in favor of such research is the fact that information security is also built on the basis of the interactions between humans and information, as well as on information relations between people, which in the event of information barriers can be deeply disturbed.
Keywords: *information, information security, information barriers, information society*

ROBERT ZAPART
ORCID: 0000-0002-3590-1189
Uniwersytet Rzeszowski, Kolegium Nauk Społecznych

Perspektywa politycznego wykorzystywania informacji niejawnych w komunikowaniu publicznym

Realizacja konstytucyjnego prawa obywateli do uzyskiwania informacji o działalności organów państwa, szczególnie w sferze jego bezpieczeństwa, nastręcza wiele problemów będących następstwem obowiązywania ustawy o ochronie informacji niejawnych. Narzucone jej zapisami ograniczenia jawności w sferze publicznej stwarzają ryzyko jej instrumentalnego wykorzystania przez elity rządzące w celach służących ich partykularnym interesom politycznym. Tymczasem oczekiwania obywateli w tym zakresie są zgoła odmienne. Liczą oni bowiem na to, że ich reprezentanci będą bardziej rygorystycznie od innych grup zawodowych przestrzegać wysokich standardów etycznych i moralnych. Ich sojusznikiem w tych opiniach pozostają wolne i nieskrępowanie działające media, które w ramach swojej misji demaskują nadużycia władz, ograniczają ich poczucie bezkarności oraz kształtują społeczny osąd w tym zakresie. Wspierając funkcje obywatelskiej kontroli, narażają się na nieustannie trwający konflikt z elitami rządzącymi. Te ostanie natomiast, zabiegając o pozytywną dla siebie w przyszłości decyzję obywateli pozwalającą im utrzymać polityczne przywództwo, wykorzystują wszelkie dostępne środki zwrotnego oddziaływania, które wyeliminują lub ograniczą negatywne następstwa zewnętrznego przekazu. Wśród nich znajdują się jednostronne komunikaty kierowane do społeczeństwa oraz realizowana na gruncie jawnym i niejawnym wobec mediów – nadmiernie próbujących ingerować w chronione przez państwo aktywa – praca operacyjna i procedura procesowa.

Zarówno pierwsze, jak i drugie kierunki działania wykorzystywane w sposób nieuzasadniony i nieuprawniony podważają fundamenty demokratycznego państwa prawa, w tym – ograniczają podmiotowość obywateli z perspektywy możliwości wyrażania przez nich obiektywnych ocen i opinii o poczynaniach władzy na bazie dostępu do wolnych od ich ingerencji, alternatywnych źródeł informacji. Czy zatem istnieje ryzyko wykorzystania w komunikacji państwo – obywatel pojęć przypisanych ochronie informacji niejawnych do nadmiernego ograniczania jawności życia publicznego, a tym samym uznaniowego limitowania suwerenowi przez jego reprezentantów obiektywnej wiedzy o państwie? Będzie to przedmiotem poniższych analiz wykorzystujących wybrane metody naukowe, w szczególności – porównawczą, systemową oraz w mniejszym stopniu instytucjonalno-prawną. Towarzyszyć im będzie teza o konieczności zwiększenia profesjonalizmu mediów podejmujących tematykę bezpieczeństwa wspólnoty, co powinno ograniczyć wskazane ryzyko wykorzystywania przez elity rządzące posiadanej obecnie merytoryczno-prawnej przewagi, a w następstwie zadbać o właściwie ustanowione granice jawności i przyczynić się do zwiększenia pożądanej świadomości obywatelskiej w tym zakresie.

W dostępnej literaturze przedmiotu trudno doszukać się prac bezpośrednio nawiązujących do tytułowego zagadnienia, zatem poniższe rozważania stanowią w zamyśle autora wstęp do pogłębionych w przyszłości badań naukowych na temat wykorzystywania przez władze w komunikowaniu publicznym przewagi wiedzy i prawa wynikających z ustawowego obowiązku dbania o państwo i jego bezpieczeństwo.

Jawność i ograniczenia informacji z perspektywy bezpieczeństwa demokratycznego państwa prawa

W demokratycznym państwie prawnym limitowanie obywatelom dostępu do informacji o jego działaniach ma stopniowalny charakter i dokonuje się na kilku poziomach: pełnym i bezwarunkowym, pełnym i warunkowym, niepełnym i bezwarunkowym, niepełnym i warunkowym oraz brakiem takowego[1]. Podstawową zasadą pozostaje jawność jako, jak utrzymuje Zbigniew Cieślak,

[1] Z. Cieślak, *Aksjologiczne podstawy jawności. Perspektywa nauk o administracji*, [w:] *Jawność i jej ograniczenia*, red. G. Szpor, t. II, *Podstawy aksjologiczne*, red. Z. Cieślak, Warszawa 2013, s. 9.

„element funkcji koniecznych układów administracyjnych, a więc stanów rzeczy opisanych skutkami zachowań ludzi motywowanych oddziaływaniem norm prawnych, regulujących dostęp do informacji, które warunkują procesy realizacji wyróżnionych przez ustawodawcę wartości”[2]. Jej ograniczenie może być wynikiem fundamentalnych potrzeb wspólnoty odwołujących się do jej własnego bezpieczeństwa oraz stabilnej i pokojowej egzystencji, które utożsamiamy z racją stanu[3]. Nadrzędność tej ostatniej nad partykularyzmami grup i jednostek oznacza ochronę podstawowych wartości tworzących fundament państwa. Nie mogą być zatem dostępne powszechnie informacje dotyczące metod ich ochrony w przypadku części, podejmowanych przez władze w sytuacji zagrożenia, decyzji. Dopuszczalność powyższego uzasadnienia warunkuje rzeczywistość istnienia jego odpowiedniego poziomu, co wiąże się też z koniecznością adekwatności wprowadzanych ograniczeń jawności i uzasadnionym czasowym przesuwaniem przez państwo granic ochrony informacji. W innym przypadku będziemy mieć do czynienia z nieuprawnionym okolicznościami zawłaszczaniem przestrzeni przynależnej obywatelom. Musimy jednak zauważyć, że będzie to zawsze pole do sporów bazujących na konflikcie dwóch wartości – praw jednostki i praw wspólnoty. Ważne jest zatem, aby ograniczenia jawności następowały wyłącznie w następstwie pojawienia się określonych przesłanek bezpośrednio powiązanych ze zmianą stanu bezpieczeństwa publicznego i poczucia zagrożenia wśród obywateli[4]. Przy ich niskim zaufaniu do rządzących odpowiednią gwarancję stanowią normy prawa międzynarodowego oraz zapisy Konstytucji RP dopuszczające zmiany wyłącznie w drodze ustawy[5].

Z perspektywy ustawy o ochronie informacji niejawnych (dalej u.o.i.n.) spotykamy się generalnie z dwoma poziomami praktycznego odzwierciedlenia zasady jawności, a mianowicie: z brakiem dostępu do informacji oraz z jej niepełną

[2] Tamże.

[3] A. Dylus, *Aksjologiczne podstawy jawności i jej ograniczenia. Perspektywa etyki politycznej*, [w:] tamże, s. 48. Szerzej o racji stanu w: A. Rzegocki, *Racja stanu a polska tradycja myślenia o polityce*, Kraków 2008.

[4] R. Zapart, *Polityka a ochrona informacji niejawnych. W poszukiwaniu nadrzędnych wartości w państwie w obliczu zewnętrznego zagrożenia*, [w:] *Informacje prawnie chronione – wybrane zagadnienia*, red. S. Topolewski, Siedlce 2019, s. 194-195.

[5] Art. 61 Konstytucji Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 z późn. zm.).

i warunkowaną formą. W przypadku tego pierwszego – obywatel niespełniający określonych w u.o.i.n. kryteriów nie może zapoznać się z chronionymi zasobami wiedzy, nawet jeżeli powoła się na uzasadniony interes publiczny[6]. W drugim przypadku – dostęp obywatelom do informacji niejawnych umożliwia uchylająca decyzja osób uprawnionych (art. 6 u.o.i.n.), które weryfikują ustanie pierwotnych przesłanek ochrony. Nie dotyczy to jednak tych wyłączonych bezterminowo[7]. Ujawnienie umożliwiające powszechne upublicznienie może nastąpić w nieprzewidywalnym okresie obejmującym także przeprowadzany, nie rzadziej niż raz na 5 lat, wewnętrzny przegląd materiałów niejawnych w celu weryfikacji faktycznego zaistnienia takiej sytuacji. Podejmowane w tym zakresie decyzje mogą obejmować nie tylko postulowane przez zainteresowanych obywateli, w tym w szczególności przez cenzurujące poczynania władz media, całkowite, ale też tylko częściowe, zniesienie klauzul ochrony informacji oraz wykluczającą odmowę, obniżenie poziomu ochrony lub częściowe odtajnienie[8]. Jest to wynikiem całościowej analizy, w tym szacowania ryzyka wystąpienia ewentualnych następstw określonych interpretacji, która w następstwie nacisków politycznych może nieść ze sobą ryzyko nieuzasadnionego obiektywnymi przyczynami odwlekania lub odmowy ujawnienia informacji. Nadmierny obszar arbitralności organów państwa w tym zakresie, wsparty problematyczną zaskarżalnością podejmowanych przez nie negatywnych decyzji, stanowi potencjalne pole do nadużyć i stanowi dla nich zachętę do ograniczenia transparentności życia publicznego, pozostawiając obywatelom wyłącznie etyczno-moralną ocenę tych działań. Motywowana partykularnymi interesami metoda komunikowania się ze społeczeństwem może być w związku z nieuzasadnionym przekraczaniem przez rządzących granic jawności, utożsamiana z planowym antydialogiem, propagandą i dezinformacją, realizowanymi w celach niekoniecznie związanych z racją stanu, ale dla doraźnych celów politycznych.

[6] Art. 4 ust. 1. Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2018 r., poz. 412 z późn. zm.).
[7] Art. 7. us. 1. u.o.i.n.
[8] Art. 6. u.o.i.n.

Komunikowanie jako metoda realizacji celów i interesów politycznych

Komunikowanie jest procesem składającym się z wytworów sekwencyjnej aktywności biorących w niej udział stron. W przypadku jego politycznego czy też publicznego kategoryzowania mówimy o systemie wytwarzającym specyficzne relacje i sieci interakcji pomiędzy obywatelami, mediami i aktorami promującymi określone idee. Jego cechą charakterystyczną jest ułomna pozycja najliczniejszej, ale jednocześnie w największym stopniu zaniedbywanej, grupy złożonej z obywateli. Najsłabiej zorganizowani i reprezentowani przegrywają konfrontację interesów z głównymi aktorami, politykami oraz mediami[9]. Kolejnym kotwiącym elementem systemu komunikowania są instytucje o charakterze publicznym realizujące określone przez normy prawne cele i zabezpieczające jednocześnie służebność zarówno wobec jednostek, jak i pozostałych członków zmagań o prawdę. Kluczem do rozróżnienia w systemie komunikowania publicznego i politycznego są składające się na nie podmioty i wiążące ich relacje. Część z nich ma podwójną rolę, co pociąga za sobą problemy definicyjne, a jeszcze inne, pomimo że zaliczane do podległych administracji rządowej instytucji spełniających usługi publiczne, mogą być absorbowane w przestrzeń bieżącej polityki z uwagi na swoją pozycję, kompetencje i bliskie personalne związki ich kierownictw ze sprawującymi władzę. W przypadku komunikowania politycznego mamy do czynienia z intencjonalnym przekazem ukierunkowanym nie na zwrotną i braną pod uwagę odpowiedź, ale na realizację określonego interesu. Wykorzystuje się dla jego osiągnięcia public relations, propagandę, reklamę lub inne użyteczne środki perswazji, wykorzystując niejednokrotnie w tym celu media[10].

W teoriach komunikacji przyjmuje się, że powyższy proces przebiega wielowymiarowo, a informację końcową kształtują różne elementy zaangażowane w nadawanie i odbiór przekazów. Wśród ogólnych przesłanek skuteczności znajdują się najczęściej eksponowane odpowiednio zasady: prawdziwości, zrozumiałości, masowości, długotrwałości, specjalizacji, informacji pożądanej, emocjonalnego pobudzenia, rzekomej oczywistości czy też stopniowalności. Towarzyszą im funkcje, informacyjno-interpretacyjna (przekaz perswazyjny) i dezinformacyjna

[9] B. Dobek-Ostrowska, *Komunikowanie polityczne i publiczne*, Warszawa 2007, s. 120.

[10] J. Garlicki, *Komunikowanie polityczne – od kampanii wyborczej do kampanii permanentnej*, „Studia Politologiczne" 2010, t. 16, s. 26-28.

(upowszechnianie nieprawdziwych informacji), a także formy zarządcze związane z identyfikacją problemów i ustaleniem dróg wyjścia z kryzysu[11]. W praktyce mamy zatem do czynienia:

1) ze strukturową organizacją komunikatu polegającą na celowym ukrywaniu przez tendencyjnego nadawcę obiektywnej informacji;
2) z sekwencyjnym preparowaniem przekazu od pojedynczej prawdy do ogólnej nieprawdy;
3) z tworzeniem mitów związanych z długotrwałym powtarzaniem określonych stanowisk do czasu ich publicznego utrwalenia;
4) z budowaniem wersji wyprzedzającej, w której pierwsza podana informacja ma większą – od sprostowań i uzupełnień – siłę wpływu;
5) z emocjonalnymi podpowiedziami powiązanymi z powoływaniem się na rację stanu i bezpieczeństwo państwa wpływającymi na świadomość lub podświadomość odbiorców za pośrednictwem werbalnych i niewerbalnych środków;
6) z wykorzystywaniem formalno-prawnej przewagi związanej z dostępem do wiedzy;
7) z prewencyjnym i arbitralnym sterowaniem uprzedzaniami do innych osób lub podmiotów;
8) z celowym dezorientowaniem odbiorców przekazu w postaci powielania związanych z własnymi potrzebami odpowiednio skonstruowanych opinii przez odpowiednio dobrane autorytety;
9) z ignorowaniem materialnej prawdy i zafałszowywaniem rzeczywistego przebiegu wydarzeń lub zjawisk[12].

Sformalizowana i scentralizowana transmisja komunikatów odbywa się wertykalnie z góry na dół, a zatem od elit rządzących do obywateli, za pośrednictwem wszystkich kanałów komunikowania (na przykład w formie wystąpień publicznych, oświadczeń, opracowań specjalistycznych), przy wykorzystaniu

[11] B. Dobek-Ostrowska, dz. cyt., s. 208-209; *Leksykon politologii*, red. A. Antoszewski, R. Herbut, Warszawa 2004, s. 351; J. Kossecki, *Cybernetyka społeczna*, Warszawa 1981, s. 434-445.

[12] M. Karwat, *Teoria prowokacji. Analiza politologiczna*, Warszawa 2007, s. 48-65; R. Borecki, *Propaganda a polityka (zarys problematyki funkcjonowania środków masowego przekazu w systemach społeczno-politycznych)*, Warszawa 1987, s. 117-139; B. Dobek-Ostrowska, dz. cyt., s. 207; M. Pabijańska, *Psychomanipulacje w polityce: metody, techniki, przykłady*, Kraków 2007.

dostępnych technik marketingowych i perswazyjnych[13]. Przewaga rządzących i ich medialne doświadczenie z publicznych spotkań face to face pozwalają im na kontrolowanie zakresu treści emitowanych wystąpień w przypadku mniej merytorycznie przygotowanych odbiorców, co zwrotnie ogranicza ryzyko konfrontacji, sprzyjając forsowaniu nieobiektywnego przekazu. W przypadku nagłego kryzysu spowodowanego wścibskością mediów mogą szybko zmodyfikować formę komunikowania, sprowadzając lansowaną wiedzę do ogólników lub ograniczyć się do nic nieznaczących banałów, dzięki czemu chronią reprezentowany podmiot i własną karierę. Pewnym problemem jest mierzenie się z merytorycznie przygotowanymi i dociekającymi odbiorcami, którymi najczęściej są dziennikarze. W następstwie rozterki lub emocji może to doprowadzić przedstawicieli rządzących do nieplanowanego ujawnienia chronionej przepisami u.o.i.n. lub bieżącymi potrzebami wiedzy, z powołaniem się na przykład na bezpieczeństwo państwa. Skutkować to będzie koniecznością podjęcia kolejnych działań, niejednokrotnie przy wsparciu specjalistów minimalizujących powstałe straty wizerunkowe i systemowe. Mogą zatem zostać zastosowane podważające pierwotne informacje kontrolowane przecieki, zaaranżowane skandale czy też inne reaktywne użyteczne techniki wywołujące pożądane skutki i pozwalające odbudować pozycję nadawcy. Wymaga to wykorzystania masowych kanałów komunikowania się z otoczeniem, których częścią pozostają pośredniczące w tych relacjach różnego rodzaju media, narażone na problemy z oceną wiarygodności przekazu, a czasami sprowadzone do marketingowego narzędzia. Stąd – dyskusyjna pozostaje teza o ich informacyjno-służebnej roli profesjonalnego recenzenta władzy we współczesnych demokracjach, w szczególności, gdy mamy do czynienia z prawną i organizacyjną przewagą tej ostatniej. Pozostające w permanentnej kampanii wyborczej elity rządzące, jak uważa Jan Garlicki, korygują wyłącznie intensywność komunikowania politycznego, któremu w nadmierny sposób nie przeszkadzają nawet nowe nośniki elektronicznego przekazu[14]. Wykorzystywanie przez nie uprzywilejowanej pozycji i pozbawianie partnerskiego charakteru tych relacji, szczególnie w przypadku publicznej dyskusji o systemie bezpieczeństwa państwa, uprzedmiotawia i ubezwłasnowolnia media, a w następstwie dodatkowo wpływa destrukcyjnie na społeczeństwo i jego świadomość praw i obowiązków.

[13] M. Kolczyński, *Strategie komunikowania politycznego*, Katowice 2008, s. 22.
[14] J. Garlicki, dz. cyt., s. 43.

Informacje niejawne w bieżącym przekazie publicznym

We wzorcowym modelu komunikowania publicznego pomiędzy podmiotami politycznymi a obywatelami, w którym pośredniczą media dysponujące pełnią podmiotowych możliwości profesjonalnej analizy i oceny podejmowanych przez strony działań, można monitorować zarówno sekwencyjność, jak i systematykę wzajemnych relacji, sygnalizując na wstępnym etapie zagrażające jawności odstępstwa od pierwotnych założeń. W przypadku informacji niejawnych powyższy wzorzec pozostaje nieosiągalny z uwagi na posiadaną przez państwo formalnoprawną przewagę w zakresie ich ochrony przed nieuzasadnionym ujawnieniem. W ślad za tym pojawia się u sprawujących władzę pokusa jej zdyskontowania w postaci jednostronnego, rozstrzygającego i służącego partykularnym interesom komunikowania. W opinii Sławomira Zalewskiego, polityczni aktorzy wykorzystują w publicznym spektaklu informacje niejawne do instrumentalnego wpływania na otoczenie, a związana z chronioną wiedzą tajemnica, nie tylko konstytuuje ten proces, ale również symbiotycznie wpływa na społeczne postrzeganie oponentów, kategoryzując ich jako wymagających eliminacji ze sceny przeciwników[15]. Możemy mieć zatem do czynienia z praktycznym wykorzystaniem tajemnic związanych z bezpieczeństwem państwa w politycznych sporach, których częścią są zarówno kreacja pożądanego przez władze pozytywnego wizerunku jedynych odpowiedzialnie zatroskanych bezpieczeństwem, jak i planowa kompromitacja osób oraz instytucji o odmiennych poglądach, na bazie ujawnianych nieznanych wcześniej faktów oraz powiązań, z nadaniem im określonego sensu i wydźwięku. W ślad za tym pojawić się powinny profesjonalnie przygotowane komunikaty, których rozpoznanie i zrozumienie będzie nastręczać, z uwagi na materię informacji niejawnych, wiele problemów obywatelom nieprzygotowanym do ich dekodowania. Będzie to wskazywać na stosowanie przez rządzących mechanizmów chroniących ich domenę odpowiedzialności przed kolizyjną, z perspektywy ich interesów, jawnością. Przezwyciężać promowane formy komunikowania, odsłaniając kulisy nadużyć z obszaru ochrony informacji niejawnych, mogą profesjonalnie przygotowane media, pod warunkiem umożliwienia im nieskrępowania nadmiernością przepisów aktywności. Cenzurując poczynania władzy i demaskując fałszywość narracji, promują odpowiedzialność społeczną, pożądane systemy

[15] S. Zalewski, *Bezpieczeństwo polityczne. Zarys problematyki*, Siedlce 2013, s. 209.

wartości, wytwarzają reakcje na bodźce oraz przekazywane dziedzictwo[16]. Wystarczy przywołać – w kontekście powyższych uwag – światowe następstwa Snowdengate, które nie dotyczyły wyłącznie relacji pomiędzy sojusznikami Paktu Północnoatlantyckiego, ale też – forsowanego przez Unię Europejską z perspektywy ochrony informacji o obywatelach „prawa do bycia zapomnianym"[17]. W tym przypadku demaskatorską funkcję czwartej władzy, eliminującej uprzywilejowanie elit rządzących, pełnił jeden z nielegalnie zasilonych dokumentami amerykańskiej administracji portali internetowych, który, poddając w wątpliwość skuteczność obywatelskiej kontroli nad rządzącymi, wskazał jednocześnie na nieprawidłowości w systemie bezpieczeństwa ochrony informacji. Nie rozstrzygając kwestii, czy powyższe działanie było następstwem braku akceptacji przez przekazującą mediom materiały chronione jednostkę wątpliwych prawnie i etycznie działań organów państwa, czy też wiązało się z dodatkową aktywnością czynników zewnętrznych zainteresowanych destabilizacją pozycji Stanów Zjednoczonych w stosunkach międzynarodowych, zauważamy, że upublicznienie nastąpiło w wyniku nieskuteczności zabezpieczeń w systemie, co świadczy o niskim poziomie mediatyzacji tej zdominowanej przez służby państwa sfery jego aktywności. Polskie doświadczenia wskazują na pozytywny wpływ mediów na próby nadmiernego ograniczenia jawności w związku ze zmianami ustawodawstwa o ochronie informacji niejawnych. Uczestnicząc w procesie legislacyjnym, wskazały one na zbyt daleko idące uszczuplenia w tym zakresie uniemożliwiające otrzymanie przez obywateli za ich pośrednictwem obiektywnej wiedzy na temat aktywności podmiotów publicznych[18]. Nie wszystkie postulaty zostały uwzględnione w kolejnych nowelizacjach, a praktyka pokazała istnienie obszarów niedomówień lub niejasności pozwalających na ich praktyczne zastosowanie w jednostronnym komunikowaniu. Wykorzystuje się w nim najczęściej formalno-prawną przewagę wynikającą z powierzonego organom państwa obowiązku ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, ze świadomością nieistnienia realnie szybkich

[16] B. Dobek-Ostrowska, dz. cyt., s. 33.

[17] M. Grzelak, *Skutki sprawy Edwarda Snowdena dla prywatności danych w cyberprzestrzeni*, „Bezpieczeństwo Narodowe" 2015, nr 33, s. 191-211.

[18] Ł. Kister, *Ustawa o ochronie informacji niejawnych w opiniach dziennikarzy*, [w:] *X lat ustawy o ochronie informacji niejawnych 1999-2009: materiały konferencyjne*, red. M. Gajos, Katowice 2009, s. 73-84.

możliwości weryfikacji tego faktu przez osoby zainteresowane niewygodną dla nich wiedzą. Może ona obejmować przekaz perswazyjny, w którym wskazuje się na brak możliwości udzielenia odpowiedzi na wniosek z jednoczesnym powołaniem się na obowiązujące klauzule niejawności. Może to skutkować u potencjalnie zainteresowanych porzuceniem tematu z uwagi na nieprzewidywalny czas oczekiwania na zmianę stanowiska organów państwa i – w konsekwencji – porzuceniem woli upublicznienia informacji. Obowiązujące przepisy wskazują na możliwość odtajnienia materiałów w przypadku ustania przesłanek ich ochrony, a zatem zniesienia klauzul na wniosek lub w następstwie cyklicznego (5 lat) przeglądu[19]. Warunkiem przyszłego medialnego sukcesu jest zatem oczekiwanie monitorujące przesłanki ochrony.

Skutecznym przekazem perswazyjnym organów państwa może być również brak odpowiedzi na trudne pytania związane z, chronionymi lub nie, informacjami. Brak cierpliwości zainteresowanych w tym zakresie przynosi faktyczną stratę dla jawności, a w odwrotnych przypadkach – może na nią pozytywnie wpływać, ograniczając zamiary nadużyć, pomimo oczywistej zwłoki związanej z koniecznością zrealizowania wspomnianych wcześniej procedur. Jest wobec tego formą proobywatelskiej aktywności, o którą z pewnością należy zabiegać, pomimo świadomości, że powtórzenie zagadnienia już niekoniecznie może wzbudzić zainteresowanie odbiorców. Należy pamiętać, że i w tej sytuacji mogą wystąpić odstępstwa od reguły. Zainteresowanie społeczeństwa, które wsłuchuje się w pełny opis wcześniej niepełnego komunikatu i wyciąga w stosunku do rządzących odpowiednie wnioski, świadczyć będzie zarówno o poziomie jego obywatelskiej dojrzałości, jak i wpłynie na nich hamująco z powodu świadomości nieuniknionych w przyszłości rozliczeń.

Interesująco przedstawia się również komunikowanie polityczne w przypadku nieuprawnionego ujawnienia chronionych klauzulami informacji w odniesieniu do mediów. Jedną z zastosowanych metod jest dyskredytowanie upubliczniających je dziennikarzy oraz wspierających ich źródeł, kierowanie wobec nich gróźb pociągnięcia do odpowiedzialności karnej lub zawiadomień w tym zakresie, kreowanie mrożącego efektu posiadanej nad jednostkami przewagi itp.

[19] Art. 6. ust. 2-8 u.o.i.n. Zmiana statusu materiałów niejawnych nie obejmuje wyłączeń wskazanych w art. 7. ust. 1 tej ustawy.

W annałach historii polskiego sądownictwa zapisał się trwający od 1996 r. przez kolejnych 12 lat proces przeciwko jednemu z dziennikarzy, który został oskarżony w latach 90. z zawiadomienia ówczesnego Urzędu Ochrony Państwa, o ujawnienie tajemnicy państwowej polegającej na podaniu do publicznej wiadomości personaliów operacyjnych (zatem i tak fałszywych) funkcjonariusza uczestniczącego w jednej z głośnych ówcześnie spraw dotyczących znanego powszechnie polityka. Komentujący po latach wydarzenia obrońca obwinionego stwierdził z sarkazmem: „służby kochają tajemnice. Każdy, kto się zbliża do granic, dotyka tajemnicy, automatycznie staje się czynnie pobudzającym służby do kontrposunięć”[20]. Powyższy komunikat znającego kulisy sprawy prawnika wskazuje na zastosowaną przez organy państwa metodologię zarządzania kryzysem, wywołanym ujawnieniem chronionych informacji, który może być inspiracją dla każdej elity rządzącej. Zasada zastraszania, nawet potencjalnymi oskarżeniami o szpiegostwo, połączona z przewlekaniem działań operacyjnych i postępowania procesowego może „zmęczeniowo” wpływać na jednostkę w starciu z profesjonalnie przygotowanym i zarządzanym przez polityków aparatem państwa, a tym samym skutecznie zniechęcać ewentualnych następców do podjęcia podobnych kroków. Zaburza to tym samym aktywność mediów i iluzorycznymi czyni ich starania o zachowanie jasnych granic jawności. Jedynym wzmacniającym w stosunku do nich rozwiązaniem jest prawna ochrona źródeł informacji, która utrudnia, ale nie uniemożliwia, ich ustalenie[21].

Stosunkowo łatwo można również manipulować procesem poznawczym odbiorcy, świadomie wykorzystując jego niewiedzę w odniesieniu do obowiązującego stanu prawnego. Najczęściej spotyka się niekorygowanie przez przedstawicieli władz w publicznych odpowiedziach nieobecnego od nowelizacji u.o.i.n. w 2010 r. pojęcia tajemnicy państwowej. Z uwagi na brak precyzji zadających pytanie, trudno mówić o formalnych następstwach wykorzystywania przewagi wiedzy. Z perspektywy komunikowania nie ponosi się zatem ryzyka związanego z następstwami mówienia nieprawdy, a tym samym intensywnego przeciwdziałania w przypadku ujawnienia niewygodnych dla sprawujących władzę informacji.

[20] *Najdłuższy proces o ujawnienie tajemnicy państwowej*, https://www.polskieradio24.pl/130/5561/Artykul/1703537,Najdluzszy-proces-o-ujawnienie-tajemnicy-panstwowej [dostęp 13.04.2019].
[21] Art. 85 u.o.i.n. zmieniający zapis Ustawy z dnia 26 stycznia 1984 r. Prawo prasowe (Dz.U. z 1984 r. Nr 5, poz. 24 z późn. zm.).

Nieco odmiennie przebiega proces zarządzania kryzysem w przypadku popełnionych błędów. Przyjmując określone założenia związane z niejawnością i niedostępnością części źródeł, można spróbować wskazać na wyprzedzające ostateczne rozstrzygnięcia prawne komunikaty ze strony zarządzanych przez polityków organów państwa o utracie przez: byłego szefa CBA Pawła Wojtunika oraz dyrektora Departamentu Zwierzchnictwa nad Siłami Zbrojnymi BBN, doradcę prezydenta RP Andrzeja Dudy gen. Jarosława Kraszewskiego, rękojmi do pracy z materiałami niejawnymi. W jednostronnym komunikowaniu można doszukać się przywoływanych wcześniej, a tworzonych na użytek szerokiego kręgu odbiorców, dyskredytujących ich pozycję zawodową opinii, opiniotwórczych wystąpień z przywoływaną uwagą o niemożliwości ujawnienia potwierdzających tezy źródeł itp. Informacje o porażce organów państwa w następstwie wyroku NSA w sprawie Wojtunika, ale przede wszystkim pokazu siły Pałacu Prezydenckiego w sporze o gen. Kraszewskiego, były lakoniczne lub pozbawione dodatkowych komentarzy. W tym drugim przypadku, chroniąc wizerunek polityczny formacji rządzącej, odwołano osoby odpowiedzialne za pierwotne decyzje podejmowane w tle ważniejszych i absorbujących społeczną uwagę wydarzeń[22].

Podsumowanie i wnioski

Powoływanie się na bezpieczeństwo państwa i wynikającą z tego tytułu konieczność ochrony informacji jest przystępnym i wykorzystywanym przez elity rządzące narzędziem komunikowania się z obywatelami. Warunkowe ograniczenia jawności życia publicznego nie mogą być jednak kojarzone ze stanowiącym pole do nadużyć makiawelicznym rozumieniem racji stanu, gdzie „cel uświęca środki", a politykę w okresie kryzysu pozbawia się elementarnej moralności, dobro państwa kładzie się na karb subiektywnej oceny przedstawicieli jego organów, podobnie jak długofalowe interesy wykraczające poza wymiar kadencji czy okresów wyborczych. Z jednej strony należy oczekiwać, że będzie się zwiększać interaktywność komunikowania stron i powstaną nowe możliwości samoorganizacji obywateli, a z drugiej – system stanie się prawdopodobnie bardziej podatny na profesjonalne działanie elit rządzących zmierzających do organizowania

[22] R. Zapart. *Niebezpieczeństwo politycznego wykorzystania ustawodawstwa o ochronie informacji niejawnych*, „Polityka i Społeczeństwo" 2019, nr 3 (17), s. 125-126.

i wzmacniania wyrazów poparcia dla ich interesów[23]. Eliminacji pojawiających się w tym obszarze obaw może służyć takie ograniczenie w dostępie do informacji o działaniach władz związanych z zabezpieczeniem wspólnotowego bezpieczeństwa, które będzie spełniać łącznie warunki pragmatyki i racjonalności, zostanie wyważone na płaszczyźnie normatywnej z perspektywy praw jednostki i praw wspólnoty, przygotowane w sposób jawny i przy powszechnej akceptacji oraz adekwatnie do występującego w danym okresie zagrożenia[24]. Wskazane podejście winno redukować ryzyko arbitralności działań elit politycznych i pozostawić, niedotkniętą skazą braku obywatelskiego zaufania do nich, przestrzeń do poprawy relacji i pożądanego w większym wymiarze – komunikowania publicznego. Powinny się w niej pojawić przynajmniej trzy kierunki działania. Pierwszy obejmowałby położenie silniejszego społecznego nacisku na etykę i moralność u elit rządzących, co w następstwie służyłoby wzmocnieniu dialogu i prawidłowych relacji pomiędzy stronami i zracjonalizowałoby działania państwa[25]. Drugi wskazywałby na wzmocnienie praktycznego zastosowania w podmiotach odpowiedzialnych za ochronę informacji niejawnych zasad „dobrej administracji", co oznacza prawo do ochrony przez administrację a nie przed nią[26]. Natomiast trzeci dotyczyłby wyposażenia mediów w skuteczniejsze narzędzia umożliwiające im spełnianie, przy zachowaniu pełnej odpowiedzialności za skutki przedstawianych publicznie ocen i opinii, służebnej roli wobec obywateli w kontekście nieustannego przypominania o konieczności sprawowania kontroli nad swoimi reprezentantami w strukturach władzy. Z perspektywy demokratycznego państwa prawa pożądanym byłoby łączenie wszystkich wskazanych kierunków. Trudno jednak być optymistą i pozytywnie prognozować w tym zakresie, bowiem elity rządzące, niezależnie od orientacji ideologicznej, niechętnie będą chciały zrezygnować z gwarantujących im przewagę komunikacyjną narzędzi wpływających na jawność życia publicznego.

[23] J. Garlicki, dz. cyt., s. 44.
[24] R. Zapart, *Polityka a ochrona...*, dz. cyt., s. 195.
[25] J. Czaputowicz, *Etyka w służbie publicznej*, [w:] *Etyka w służbie publicznej*, red. J. Czaputowicz, Warszawa 2013, s. 13.
[26] T. Lipowicz, *Prawo obywatela do dobrej administracji*, https://www.nik.gov.pl/plik/id,1555.pdf [dostęp 14.04.2019].

Bibliografia

Dobek-Ostrowska B., *Komunikowanie polityczne i publiczne*, Warszawa 2007.

Karwat M., *Teoria prowokacji. Analiza politologiczna*, Warszawa 2007.

Kolczyński M., *Strategie komunikowania politycznego*, Katowice 2008.

Kossecki J., *Cybernetyka społeczna*, Warszawa 1981.

Leksykon politologii, red. A. Antoszewski, R. Herbut, Warszawa 2004.

Pabijańska M., *Psychomanipulacje w polityce: metody, techniki, przykłady*, Kraków 2007.

Rzegocki A., *Racja stanu a polska tradycja myślenia o polityce*, Kraków 2008.

Zalewski S., *Bezpieczeństwo polityczne. Zarys problematyki*, Siedlce 2013.

Artykuły

Borecki R., *Propaganda a polityka (zarys problematyki funkcjonowania środków masowego przekazu w systemach społeczno-politycznych)*, Warszawa 1987.

Cieślak Z., *Aksjologiczne podstawy jawności. Perspektywa nauk o administracji*, [w:] *Jawność i jej ograniczenia*, red. G. Szpor, t. II, *Podstawy aksjologiczne*, red. Z. Cieślak, Warszawa 2013.

Czaputowicz J., *Etyka w służbie publicznej*, [w:] *Etyka w służbie publicznej*, red. J. Czaputowicz, Warszawa 2013.

Dylus A., *Aksjologiczne podstawy jawności i jej ograniczenia. Perspektywa etyki politycznej*, [w:] *Jawność i jej ograniczenia*, red. G. Szpor, t. II, *Podstawy aksjologiczne*, red. Z. Cieślak, Warszawa 2013.

Garlicki J., *Komunikowanie polityczne – od kampanii wyborczej do kampanii permanentnej*, „Studia Politologiczne" 2010, t. 16.

Grzelak M., *Skutki sprawy Edwarda Snowdena dla prywatności danych w cyberprzestrzeni*, „Bezpieczeństwo Narodowe" 2015, nr 33.

Kister Ł., *Ustawa o ochronie informacji niejawnych w opiniach dziennikarzy*, [w:] *X lat ustawy o ochronie informacji niejawnych 1999-2009: materiały konferencyjne*, red. M. Gajos, Katowice 2009.

Lipowicz T., *Prawo obywatela do dobrej administracji*, https://www.nik.gov.pl/plik/id,1555.pdf [dostęp 14.04.2019].

Najdłuższy proces o ujawnienie tajemnicy państwowej, https://www.polskieradio24.pl/130/5561/Artykul/1703537,Najdluzszy-proces-o-ujawnienie-tajemnicy-panstwowej [dostęp 13.04.2019].

Zapart R., *Niebezpieczeństwo politycznego wykorzystania ustawodawstwa o ochronie informacji niejawnych*, „Polityka i Społeczeństwo" 2019, nr 3(17).

Zapart R., *Polityka a ochrona informacji niejawnych. W poszukiwaniu nadrzędnych wartości w państwie w obliczu zewnętrznego zagrożenia*, [w:] *Informacje prawnie chronione – wybrane zagadnienia*, red. S. Topolewski, Siedlce 2019.

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 z późn. zm.).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2018 r., poz. 412 z późn. zm.).

Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe (Dz.U. z 1984 r. Nr 5, poz. 24 z późn. zm.).

The perspective of the political use of classified information in public communication

Summary: The exercise of the constitutional right of citizens to information about the activities of state authorities, particularly in the field of state security, presents many problems following from the applicability of the Act on the Protection of Classified Information. The limitations of openness in the public sphere imposed by this Act create the risk of its instrumental use by the ruling elites for the purposes of their particular political interests. In the light of the author's research, free media, being one of the allies of society, exposes abuse and, at the same time, supports society's control functions, shapes its proper judgment of reality and limits the effects of unilateral communication in politics. For the functioning of a democratic state of law, it would also be desirable to place greater emphasis on the ethical and moral sphere of activity of politicians and on the implementation of the principles of good administration in their subordinate institutions. However, it is difficult to be optimistic and offer positive forecasts in this respect since the ruling elites, regardless of their ideological orientation, will be unwilling to resign from the tools that give them communication advantage and affect the openness of the public life.
Keywords: *classified information, openness, communication, politics, power, media*

WALDEMAR KRZTOŃ
ORCID: 0000-0001-8292-4327
Politechnika Rzeszowska im. Ignacego Łukasiewicza
Wydział Zarządzania

Zarządzanie informacją – zarys problemu

Zarządzanie informacją dotyczy informacji utrwalonej w postaci zarówno tradycyjnej – papierowej, jak i elektronicznej. Zasoby informacyjne podlegają planowaniu, organizowaniu, kierowaniu oraz kontrolowaniu na każdym etapie istnienia. Rozumienie potrzeby zarządzania informacją nie jest dla wszystkich oczywiste. Często ogranicza się tylko do zasobów elektronicznych, ponieważ zazwyczaj pojęcie to kojarzone jest ze społeczeństwem informacyjnym. Współczesne społeczeństwo za pomocą najnowocześniejszych technologii teleinformatycznych wytwarza, przetwarza, gromadzi, przekazuje i odbiera ogromne ilości informacji. Dlatego też zarządzanie informacją musi być kompleksowym działaniem w obszarze kierowania każdą organizacją (urzędem, przedsiębiorstwem, organizacją społeczną lub gospodarczą).

Artykuł jest próbą zaprezentowania procesu zarządzania informacją w organizacji i pokazania istotnych elementów tego zagadnienia. W artykule ujęto zagadnienia zarzadzania informacją, uwzględniając zarówno tradycyjne, jak i teleinformatyczne systemy informacyjne.

Natura informacji

Informacja jest pojęciem ogólnym, uważanym za interdyscyplinarne. Liczni autorzy, zastanawiając się nad tym, czym jest informacja, przyjmują jej definicję w zależności od potrzeb danej dziedziny. Inni używają tego terminu bez definiowania, jako pojęcia pierwotnego i naturalnego – czegoś co zwyczajnie istnieje i jest zrozumiałe. Jeszcze inni określają informację poprzez jej naturę, cechy,

własności i spełniane funkcje. W literaturze przedmiotu można także zauważyć pojmowanie informacji jako terminu niedefiniowalnego, który należy rozumieć w sposób intuicyjny. Ze względu na wielopłaszczyznowy charakter informacji nie jest ona prosta do jednoznacznego określenia.

Wieloaspektowe podejście prezentują autorzy *Słownika języka polskiego PWN*, definiując informację w trzech ujęciach[1]:

1) jako to, co zostało napisane lub powiedziane o czymś lub o kimś oraz zakomunikowanie komuś czegoś;
2) jako dział informacyjny instytucji, urzędu;
3) jako dane będące przetwarzane przez komputer.

Słownik synonimów języka polskiego zawiera ponad dwieście wyrazów pokrewnych m.in.: doniesienie, komunikat, opis, przekaz, wiadomość, wieść, tekst, znak[2].

Informacja identyfikowana jest przeważnie w procesach myślowych, poznawczych, dlatego też funkcje kognitywne, tj. pamięć, uwaga, mowa, postrzeganie oraz wykonywanie obliczeń, myślenie abstrakcyjne, formułowanie sądów, są charakteryzowane w kategoriach przetwarzania informacji. Umożliwiają one odbieranie, analizowanie, gromadzenie, opracowywanie, przetwarzanie oraz pozyskiwanie informacji otrzymanych za pośrednictwem bodźców zewnętrznych.

Jerzy Kisielnicki uważa, że informacja jest wynikiem uporządkowania i przeanalizowania danych (surowe liczby i fakty). To taki rodzaj zasobów, który pozwala na zwiększenie naszej wiedzy o nas i otaczającym nas świecie[3]. Są to dane poddane filtrowaniu przez sito obiektywnych lub subiektywnych odniesień[4].

Z kolei według teorii Börje Langeforsa informacja tworzy się jedynie w ludzkim umyśle i jest procesem interpretowania danych, uwzględniającym wiedzę i czas. Wzór informacji Langeforsa nazywany infologicznym (subiektywnym) ma postać[5]:

[1] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/ [dostęp 14.01.2020].
[2] *Internetowy słownik synonimów języka polskiego*, https://synonim.net/synonim/informacja [dostęp 20.03.2020].
[3] J. Kisielnicki, *MIS – systemy informatyczne zarządzania*, Placet, Warszawa 2008, s. 19, 23.
[4] M. Dutko, M. Karciarz, *Informacja w Internecie*, PWN, Warszawa 2010, s. 64.
[5] B. Langefors, *Theoretical Analysis of Information Systems*, (4th ed.) Studentlitteratur, Lund, Sweden, uerbach Publishers, Philadelphia 1973, s. 247-250.

$$\mathbf{I = i(D, S, t)}$$

gdzie:
I – informacja, **i** – proces interpretacji, **D** – dane, **S** – przedwiedza, **t** – czas.

Przyjmując ten tok rozumowania, należy uznać, że informacja może mieć swoje źródło tylko w twórczym nadawcy, który samodzielnie myśli, posiada własną wolę i działa w określonym celu[6].

Interesujące badania pojęcia informacji przeprowadził Czesław Berman, rozważając cztery jej znaczenia: jako rzeczy, wielkości mierzalnej, potencjału oraz zmiany. Informacja w znaczeniu rzeczy jest produktem konkretnego procesu mającego źródło i odbiorcę (adresata), dlatego też może być poddawana różnym czynnościom, takim jak wytwarzanie, magazynowanie, przesyłanie, przetwarzanie, wymiana, kupno, sprzedaż itp. Znaczenie informacji jako wielkości mierzalnej spowodowane jest koniecznością ilościowego określenia wiadomości, niezbędnej w ocenie skuteczności procesu komunikacji. Wynika to z występujących sytuacji i kontekstów, w których przekazywana wiadomość ma za mało lub za dużo informacji. Znaczenie informacji jako potencjału łączy się z jej ilościowym aspektem i zdolnością do określonej zmiany stanu rzeczy, to jest „zmniejszania lub eliminacji niepewności odbiorcy w odniesieniu do rozważanych przez niego stanów, wybranych ze zbioru stanów możliwych". Z kolei znaczenie informacji w kształtowaniu postaw i zachowań wiąże się z komunikowaniem. Związek ten należy postrzegać jako szczególny przypadek informowania zorientowanego na wywołanie określonej zmiany. Informacja zmniejsza nieokreśloność oraz wpływa na zachowanie się systemu[7].

Informacja nie jest jednoznacznie sprecyzowana. Często postrzega się ją jako[8]:

1) zasób ekonomiczny – kiedy jest niezbędna do funkcjonowania i rozwoju każdej gospodarki, każdego państwa i społeczeństwa. Zasób ten stanowią wszelkie potencjalne zbiory informacji zgromadzone oraz przechowywane

[6] W. Januszko, *Społeczeństwo informacyjne – manipulacje, szanse, zagrożenia*, [w:] *Informatyka Q przyszłości*, Wyd. Nauk. WZ UW, Warszawa 2010, s. 255.
[7] C. Berman, *Informacja i aspekt komunikacji*, „Zagadnienia Naukoznawstwa" 1991, nr 3-4, s. 427--429.
[8] J. Oleński, *Ekonomika informacji*, PWE, Warszawa 2001, s. 246-284.

w miejscu i czasie przy zastosowaniu technologii, jak też organizacji umożliwiającej ich wykorzystanie przez podmioty ekonomiczne w gospodarce;

2) produkt – w przypadku, gdy występuje w formie wyrobów informacyjnych – wiadomości odwzorowanych za pomocą fizycznie wyodrębnionych zbiorów materialnych nośników informacji;
3) wyrób – jeżeli będzie to skończony zbiór informacji odwzorowanych w określonym języku na względnie trwałym nośniku;
4) usługę – kiedy informacja występuje jako usługa informacyjna;
5) towar – jeżeli jest przedmiotem transakcji na rynku, a więc w przypadku, gdy następuje przeniesienie prawa własności;
6) dobro konsumpcyjne – o tym, czy informacja jest dobrem konsumpcyjnym decyduje ostatecznie jej odbiorca. Ta postać dominuje w środowisku masowego przekazu.

Prowadzone badania nad istotą informacji pokazują, że informacja różni się od materii i energii, ale bez nich nie może istnieć w środowisku materialnym. Na ogół jest w jakiś sposób wyrażana: najczęściej za pomocą kodu dzieli się ją na mniejsze części nazywane wiadomościami lub komunikatami. Aby spełniała swoją funkcję, musi uzyskać postać materialną – nośnik, który można przesyłać, przekształcać, niszczyć, odtwarzać, powielać. Na tym polega utrwalanie informacji, czyli dokumentacja[9]. Dzięki stosowanym nośnikom w postaci zjawisk i przedmiotów materialnych, podlega przenoszeniu w przestrzeni i w czasie.

Bogdan Stefanowicz po analizie podstawowych własności informacji uważa, że[10]:

1) informacja jest pojęciem niematerialnym, a jej ujawnienie wymaga danych;
2) w ujęciu infologicznym można ją traktować jako relację;
3) istnieje niezależnie od subiektywnego odbioru, a więc jest obiektywna;
4) ma różne znaczenie dla różnych odbiorców;
5) jest odzwierciedleniem pewnej cechy obiektu lub wycinkowym jej opisem;
6) stanowi uproszczony model określonego wycinka rzeczywistości;
7) przejawia cechę synergii;

[9] W.K. Roman, *Podstawy zarządzania informacją*, Wyd. Nauk. UMK, Toruń 2012, s. 18.
[10] B. Stefanowicz, *Informacja*, OW SGH, Warszawa 2010, s. 32-37.

8) jest łączona przez odbiorców ze znanymi im innymi informacjami;
9) mimo że nie jest energią, podlega ilościowemu pomiarowi;
10) wykazuje się różnorodnością, wynikającą z odmienności rozpatrywanych obiektów, rozmaitości źródeł, subiektywizmu interpretacyjnego odbiorców;
11) polega na powielaniu i przenoszeniu w czasie i przestrzeni, a także przetwarzaniu, nie ulegając zniszczeniu, lecz najwyżej zniekształceniom i deformacjom;
12) jest zasobem niewyczerpalnym, co wynika z możliwości jej powielania, nieskończonej liczby obiektów i ich nieskończonej złożoności;
13) pozyskiwanie, przechowywanie, przesyłanie i udostępnianie informacji wymagają określonych kosztów;
14) rozkład informacji w otoczeniu jest nierównomierny, co wywołuje jej asymetrię, czyli niejednakową dostępność dla różnych odbiorców ze względu na źródła i koszty jej pozyskania, preferencje w ustalaniu faktów i inne czynniki.

Pojęcie zarządzania

Wyniki analizy literatury przedmiotu pokazują różne interpretacje terminu „zarządzanie". Funkcjonuje wiele definicji tego pojęcia często utożsamianego z pojęciem kierowanie. W polskiej literaturze naukowej oznaczają odmienne zjawiska, choć w praktyce stosuje się je zamiennie.

Należy podkreślić, że oba te pojęcia wywodzą się z terminu sterowanie, które oznacza „[...] oddziaływanie jednego systemu na drugi (sterującego na sterowany), zmierzające do uzyskania określonego zdarzenia [...]"[11]. Zadaniem sterowania jest stosowanie konkretnych mechanizmów, aby doprowadzić do zmiany jednego wyróżnionego stanu układu w inny wyróżniony, który bardziej odpowiada sterującemu. Jest wywieraniem pożądanego wpływu na określone zjawisko lub wywołaniem pożądanych zmian struktury układu.

Sterowanie, jako pojęcie, dotyczy zarówno człowieka, zwierzęcia, maszyny i systemu. Ma na celu spowodowanie zachowania się systemu w pożądany

[11] T. Pszczołowski, *Mała encyklopedia prakseologii i teorii organizacji*, Ossolineum, Wrocław 1978, s. 231.

sposób i wyeliminowania czynników, które to zachowanie zakłócają, poprzez oddziaływanie na ten system.

Rozważając problem w odniesieniu do ludzi i organizacji, stosując polską terminologię, wyróżnia się pojęcia „kierowanie" i „zarządzanie". Kierowanie „dotyczy w zasadzie ludzi", zaś zarządzanie „odnosi się do instytucji (organizacji)". Stąd też określenia „kierowanie zespołem ludzkim" i „zarządzanie przedsiębiorstwem (firmą, uczelnią)". Z drugiej strony wyniki badań literatury przedmiotu wskazują na częste zamienne używanie tych pojęć. Mówi się także o „zarządzaniu personelem" i „kierowaniu firmą"[12].

W praktyce dopuszczalne wydaje się zatem utożsamianie zarządzania z kierowaniem. Trzeba i należy, posługując się analizowanymi terminami, przyjmując ich polskie rozumienie, dążyć do stosowania pojęcia „kierowanie" w odniesieniu do zespołów ludzkich, zaś „zarządzanie" w stosunku do organizacji. Jednak w codziennym użytkowaniu ich rozróżnianie, teoretycznie możliwe do uzasadnienia, jest mało istotne[13]. Istota zarządzania tkwi w podejmowaniu decyzji i rozwiązywaniu problemów kierowniczych.

Funkcjonuje wiele definicji zarządzania, a uniwersalne rozumienie pojęcia zarządzanie nie jest zadaniem prostym. Spotyka się bowiem różne interpretacje tego terminu, np.:

1) proces zarządzania to ciąg działań będących funkcjami planowania, pobudzania, organizowania i kontroli, które uporządkowane są w określonych układach przebiegów organizacyjnych (zwykle w układach informacyjno-decyzyjnych) i spełniane są przez jednostki zarządzania oraz stanowiska kierownicze[14];
2) zarządzanie to proces planowania, nadawania mocy i oceniania starań (wysiłków) zespołów ludzkich dążących do osiągnięcia wspólnego celu[15];
3) zarzadzanie to zestaw działań (obejmujący planowanie i podejmowanie decyzji, organizowanie, przewodzenie) skierowanych na zasoby organizacji

[12] *Podstawy dowodzenia w aspekcie działań sieciocentrycznych*, red. J. Wołejszo, J. Kręcikij, Wyd. AON, Warszawa 2013, s. 38.
[13] Z. Ścibiorek, *Analiza możliwości wykorzystania ogólnej teorii kierowania podczas podejmowania decyzji do działań bojowych*, Wyd. AON, Warszawa 1999, s. 24.
[14] *Organizacja i zarządzanie*, red. A. Stabryła, J. Trzcieniecki, PWN, Warszawa 1986, s. 132.
[15] W.J. Stanton, M.J. Etzel, B.J. Walker, *Fundamentals of Marketing*, McGraw-Hill, New York 1994, s. 661.

(ludzkie, finansowe, rzeczowe oraz informacyjne) i wykonywanych z zamiarem osiągnięcia celów organizacji w sposób sprawczy i skuteczny[16].

Z przedstawionych definicji wynika istota zarządzania, którą są procesy informacyjno-decyzyjne przebiegające przede wszystkim w warstwie funkcjonalnej (planowanie, organizowanie, motywowanie i kontrolowanie) oraz w warstwie zasobowo-kapitałowej, przez którą rozumieć należy zasoby ludzkie, rzeczowe, finansowe, technologiczne i informacyjno-organizacyjne.

Zarządzanie to zespół działań decyzyjnych, proces wieloetapowy, obejmujący podejmowanie decyzji, które mają prowadzić do osiągnięcia celów. Zarządzanie jest procesem działania skutecznego, sprawnego, prowadzącego do wykonywania zadań przez organizację. Polega na koordynowaniu zespołowych i zbiorowych wysiłków ludzkich, a także wykorzystania zasobów organizacji oraz techniki, aby osiągnąć założony cel.

Do podstawowych narzędzi zarządzania należą[17]:

1) strategia;
2) struktura;
3) procedury organizacyjne;
4) kultura organizacyjna.

Strategia to proces tworzenia i realizacji długookresowego planu, uzyskiwanie określonej pozycji względem otoczenia, względnie trwały wzorzec działania. Strategia organizacji to zespół niesprzecznych, dostosowanych do potencjału oraz sytuacji w jej otoczeniu, sposobów działania umożliwiających osiąganie długookresowych celów organizacji[18]. Strategia w zarządzaniu obejmuje to wszystko, co ma umożliwić szansę zrealizowania zakładanych celów i dalszego funkcjonowania organizacji. Przeważnie są to: plany działania, zespół idei, pozycja organizacji w otoczeniu, wzorce działania, zbiory kryteriów i reguł decyzyjnych.

Struktura organizacyjna tworzy zbiór elementów organizacji wyrażony jako konkretny układ tych elementów i ich wzajemnych powiązań. Układ ten najczęściej jest schematem organizacyjnym. Określa on osoby realizujące poszczególne funkcje zarządzania i ich miejsce w organizacji jako całości[19]. Elementami

[16] R.W. Griffin, *Podstawy zarządzania organizacjami*, PWN, Warszawa 1996, s. 38.
[17] W.K. Roman, dz. cyt., s. 36.
[18] K. Obłój, *Strategia organizacji*, PWE, Warszawa 2001, s. 23.
[19] R.W. Griffin, dz. cyt., s. 330.

struktury organizacyjnej są: indywidualne stanowiska pracy, komórka organizacyjna, zespoły komórek organizacyjnych, pion organizacyjny, zakłady, oddziały.

Struktura organizacyjna określa niezbędne powiązania (więzi organizacyjne) między stanowiskami pracy a komórkami organizacyjnymi, dwustronne – między komórkami organizacyjnymi, między kierującymi a podwładnymi. Więzi organizacyjne uwidaczniają się poprzez przepływ informacji na określonych nośnikach[20]. Do najważniejszych rodzajów więzi organizacyjnych zalicza się więzi: służbowe, funkcjonalne, techniczne, informacyjne. Więzi informacyjne ustalają przepływ informacji, a wynikają z obowiązku jednostronnego lub wzajemnego przekazywania informacji w celu sprawnego wykonywania obowiązków, co warunkuje sprawność funkcjonowania organizacji.

Procedury organizacyjne obejmują określony, uzgodniony, ujednolicony, przyjęty według określonych standardów sposób realizacji działań i procesów w organizacji.

Kultura organizacyjna jest zasobem organizacji zawierającym normy i sposoby postepowania funkcjonujące wewnątrz organizacji. Kultura kształtuje porządek społeczny, buduje tożsamość grupową i wspólne zaangażowanie, wytwarza więzi, formuje morale pracowników, tworzy ich stan emocjonalny.

Zarządzanie zawsze związane jest z obiektem (czym zarządzać), celem (dlaczego zarządzać) oraz środkami i metodami (w jaki sposób i za pomocą czego zarządzać)[21]. Zarządzanie dotyczy też informacji, gdyż informacja jest jednym z zasobów (obiektem), bez którego organizacja funkcjonować nie może.

Istota zarządzania informacją

W dobie społeczeństwa informacyjnego, potrzebującego ogromnej ilości informacji, gromadzącego i wytwarzającego je, wystąpiła konieczność zarządzania informacją. Zarządzanie informacją jest konsekwencją potrzeby przechowywania zasobów informacji, ich przetwarzania oraz udostępniania. Z kolei celem jest ustalenie sytuacji wewnątrz i na zewnątrz organizacji oraz dostarczanie

[20] J. Zieleniewski, *Organizacja i zarządzanie*, PWN, Warszawa 1969, s. 33.

[21] B. Stefanowicz, *Informacyjne systemy zarządzania. Przewodnik*, OW SGH**,** Warszawa 2007, s. 29.

informacji zgodnych z potrzebami, które są niezbędne do podejmowania decyzji i rozwiązywania zaistniałych problemów.

Informacje posiadają indywidualną wartość i są podatne na zagrożenia, takie jak np. zniszczenie, kradzież czy wyciek. Istotnym zadaniem, wraz ze wzrostem znaczenia informacji, jest zapewnienie jej bezpieczeństwa. Coraz częściej występują zdarzenia związane z naruszeniem bezpieczeństwa informacji. Wraz ze wzrostem ilości przetwarzanych informacji i zastosowaniem coraz bardziej nowoczesnych technologii teleinformatycznych rośnie ryzyko ich utraty[22].

Zarządzanie zasobami informacyjnymi nie jest procesem prostym. Szybko rosnące zasoby informacyjne oraz lawinowy rozwój technologiczny i techniczny potrzebują ujednoliconego funkcjonowania i współdziałania wielu czynników. Współcześnie o konieczności zarządzania informacją decyduje postrzeganie jej jako pożądanego i uznanego produktu, który jest obiektem obrotu i transakcji oraz wzrostem roli informacji w życiu społeczeństwa, państwa, organizacji i obywatela (jednostki).

Argumentów dostarcza również sytuacja wewnątrz organizacji[23]:

1) wzrost różnorodności informacji i różnorodności procesów informacyjnych;
2) konieczność zapanowania nad ogromnymi ilościami informacji pochodzącymi z coraz to nowszych źródeł;
3) wzrastająca intensywność strumieni informacyjnych;
4) coraz szerszy zakres strumieni informacyjnych obligatoryjnie przesyłanych drogą elektroniczną.

Wymienia się trzy perspektywy zarządzania informacją[24]:

1) perspektywa organizacyjna – z organizacyjnego punktu widzenia zarządzanie informacją jest traktowane jako jeden z zasobów strategicznych, który musi być zarządzany tak, jak każdy inny zasób organizacji (np.

[22] W. Krztoń, *Informacja wyzwaniem dla bezpieczeństwa współczesnego świata*, [w:] *Informacje prawnie chronione – wybrane zagadnienia*, red. S. Topolewski, Wyd. Nauk. UPH, Siedlce 2019, s. 23.

[23] M. Mazur, *Koncepcje wartości i ich przydatność do pomiaru wartości na potrzeby zarządzania*, [w:] *Informacja w społeczeństwie XXI wieku*, red. A. Łapińska, Wyd. UWM**,** Olsztyn 2003, s. 176--177.

[24] B. Detlor, *Information managment*, "International Journal of Information Management", Volume: 30, Issue: 2, April, 2010, s. 103-104.

ludzie, sprzęt, kapitał). Oznacza kompleksowe podejście do planowania, organizowania, budżetowania, kierowania, monitoringu i kontrolowania ludzi, środków finansowych, technologii i działań związanych z pozyskiwaniem, przechowywaniem i dystrybucją danych niezbędnych do spełnienia potrzeb biznesowych na rzecz przedsiębiorstwa. Powiązane z zarządzaniem systemami i technologiami informatycznymi, zarządzaniem danymi, zarządzaniem treścią. Zarządzanie informacją obejmuje zarządzanie informacjami uporządkowanymi i sformalizowanymi (tj. dane starannie zawarte w bazie danych lub hurtowni danych), jak i nieuporządkowanymi (rodzaj informacji, które można znaleźć w raportach, dokumentach, wiadomościach e-mail, prezentacjach PowerPoint, fakturach, listach przewozowych, umowach itp.);

2) perspektywa biblioteki – celem zarządzania jest udostępnianie i pożyczanie elementów informacji przechowywanych w zbiorach takich instytucji, jak biblioteki publiczne, biblioteki akademickie i badawcze, biblioteki korporacyjne, elektroniczny dostęp do raportów branżowych i elektronicznych baz danych dla pracowników i pracodawców w ich organizacjach. Występuje tu organizacja wiedzy, klasyfikacja, katalogowanie, systemy wyszukiwania informacji. Z perspektywy bibliotek, zarządzanie informacją jest zarządzaniem zbiorami informacji;
3) osobista perspektywa – podobny punkt widzenia do organizacyjnego, ponieważ wiąże się z zarządzaniem wszystkimi procesami informacyjnymi w cyklu życia informacji. Główną różnicą jest jednak to, że perspektywa organizacji dotyczy zarządzania informacją dla sukcesu i dobrobytu organizacji, podczas gdy z perspektywy osobistej zarządzanie informacją ma przynieść korzyść jednostce. Elementy informacyjne są tworzone, nabywane, organizowane, przechowywane, rozprowadzane i użytkowane przez ludzi do celów osobistych. Są to osobiste notatki, czasopisma, strony internetowe, wiadomości e-mail, artykuły prasowe, książki adresowe, daty w kalendarzu, przypomnienia, komunikaty, faksy itp.

Zarządzanie organizacją dotyczy zarządzania strukturą, różnymi zasobami (ludzkimi, finansowymi, rzeczowymi) oraz zarządzania informacją. Ze względu na to, że informacja powinna być zarządzana w sposób zamierzony i ciągły, proces ten należy prowadzić poprzez funkcje zarządzania: planowanie, organizowanie

i kontrolę. Wyszczególnione funkcje pozostają spójne z funkcjami rzeczowymi powiązanymi z procesami wytwarzania, gromadzenia, przechowywania, obiegu, przetwarzania, wykorzystania i udostępniania informacji.

Według Adama Stabryły do specyficznych funkcji zarządzania informacjami zalicza się[25]:

1) planowanie potrzeb i zasobów informacyjnych;
2) organizację monitoringu procesów podstawowych i pomocniczych;
3) rozdział i kontrolę realizacji zleceń;
4) koordynowanie pracy zespołów zadaniowych;
5) sterowanie procesami techniki informacyjnej;
6) nadzór informatyczny.

Przeważnie zarządzanie informacją dotyczy wybranych aspektów, czyli aspektu statycznego i dynamicznego. W aspekcie statycznym zarządzanie odnosi się do zasobów informacyjnych, które można planować, organizować oraz kontrolować w ramach polityki informacyjnej, jednocześnie dbając o jakość informacji i jej bezpieczeństwo. Ujęcie dynamiczne dotyczy procesów, którym poddawana jest informacja (procesów informacyjnych) i obejmuje planowanie, organizowanie i kontrolowanie generowania (tworzenia) informacji, gromadzenia (pozyskiwania) informacji, przechowywania informacji, jej przetwarzania, wykorzystywania i dystrybucji. Oba ujęcia uzupełniają się wzajemnie[26].

Według Kazimiery Materskiej zarządzanie informacją pojmowane jest między innymi jako zarządzanie[27]:

1) technologią informacyjną;
2) systemami informacyjnymi;
3) zasobami informacji;
4) procesami informacyjnymi.

Z kolei Małgorzata Pańkowska określa najbardziej istotne problemy i zakresy występujące w trzech obszarach zarządzania informacją[28]:

[25] A. Stabryła, *Podstawy zarządzania firmą*, PWN, Warszawa 1995, s. 254.
[26] K. Materska, *Informacja w organizacjach społeczeństwa wiedzy*, Wyd. SBP, Warszawa 2007, s. 266.
[27] Tamże, s. 268.
[28] M. Pańkowska, *Zarządzanie zasobami informatycznymi*, Difin, Warszawa 2001, s. 31.

1) zarządzania informacją – główny problem dotyczy przyczyn zarządzania oraz jego planowania, sterowania i koordynacji. Zorientowane jest na procesy i przedsięwzięcia związane ze strategicznymi kierunkami organizacji. Celem jest całościowy rozwój organizacji. Kryteria oceny dotyczą użycia, jakości i integralności informacji;
2) zarządzania systemami informacyjnymi – główny problem dotyczy tego, co robić, co przetwarzać, czyli zorientowanie na dane, zdarzenia i transakcje. Kryteria oceny dotyczą jakości oprogramowania, szybkości rozwoju, poziomu aktualizacji. Rozwiązuje się problemy zarządzania przedsięwzięciem budowy oprogramowania, jakości projektów systemów informacyjnych, jakości i możliwości technik i narzędzi informatycznych zarządzania danymi;
3) zarządzania technologią informacyjną – główny problem wiąże się z tym, jak przetwarzać informacje. Obejmuje przegląd, wybór i dostarczenie odpowiednich technik, produktów i usług informatycznych. Kryteria oceny dotyczą wiarygodności, elastyczności, łatwości użycia, ceny i wykonania. Zasoby z tym związane to sieci, serwery, systemy operacyjne, oprogramowanie, interfejsy użytkowników, jakość pracy, narzędzi i technik zarządzania infrastrukturą.

Zarządzanie informacją jest wieloaspektowym pojęciem mającym różnorodne znaczenie i interpretacje między różnymi odbiorcami. Dotyczy zarządzania informacją przez państwo, instytucje publiczne, organizacje lub pojedynczą osobę, ale także może dotyczyć procesu realizowanego przez człowieka lub przez system informatyczny. Definicje terminu zarządzanie informacją obejmują zakres, przedmiot oraz wymagania, które należy spełniać, aby zarządzanie było efektywne i skuteczne.

Według różnych autorów zarzadzanie informacją:

1) to proces, który powinien zagwarantować integralność, poufność i wiarygodność przetwarzanej informacji z udziałem systemu informatycznego – inaczej – planowe używanie źródeł informacji do osiągnięcia określonych wyników pracy i realizacji zakładanych celów[29];

[29] L. Kiełtyka, R. Kucęba, *Klasyfikacja i i funkcjonalność informacji rynkowych oraz integratorów przepływu informacji w strukturach SIR*, [w:] *Zarządzanie przepływem i ochroną informacji*, red. M. Kwieciński, OW AFM, Kraków 2007, s. 28.

2) to dziedzina działalności, której celem jest rozpoznanie zdarzeń determinujących funkcjonowanie przedsiębiorstwa i dostarczenie informacji użytkownikom w celu zaspokojenia potrzeb[30];
3) świadome postępowanie ludzi zmierzające w kierunku optymalizacji roli informacji w osiąganiu celów przez organizację[31].

Marek Mazur proponuje następujący obszar przedsięwzięć zarządzania informacją[32]:

1) opracowanie i wdrażanie strategii informacyjnych będących wyrazem polityki informacyjnej przedsiębiorstwa;
2) rozwój systemów informacyjnych, czyli racjonalne planowanie środków inwestycyjnych na projektowanie i wdrażanie środków informatyki;
3) zapewnienie integracji systemów wykorzystywanych na różnych szczeblach zarządzania i w różnych podsystemach funkcjonalnych;
4) sterowanie przepływami informacji w sieci komunikacyjnej;
5) zapewnienie efektywności eksploatacji systemów informatycznych;
6) zarzadzanie jakością informacji;
7) stworzenie polityki bezpieczeństwa informacji;
8) konserwacja systemów informacyjnych – utrzymanie w gotowości do eksploatacji;
9) zapewnienie pożądanego rozwoju kadr informacyjnych przez organizowanie efektywnych form kształcenia;
10) tworzenie efektywnych związków z rynkiem informacyjnym;
11) organizowanie kadr potrzebnych do eksploatacji i rozwoju systemu informacyjnego odpowiadającego bieżącym i przyszłym potrzebom;
12) kontrola funkcjonowania i procesu rozwoju systemu informacyjnego;
13) rozdział kompetencji i przydział środków między poszczególne jednostki organizacyjne i stanowiska pracy realizujące zadania na rzecz systemu informacyjnego;
14) przygotowanie, wdrażanie i rozwój systemu motywacyjnego potrzebnego do realizacji celów systemu informacyjnego;

[30] *Organizacja i zarządzanie*, dz. cyt., s. 254.
[31] R. Zygała, *Podstawy zarządzania informacją w przedsiębiorstwie*, AE im. Oskara Langego, Wrocław 2007, s. 46.
[32] M. Mazur, dz. cyt., s. 183-185.

15) opracowanie systemu mierników do sprawowania funkcji zarządczych w sferze informacyjnej.

Podsumowanie

Zapewnianie informacji dla organizacji związane jest przede wszystkim z podejmowaniem decyzji oraz stworzeniem takich warunków, aby realizowane funkcje zarządzania zapewniały osiągnięcie przez organizację założonych celów. Dlatego zarządzanie informacją obejmuje planowanie, organizowanie, kierowanie i kontrolę obiegu informacji w organizacji podczas wszystkich procesów informacyjnych (gromadzenia, przechowywania, przetwarzania i udostępniania informacji). Zarządzanie informacją dotyczy zapewnienia organizacji niezbędnych zasobów informacji, sposobów korzystania z nich oraz zapewnienia warunków do realizacji każdego procesu informacyjnego. Innymi ważnymi obszarami zarządzania informacją są: porządkowanie informacji, systematyzowanie, aktualizowanie zgodnie z potrzebami i oczekiwaniami, zapewnienie ochrony i bezpieczeństwa.

Istotą zarządzania informacją jest stworzenie warunków do dostarczenia dokładnej, aktualnej, kompletnej i adekwatnej informacji potrzebującemu jej podmiotowi w odpowiednim miejscu i czasie.

Bibliografia

Berman C., *Informacja i aspekt komunikacji*, „Zagadnienia Naukoznawstwa" 1991, nr 3-4.

Detlor B., *Information management*, "International Journal of Information Management", Volume: 30, Issue: 2, April, 2010.

Dutko M., Karciarz M., *Informacja w Internecie*, PWN, Warszawa 2010.

Griffin R.W., *Podstawy zarządzania organizacjami*, PWN, Warszawa 1996.

Internetowy słownik synonimów języka polskiego, https://synonim.net/synonim/informacja.

Januszko W., *Społeczeństwo informacyjne – manipulacje, szanse, zagrożenia*, [w:] *Informatyka Q przyszłości*, Wyd. Nauk. WZ UW, Warszawa 2010.

Kiełtyka L., Kucęba R., *Klasyfikacja i i funkcjonalność informacji rynkowych oraz integratorów przepływu informacji w strukturach SIR*, [w:] *Zarządzanie przepływem i ochroną informacji*, red. M. Kwieciński, OW AFM, Kraków 2007.

Kisielnicki J., *MIS – systemy informatyczne zarządzania*, Placet, Warszawa 2008.

Krztoń W., *Informacja wyzwaniem dla bezpieczeństwa współczesnego świata*, [w:] *Informacje prawnie chronione – wybrane zagadnienia*, red. S. Topolewski, Wyd. Nauk. UPH, Siedlce 2019.

Langefors B., *Theoretical Analysis of Information Systems*, (4th ed.) Studentlitteratur, Lund, Sweden, uerbach Publishers, Philadelphia 1973.

Materska K., *Informacja w organizacjach społeczeństwa wiedzy*, Wyd. SBP, Warszawa 2007.

Mazur M., *Koncepcje wartości i ich przydatność do pomiaru wartości na potrzeby zarządzania*, [w:] *Informacja w społeczeństwie XXI wieku*, red. A. Łapińska, Wyd. UWM**,** Olsztyn 2003.

Obłój K., *Strategia organizacji*, PWE, Warszawa 2001.

Oleński J., *Ekonomika informacji*, PWE, Warszawa 2001.

Organizacja i zarządzanie, red. A. Stabryła, J. Trzcieniecki, PWN, Warszawa 1986.

Pańkowska M., *Zarządzanie zasobami informatycznymi*, Difin, Warszawa 2001.

Podstawy dowodzenia w aspekcie działań sieciocentrycznych, red. J. Wołejszo, J. Kręcikij, Wyd. AON, Warszawa 2013.

Pszczołowski T., *Mała encyklopedia prakseologii i teorii organizacji*, Ossolineum, Wrocław 1978.

Roman W.K., *Podstawy zarządzania informacją*, Wyd. Nauk. UMK, Toruń 2012.

Słownik języka polskiego PWN, https://sjp.pwn.pl/.

Stabryła A., *Podstawy zarządzania firmą*, PWN, Warszawa 1995.

Stanton W.J., Etzel M.J., Walker B.J., *Fundamentals of Marketing*, McGraw-Hill, New York 1994.

Stefanowicz B., *Informacja*, OW SGH, Warszawa 2010.

Stefanowicz B., *Informacyjne systemy zarządzania. Przewodnik*, OW SGH**,** Warszawa 2007.

Ścibiorek Z., *Analiza możliwości wykorzystania ogólnej teorii kierowania podczas podejmowania decyzji do działań bojowych*, Wyd. AON, Warszawa 1999.

Zieleniewski J., *Organizacja i zarządzanie*, PWN, Warszawa 1969.

Zygała R., *Podstawy zarządzania informacją w przedsiębiorstwie*, AE im. Oskara Langego, Wrocław 2007.

Information Management – Outline of the Problem

Summary: Information management concerns information recorded in an electronic form or on paper. Information resources are subject to planning, organizing, managing as well as controlling at every stage. Understanding the need to manage the information is not clear to everyone. Frequently, it is limited only to electronic resources since this term is usually associated with information society. Modern society produces, processes, gathers, conveys and receives an enormous amount of information by means of the most advanced ICT technologies. Hence, information management has to be a complex acting in managing every organization (office, company, community or business organization). The following article is an attempt to present the process of information management in an organization and to explain the crucial elements of the subject. This article consists of information management issues, including traditional information systems as well as ICT systems.
Keywords: *information, organization, management*

STANISŁAW TOPOLEWSKI
ORCID: 0000-0001-8268-3754
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych

Zagrożenia dla bezpieczeństwa informacji

Dlaczego chronimy informacje?

Jedną z charakterystycznych cech współczesnej cywilizacji jest bez wątpienia permanentny wzrost zarówno roli, jak i znaczenia informacji.

Informacja jest jednym z najcenniejszych naszych zasobów i przybiera postać nie tylko danych, ale również wiedzy i umiejętności. Jest nośnikiem najnowszych technologii przemysłowych, pokojowych czy wojskowych. Zasoby informacyjne są nie tylko najbardziej wartościowymi narzędziami na rynkach kapitałowych i inwestycyjnych, lecz także doskonale sprawdzają się w walce na scenie politycznej i służą osiąganiu wpływów politycznych[1].

Współcześnie zdecydowana większość podmiotów i organizacji uzależniona jest od dostępu do informacji, które decydują o ich rozwoju i pozycji na rynku. Bowiem obok zasobów surowcowych i energetycznych, zasoby informacyjne stanowią najistotniejszy czynnik potencjału cywilizacyjnego. Posiadają charakter zasobów strategicznych o istotnej wartości, są czynnikiem rozwoju cywilizacyjnego i gospodarczego oraz sprzyjają powstawaniu nowych branż i nowych profesji. Elementem efektywnej strategii ekonomicznej (gospodarczej) jest przewaga informacyjna na rynkach lokalnych i globalnych[2].

[1] K. Lidel, *Cyberbezpieczeństwo – wyzwanie przyszłości. Działania społeczności międzynarodowej*, [w:] *Bezpieczeństwo XXI wieku. Asymetryczny świat*, red. K. Liedel, P. Piasecki, T.R. Aleksandrowicz, Difin, Warszawa 2011, s. 27.

[2] P. Sienkiewicz, *Bezpieczeństwo informacji – wspólne dobro dla racji stanu, bezpieczeństwa i obronności kraju, firm i obywateli,* [w:] *Ochrona informacji niejawnych i biznesowych. Materiały IV Kongresu*, KSOIN, UŚ, Katowice 2008, s. 15-16.

Zdecydowana większość obywateli naszego kraju posiada, dysponuje i przetwarza wiadomości, informacje, materiały (dokumenty), które – z różnych względów – nie powinny być powszechnie dostępne. Dotyczy to informacji wynikających z charakteru pracy, jak również szeroko rozumianej sfery prywatnej (korespondencja, banki, urzędy, szkoły, uczelnie, placówki służby zdrowia itd.).

Najogólniej informacje możemy podzielić na wrażliwe i niewrażliwe. Wrażliwymi są te wszystkie informacje, które muszą być chronione, bo tak nakazują przepisy prawa. Zaliczyć do nich możemy informacje niejawne i dane osobowe, a także inne informacje wskazane w organizacji przez kompetentne organy (np. służby ochrony państwa czy wewnętrzne komórki bezpieczeństwa w danej organizacji) jako informacje wrażliwe[3]. Takimi informacjami mogą być też dane, w zasadzie same w sobie niewrażliwe, które w powiązaniu z innymi informacjami pozwalają na wyciągnięcie określonych wniosków. Informacjami wrażliwymi są też informacje dotyczące życia osobistego ważnych przedstawicieli państwa czy przedsiębiorców, których ujawnienie mogłoby posłużyć do nacisków czy też do szantażu określonych osób. Należy również mieć świadomość, że agregacja dokumentów (informacji) jawnych stwarza zagrożenie ich analizy i uzyskania na jej podstawie informacji wrażliwych.

Szczególną troską otacza się te informacje, których ujawnienie może wywrzeć negatywny wpływ na bezpieczeństwo państwa, jego struktury, w tym także określonych instytucji, oraz obywateli. Natomiast szczególnej ochronie podlegają informacje niejawne, czyli te, 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”[4]. Również w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej mocno akcentowane są zagadnienia związane z ochroną i bezpieczeństwem informacji w różnych wymiarach[5].

Dlatego, by zachować stabilność państwa i dawać poczucie bezpieczeństwa obywatelom, najważniejszym zadaniem i obowiązkiem rządu i jego wyspe-

[3] Tamże.

[4] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r. Nr 182, poz. 1228).

[5] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, Warszawa 2020.

cjalizowanych służb jest ochrona tych informacji. Może ją zapewnić właściwie zorganizowany i sprawnie funkcjonujący system, który będzie gwarantował ograniczenia w dostępie osób zwłaszcza do informacji wrażliwych, właściwe ich przetwarzanie, a także wykorzystanie odpowiednich i wystarczających środków bezpieczeństwa fizycznego i teleinformatycznego. Z tego też względu system ten wymaga na poziome państwa precyzyjnie określonych zasad i norm mających umocowanie w przepisach prawa, określających zasady wytwarzania informacji, sposób ich ochrony oraz sankcje, jakie mogą zostać zastosowane w przypadku niestosowania się do tych reguł.

Zagrożenia – rozumienie pojęcia

W literaturze przedmiotu znajdujemy wiele definicji terminu „zagrożenia" w zależności od przyjętego kryterium, uwarunkowań czy podejścia np. terenu, obiektu, obszaru, środowiska, czasu i wielu innych czynników. Dla przykładu kilka z wielu definicji:

1) „Zagrożenie to możliwość wystąpienia jednego z negatywnie wartościowanych zjawisk"[6].
2) „Zagrożenie to (…) sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia. Przyjmując za podstawę dziedziny, w których może wystąpić zagrożenie, wyróżnia się zagrożenia militarne i niemilitarne. Wśród zagrożeń niemilitarnych można z kolei wyróżnić zagrożenia polityczne, gospodarcze, psychospołeczne, ekologiczne, wewnętrzne i inne"[7].
3) „Zagrożenia – z jednej strony, to pewien stan psychiczny lub świadomościowy wywołany postrzeganiem zjawiska, które subiektywnie ocenia się jako niekorzystne lub niebezpieczne – z drugiej strony, czynniki obiektywne powodujące stany niepewności i obaw"[8].
4) „Zagrożenie to szeroki całokształt zjawisk, które stwarzają bezpośrednią groźbę obniżenia w krótkim czasie jakości życia ludności państwa i

[6] F.X. Kaufmann, *Koncepcja socjologii religii*, ZW Nomos, Kraków 2006.
[7] *Słownik terminów z zakresu bezpieczeństwa narodowego*, Wyd. AON, Warszawa 2008, s. 172.
[8] S. Korycki, *System bezpieczeństwa Polski*, Wyd. AON, Warszawa 1994, s. 54.

stanowią poważne ograniczenia swobody wyboru w polityce lub działaniach podmiotów nierządowych (osób, grup, korupcji)”[9].

5) „Zagrożenie to możliwość powstania sytuacji, w której dane społeczeństwo nie ma zapewnionych warunków bytu i rozwoju lub są one w sposób istotny ograniczone”[10].
6) Zagrożenia to sytuacje, w której naruszone mogą być istotne dla danego podmiotu wartości. Szersza definicja leksykalna podaje, że zagrożenie to sytuacja, w której istnieje zwiększone prawdopodobieństwo utraty życia, zdrowia, wolności albo dóbr materialnych. Zagrożenie wywołuje u człowieka niepokój lub strach o różnym stopniu natężenia, do przerażenia lub obezwładnienia włącznie, bądź odruch lub świadomą chęć przeciwdziałania. Zagrożenie może wynikać z przyczyn naturalnych (np. oddziaływania żywiołów) i spowodowanych przez innego człowieka (np. nieprzyjaciela)[11].

Zagrożenie najogólniej rozumiane jest jako brak bezpieczeństwa, przez co staje się niezmienną, nieuniknioną, a w niektórych wypadkach powszechną rzeczywistością życia ludzkiego. Jednocześnie ma ścisły związek z bezpieczeństwem. Innymi słowy bezpieczeństwo i zagrożenia są to pojęcia, które są ze sobą nierozerwalnie związane, bowiem brak bezpieczeństwa powoduje niepokój i poczucie zagrożenia. Najczęściej zjawisko zagrożenia ujmowane jest dwojako. W ujęciu subiektywnym oznacza pewien stan psychiki i świadomości, wywołany postrzeganiem zjawisk, które oceniane są jako niekorzystne lub niebezpieczne. W drugim, realnym ujęciu – akcent kładzie się na rzeczywiste czynniki powodujące ów stan niepewności i obaw[12].

Z zagrożeniem bardzo często jest utożsamiane ryzyko, które najczęściej wiąże się z możliwością pojawienia się strat, szkód w wyniku zdarzeń niepożądanych. Dlatego tak ważne jest, na każdym etapie tworzenia i modyfikacji systemu oraz przetwarzania informacji, jego szacowanie (ocena, analiza).

[9] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Wyd. AON, Warszawa 2013, s. 12.
[10] R. Wróblewski, *Wybrane problemy diagnozy bezpieczeństwa narodowego*, „Zeszyty Naukowe AON” 1991, nr 3/4, s. 69.
[11] *Leksykon wiedzy wojskowej*, red. Marian Laprus, Wyd. MON, Warszawa 1979, s. 510.
[12] K. Lidel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wyd. A. Marszałek, Toruń 2008, s. 6.

Wraz z rozwojem życia społecznego modyfikacji ulegało również rozumienie zjawiska zagrożenia. Stwierdzono, że ludzie negatywnie wartościują zarówno zjawiska godzące w przetrwanie, jak i te stanowiące wyzwanie do podjęcia określonych działań i wymagające sformułowania odpowiedzi.

Identyfikacja zagrożeń i wiedza o nich stają się zatem podstawowym warunkiem do wszczęcia działań zapobiegawczych oraz organizacji obrony. Szwajcarski politolog D. Freia, analizując subiektywne i obiektywne aspekty zagrożeń, sformułował cztery możliwe oceny stanu bezpieczeństwa:

1) stan braku bezpieczeństwa – gdy występuje rzeczywiste i istotne zagrożenie zewnętrzne, którego postrzeganie jest adekwatne;
2) stan obsesji bezpieczeństwa – gdy mało istotne zagrożenie postrzegane jest jako duże;
3) stan fałszywego bezpieczeństwa – gdy istotne zagrożenie postrzegane jest jako niewielkie;
4) stan bezpieczeństwa – gdy zagrożenie zewnętrzne jest niewielkie, a jego postrzeganie jest prawidłowe[13].

Klasyfikacje zagrożeń dla bezpieczeństwa informacji

Podobnie jak w przypadku definicji, w literaturze istnieje szereg różnego rodzaju klasyfikacji zagrożeń dla bezpieczeństwa informacji (informacyjnego). Najogólniejszy to podział ze względu na umiejscowienie źródła zagrożenia, które można podzielić na zewnętrzne i wewnętrzne.

Zewnętrzne źródła zagrożenia dzielimy na:

- wynikające z sytuacji w regionie geograficznym, położenia państwa, sojuszy, zaangażowania politycznego, militarnego i gospodarczego – zagrożenia strategiczne;
- wynikające z sytuacji w otoczeniu danej jednostki organizacyjnej.

Natomiast wewnętrzne – to w szczególności wynikające ze znaczenia jednostki organizacyjnej dla bezpieczeństwa państwa i sytuacji wewnątrz jednostki (instytucji).

[13] R. Zięba, *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych,* [*w:*] *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, red. B. Bobrow, E. Halizak, R. Zięba, Scholar, Warszawa 1997, s. 4-5.

- Przejawy zagrożeń zewnętrznych to:
  - możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne działające w sposób profesjonalny, przemyślany i zorganizowany;
  - możliwość napadu przez pojedynczych przestępców, przypadkowe osoby wykorzystujące sprzyjające okoliczności, np. na skutek niedostatecznej ochrony;
  - klęski żywiołowe mogące uszkodzić infrastrukturę instytucji;
  - akty wandalizmu polegające na niszczeniu systemów zabezpieczeń instytucji;
  - katastrofy budowlane lub inne, które mogą uszkodzić infrastrukturę instytucji;
  - długotrwałe przerwy w dostawie elektryczności.
- Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do obiektów to:
  - wzmożone zainteresowanie osób postronnych daną instytucją, pomieszczeniami, objawiające się m.in. podejmowaniem prób uzyskania informacji o obiektach, pomieszczeniach podczas rozmów z pracownikami;
  - nawiązywanie rozmów przez osoby postronne z pracownikami na temat danej instytucji;
  - podszywanie się pod byłych pracowników instytucji i przejawianie zainteresowania tym, co się po latach zmieniło;
  - interesowanie się osobami sprawującymi określone funkcje oraz sposobem wykonywania przez nie obowiązków służbowych;
  - obserwacja sposobu funkcjonowania systemu ochronnego, sekretariatu, firm dostawczych czy usługowych (np. sprzątaczek itp.);
  - rozpoznawanie systemu zabezpieczeń, w tym stosowanych urządzeń technicznie wspomagających ochronę;
  - celowe uszkadzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.;
  - próby pozyskania do grup przestępczych pracowników danej instytucji.
- Przejawy zagrożeń wewnętrznych to:
  - próby pozyskania dokumentów lub materiałów przez pracowników instytucji;

- próby, nielegalnego (nieuprawnionego) kopiowania oraz wglądu w dokumenty instytucji;
- nieostrożność w życiu towarzyskim, nieumiejętność dotrzymania tajemnicy – nadmierne „gadulstwo";
- byli pracownicy instytucji zwolnieni dyscyplinarnie.

P. Potejko[14] w publikacji *Bezpieczeństwo informacyjne* dokonuje klasyfikacji zagrożeń, które dzieli na: ogólne, wynikające z aspektów psychologicznych, środowiskowe i kryminalne, wynikające z nieuczciwej konkurencji i tradycyjne zagrożenia informacyjne.

Ogólne to: kradzież zasobów, niewłaściwe wykorzystywanie zasobów, bezprawne ujawnianie informacji osobom nieupoważnionym, podsłuchiwanie rozmów, projektowanie wadliwej infrastruktury informacji.

Wynikające z aspektów psychologicznych to: ludzkie błędy i pomyłki, nieuczciwi pracownicy, działania niezadowolonych pracowników, działalność intruzów komputerowych.

Środowiskowe i kryminalne: kataklizmy – ogień, woda, przestępczość – włamania, napady, wymuszanie itd.

Wynikające z nieuczciwej konkurencji: wywiadownie gospodarcze, opinie branży, weryfikacja dokumentów.

Następnie wskazuje na rodzaje i typowe przejawy zagrożeń:

- tradycyjne zagrożenia informacyjne: szpiegostwo, dezinformacja prowadzona przez obce służby w zakresie technologiczno-informatycznym, przestępstwa komputerowe, cyberterroryzm, walka informacyjna;
- zagrożenia technologiczno-informatyczne;
- zagrożenia odnoszące się do praw obywatelskich: przekazywanie informacji nieuprawnionym podmiotom, sprzedaż informacji, naruszanie przez władzę prywatności, bezprawne ingerowanie służb specjalnych, ograniczenie jawności życia publicznego;
- zagrożenia wynikające z błędnych, niewystarczających rozwiązań organizacyjnych czy strukturalnych: podjęte błędne decyzje, planowanie wadliwej infrastruktury, patologie, działania korupcyjne[15].

[14] P. Potejko, *Bezpieczeństwo informacyjne*, [w:] *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Aspra, Warszawa 2000, s. 196-197.
[15] Tamże, s. 197-198.

Natomiast P. Bączek[16] zagrożenia informacyjne dzieli na dwie grupy.

Do pierwszej zalicza: przestępstwa komputerowe, brak informacji, chaos informacyjny, cyberterroryzm, walkę informacyjną, działalność grup świadomie manipulujących przekazem informacyjnym.

Drugą grupę stanowią: niekontrolowany rozwój nowoczesnych technologii bioinformatycznnych; zagrożenia asymetryczne; szpiegostwo; nieuprawnione ujawnienie informacji (tzw. wyciek lub przeciek: pomyłkowy, polityczny, komercyjny); asymetria w międzynarodowej wymianie informacji: systemowa, w wyniku zaniedbań w polityce zagranicznej; naruszenie przez władze praw obywatelskich: ograniczenie jawności życia publicznego, wdzieranie się w życie prywatne, bezprawne ingerowanie służb specjalnych.

Według S. Kozieja zagrożenie to pośrednie lub bezpośrednie destrukcyjne oddziaływanie na podmiot. Wyróżnia on następujące typy zagrożeń: potencjalne lub realne, subiektywne i obiektywne, zewnętrzne i wewnętrzne, militarne i niemilitarne[17]. Ponadto umiejscawia zagrożenia informacyjne w grupie zagrożeń niemilitarnych wraz z zagrożeniami politycznymi, ekonomicznymi, społecznymi, ekologicznymi[18].

Zagrożenia można również podzielić z uwagi na lokalizację ich źródeł, jak dokonują tego A. Żebrowski i M. Kwiatkowski. I wówczas będą to: zagrożenia wewnętrzne, zewnętrzne i fizyczne.

Zagrożenia wewnętrzne, które powstają wewnątrz organizacji i obejmują zagrożenie utratą, uszkodzeniem danych lub brakiem możliwości obsługi z powodu: błędu, przypadku bądź celowego działania nieuczciwych użytkowników.

Zagrożenia zewnętrzne, które obejmują zagrożenie utratą, uszkodzeniem danych lub pozbawieniem możliwości obsługi przez celowe lub przypadkowe działanie ze strony osób trzecich w stosunku do sieci lub systemu.

Zagrożenia fizyczne, w których utrata, uszkodzenie danych lub brak możliwości obsługi występuje z powodu wypadku, awarii, katastrof lub innego

[16] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wyd. A. Marszałek, Toruń 2006, s. 177.
[17] S. Koziej, *Teoria sztuki wojennej*, Bellona, Warszawa 2011, s. 269.
[18] Tamże.

nieprzewidzianego zdarzenia wpływającego na system informacyjny bądź urządzenie sieciowe[19].

Uzupełnieniem powyższych rozważań jest stanowisko A. Żebrowskiego[20], który wskazuje, że największe zagrożenie bezpieczeństwa informacyjnego stanowi działalność człowieka. Celowe zagrożenie dla systemu bezpieczeństwa informacyjnego jest wynikiem kumulacji trzech elementów: motywu, środka realizacji włamania do owego systemu oraz okazji, czyli uzyskania dostępu do dysku komputerowego lub sieci. Człowiek może wykorzystywać różnorakie sposoby włamań do systemów informatycznych, jak np.:

- zmowę kilku sprawców;
- celowe inicjowanie awarii;
- wywoływanie fałszywych alarmów (uśpienie czujności);
- szantaż, korupcję;
- rozsyłanie do firm ankiet, zapytań, propozycji;
- rozkodowywanie hasła dostępu;
- atak słownikowy;
- podsłuch sieciowy;
- wirusy, bakterie, robaki, konie trojańskie, bomby logiczne oraz inne groźne aplikacje destabilizujące sprawność systemu;
- wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej lub serwisu informacyjnego;
- techniki obchodzenia zabezpieczeń, np. programy wykorzystujące błędy zabezpieczeń w systemach operacyjnych i oprogramowaniu użytkowym;
- przechwytywanie otwartych połączeń sieciowych.

K. Liderman z kolei podaje następujące źródła zagrożeń bezpieczeństwa informacyjnego:

- siły natury (pożary, powódzie, huragany, trzęsienia ziemi, epidemie),
- błędy ludzi i ich działania według błędnych lub niewłaściwych procedur (celowe szkodliwe działanie ludzi, awarie sprzętu komputerowego,

[19] A. Żebrowski, M. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, OW Abrys, Kraków 2000, s. 65.
[20] Tamże, s. 63-64, 70.

oprogramowania, infrastruktury usługowej – zasilania, klimatyzacji, wody, ogrzewania)[21].

M. Pańkowska[22] odnosi się zwłaszcza do zagrożeń dla bezpieczeństwa zasobów informatycznych i dzieli te zagrożenia na zdarzenia (pożary) i przyczyny zdarzeń (np. skopiowanie informacji) powodujące straty finansowe podczas budowy i eksploatacji systemu informacyjnego. W zależności od czynnika, który je powoduje, oraz sposobu oddziaływania (bezpośredni lub pośredni), rozróżnia zagrożenia: losowe zewnętrzne, losowe wewnętrzne i intencjonalne.

- Do losowych zewnętrznych zalicza: temperaturę, wilgotność, wyładowania atmosferyczne, zanieczyszczenia powietrza, awarie systemu zasilania, klimatyzacji, instalacji wodociągowej, katastrofy budowlane, kataklizmy (trzęsienia ziemi, powodzie, pożary), zamieszki zbrojne.
- Do losowych wewnętrznych należą: błędy użytkowników, przypadkowe zagubienie lub niszczenie danych spowodowane lekkomyślnością lub przeciążeniem pracą personelu, błędy administratora bazy danych lub administratora systemu operacyjnego, wadliwa konfiguracja systemu, defekty sprzętu i oprogramowania.
- Intencjonalne dzieli na pasywne i aktywne.
  Pasywne to:
  - monitorowanie sieci dla przejęcia haseł, danych finansowych, prywatnych wiadomości;
  - podgląd (obserwacja, monitorowanie pola elektromagnetycznego, fal radiowych dla odtworzenia wizualnego informacji, które dają wgląd w przebiegające procesy i w przetwarzane dane);
  - analiza ruchu w sieci (wielkość, częstość, źródło i miejsce przeznaczenia przesyłanej informacji).

  Natomiast do aktywnych zalicza:
  - bezprawną modyfikację, ujawnienie i usuwanie informacji gospodarczej, modyfikację programów i informacji przy pomocy bomby logicznej, konia trojańskiego, wirusa i robaka komputerowego, wprowadzanie nieautoryzowanego komunikatu do sieci lokalnej lub rozległej,

[21] K. Liderman, *Bezpieczeństwo informacyjne*, PWN, Warszawa 2012, s. 155.
[22] M. Pańkowska, *Zarządzanie zasobami informatycznymi*, Wyd. Dyfin, Warszawa 2001.

zmianę kierunku przepływu informacji, przetwarzanie maskaradę, czyli udawanie innej stacji sieci telekomunikacyjnej, nieautoryzowane pośrednictwo;

- oszustwa bankowe, fałszowanie urządzeń wejścia lub wyjścia (np. kart magnetycznych lub mikroprocesowych), oszustwa przez podawanie fałszywych danych identyfikacyjnych, oszustwa w systemach sprzedaży (np. w kasach fiskalnych);
- powielanie programów komputerowych, przechowywanie zabronionych prawem zbiorów;
- zakup i dystrybucja nielegalnymi kanałami sprzętu i oprogramowania;
- wymuszanie przerw w pracy systemu (poprzez uszkodzenie aplikacji, systemu operacyjnego, sprzętu komputerowego), przeszkodzenie innym w użyciu jakiejś szczególnej usługi, destabilizacja serwera bądź urządzeń zabezpieczających sieć;
- wykorzystywanie służbowego sprzętu do celów prywatnych, nieraz komercyjnych, kradzież komputerów i wyposażenia.

Podsumowując, występujące obecnie zagrożenia dla bezpieczeństwa informacji możemy podzielić na zagrożenia wynikające z:

1. Celowego działania, a w tym:
   - działalności służb specjalnych państw obcych[23];
   - terroryzmu;
   - nieuprawnionego i przestępczego działania ludzi, (np. kradzieży);
   - podsłuchów;
   - działania hackerów;
   - nieuprawnionego działania personelu organizacji (korupcja, szantaż, wyłudzenie);
2. Przypadkowego (lub nieświadomego) działania jednostek/struktur wynikającego z:
   - nieświadomości zagrożenia;

[23] Zob. B. Jakubus, M. Ryszkowski, *Ochrona informacji niejawnych*, Wyd. Projekt, Warszawa 2001, s. 11-23.

- nieostrożności w życiu towarzyskim (gadulstwo, alkohol, substancje odurzające);
- nierzetelnego wykonywania powierzonych obowiązków;
- nadawania uprawnień nieadekwatnych do zajmowanego stanowiska lub wykonywanych czynności;
- niedostatecznej znajomości, procedur, systemów, programów;
- nieodpowiedniego zabezpieczenia sieci i systemów teleinformatycznych;
- niewłaściwego zabezpieczenia stanowisk pracy.

3. Zagrożeń losowych:
   - katastrof naturalnych (kataklizmów, pożarów, zalań, huraganów, trzęsień ziemi itp.);
   - wypadków, np. podczas przewożenia materiałów wrażliwych, nagłej choroby (omdlenia, zasłabnięcia itp.).
4. Innych:
   - powoływania na odpowiedzialne stanowiska osób bez należytej wiedzy i doświadczenia;
   - naruszania przez organy władzy i administracji publicznej zasad prywatności;
   - słabej znajomości obowiązujących przepisów, norm, zasad, reguł;
   - niespójności (małej precyzyjności, wieloznaczności interpretacyjnej) prawa;
   - zemsty pracowników powodowanej różnymi pobudkami.

Zagrożenia asymetryczne to rodzaj zagrożeń obejmujący swoim zakresem prowadzenie walk informacyjnych i informatycznych. Manipulowanie informacją przez zorganizowane grupy przestępcze lub terrorystyczne, walka informacyjna (zdobywanie informacji przeciwnika – ochrona własnych), inflacja informacji (zbyt duży napływ niepotrzebnych informacji, z których nie można odróżnić prawdziwych od fałszywych) czy globalizacja informacji, to największe zagrożenia dla społeczeństwa. W znacznej mierze powiązane są one z władzą publiczną, polityką, biznesem oraz światem finansowym, zagrażając stabilności i pozycji międzynarodowej państwa.

Siły zbrojne zazwyczaj przodują w organizacji i wykorzystaniu technik informacyjnych. Szybki i precyzyjny dostęp do informacji pozwalają uzyskać systemy teleinformatyczne, które pozwalają również na jej przetwarzanie. Systemy

i sieci teleinformatyczne stały się zatem kolejnym polem prowadzenia działań i operacji militarnych[24].

W kontekście sił zbrojnych pojawił się nowy termin, mianowicie: wojna informacyjna. Departament Obrony USA definiuje ją jako „całokształt działań zmierzających do uzyskania przewagi informacyjnej poprzez oddziaływanie na zasób informacyjny przeciwnika, jego systemy informatyczne, przepływ i przetwarzanie informacji oraz obronę własnych zasobów i infrastruktury informacyjnej"[25].

Kolejny obszar szczególnie wrażliwy na zagrożenia informacyjne to gospodarka, która w znacznej części opiera się na informacji. Również administracja publiczna w Polsce w coraz większym stopniu wykorzystuje systemy przetwarzające informacje. Charakterystyczną cechą zagrożeń informacyjnych jest ich interdyscyplinarność[26]. Nie odnoszą się one tylko do pola walki militarnej, ale mogą dotknąć każdego mieszkańca kraju czy instytucji.

Skuteczne zabezpieczenia są kosztowne, dlatego też winny być dobrane adekwatnie do zagrożeń oraz do wartości szkód w przypadku braku ich zastosowania.

Jednym z najistotniejszych potencjalnych źródeł zagrożeń dla bezpieczeństwa organizacji jest naruszanie przepisów ochraniających te organizacje przez osoby posiadające dostęp do informacji, w tym również nieprzestrzeganie przepisów ustaw i innych regulacji w tym zakresie.

Należy podkreślić, że przedstawione powyżej klasyfikacje różnych zagrożeń nie stanowią katalogu zamkniętego. Ich liczba i różnorodność będzie ulegała rozszerzeniu o nowe, będzie się zmieniała również skala ich występowania. W związku z tym ważnym zadaniem każdej organizacji jest ciągłe monitorowanie zagrożeń zarówno wewnątrz, jak i w jej otoczeniu oraz dostosowywanie systemu zabezpieczeń do nowych wyzwań.

[24] K. Adamczyk, D. Sawicka-Nagańska, *Operacje informacyjne, wybór terminów, główne założenia*, „Myśl Wojskowa", nr 6(641), listopad–grudzień 2005, s. 47.
[25] S.A. Hildreth, *Cyberwarfare. CRS Report for Congress*, Washington 2001, s. 16.
[26] K. Baniak, *Analiza zagrożeń telekomunikacyjnych sektora publicznego*, [w:] *Bezpieczeństwo w telekomunikacji i teleinformatyce*, red. J. Strzelczyk, BBN, Warszawa 2007, s. 33.

Wybrane obszary zagrożeń. Przetwarzanie informacji w systemach i sieciach teleinformatycznych

Rozwój teleinformatyki powoduje, że systemy informatyczne organizacji mogą być zagrożone praktycznie ze strony każdego, kto posiada wystarczający zasób wiedzy i umiejętności.

Bezpieczeństwo systemu teleinformatycznego to najogólniej taki stan systemu, w którym ryzyko urzeczywistnienia się zagrożeń związanych z jego funkcjonowaniem jest ograniczone do akceptowalnego poziomu. Zapewnia się je, chroniąc informacje przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności. I, co ważne, zapewnia się je przed rozpoczęciem oraz w trakcie przetwarzania informacji w systemie lub sieci teleinformatycznej.

Bezpieczeństwo systemów i sieci teleinformacyjnych to takie przedsięwzięcia, które mają na celu uniemożliwienie niepowołanym osobom dostępu do zasobów informacyjnych, do których można dotrzeć poprzez przechwycenie emisji radiowych, analizę ruchu w sieciach radiowych lub wprowadzanie w błąd tych, którzy taką analizę mogą prowadzić. Natomiast bezpieczeństwo systemów łączności obejmuje systemy transmisji, bezpieczeństwo środków utrudniających oraz środków mających na celu fizyczną ochronę systemów łączności, materiałów i informacji związanych z systemami łączności[27]. Istotne jest ograniczenie możliwości nieuprawnionego dostępu do przechowywanych, przetwarzanych i przesyłanych informacji bez oddziaływania na system oraz ograniczenie możliwości nieuprawnionego oddziaływania na systemy, które może spowodować zmiany funkcjonowania sieci teleinformacyjnej, dostępu do przesyłanych, przetwarzanych i przechowywanych informacji; dezinformację; zniszczenie informacji; sfałszowanie lub nieuprawnioną modyfikację informacji[28].

Niezmiernie ważnym dla organizacji publicznych jest zapewnienie odpowiedniej ochrony takich procesów, jak: gromadzenie, przetwarzanie i udostępnianie danych wyłącznie uprawnionym osobom, co wynika z zajmowanych

[27] M. Herman, *Potęga wywiadu*, Bellona, Warszawa 2002, s. 170.

[28] A. Barczyk, T. Sydoruk, *Bezpieczeństwo systemów informacyjnych zarządzania*, Bellona, Warszawa 2003, s. 70.

stanowisk pracy i przypisanych im zadań. Często natomiast można zauważyć naklejone na monitory kartki z hasłami dostępu, bałagan na biurku, pozostawianie bez nadzoru dokumentów, wyrzucanie do kosza korespondencji z istotnymi dla organizacji informacjami, gubienie nośników informacji, które to zachowania wynikają z braku wiedzy i nieświadomości użytkowników[29]. Kolejną sytuacją powodującą zagrożenie bezpieczeństwa informacyjnego jest przesyłanie poufnych informacji pocztą elektroniczną w sposób niechroniony, nawet wtedy, gdy pracownik posiada dostęp do chronionego systemu poczty[30].

Systemy teleinformatyczne, stanowiąc obecnie najważniejszy element w zakresie przechowywania, przesyłania i przetwarzania informacji, są narażone na liczne zagrożenia. Wśród nich można wyróżnić dwie główne grupy:

- zagrożenia dla informacji przechowywanych w systemach teleinformatycznych;
- zagrożenia dla infrastruktury teleinformatycznej.

Do pierwszej grupy należą m.in.: przechwyt, zniszczenie, modyfikacja i utrudnienie (uniemożliwiające) dostęp do informacji. Działania takie mogą przybierać różne formy, do których zalicza się włamanie do sieci lub jej elektroniczny podsłuch, złamanie zabezpieczeń, bombardowanie serwera danych (jednoczesne i wielokrotne próby połączenia z serwerem danych przez dużą liczbę komputerów użytkowników nieuprawnionych do uzyskania danych, co prowadzi do tego, że legalny uczestnik nie będzie miał możliwości połączenia się z serwerem).

Do drugiej grupy zagrożeń należą fizyczne zniszczenie lub uszkodzenie urządzeń wchodzących w skład systemów teleinformatycznych, obezwładnienie ich obsługi i zabezpieczeń (np. atak terrorystyczny).

Instalowanie nielegalnego oprogramowania, przekraczanie uprawnień przez pracowników administracji, popełnianie błędów wskutek niedbalstwa użytkowników, włamanie hackerów czy kradzież kluczy kryptograficznych – to tylko niektóre zagrożenia, na które narażone są systemy teleinformatyczne, a w nich poufne dane, informacje wrażliwe oraz wszelkie informacje ważne zarówno dla pojedynczego użytkownika, jak i instytucji czy to prywatnych, czy państwowych.

[29] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, Wyd. AON, Warszawa 2010, s. 6.
[30] R.J. Sutton, *Bezpieczeństwo telekomunikacji*, WKŁ, Warszawa 2004, s. 17.

Dostępność mobilnych urządzeń zewnętrznych w pracy, przetwarzanie w chmurze czy nieświadomość pracowników oraz korzystanie z portali społecznościowych, to niektóre z przyczyn utraty danych przez większość firm.

Zagrożenia cyberprzestrzeni

Kolejną sferą działalności ludzkiej, wciąż zyskującą na znaczeniu i wymagającą ochrony i obrony, jest cyberprzestrzeń. „Oprócz pozytywnych aspektów wykorzystywania cyberprzestrzeni istnieją także negatywne formy ludzkiej działalności, a mianowicie, podobnie jak w normalnej przestrzeni, tak i tu dochodzi do popełniania przestępstw czy też aktów cyberterroryzmu, a nawet wykorzystywania tej przestrzeni przez różne państwa do nielegalnej działalności lub agresji przeciwko innym podmiotom[31].

Cyberprzestrzeń można określić jako pewnego rodzaju przestrzeń komunikacyjną, która jest tworzona dzięki systemowi powiązań internetowych. Zauważyć należy, że cyberprzestrzeń stanowi obszar kooperacji o charakterze pozytywnym, co doprowadzić może do rozwijania się sfery edukacyjnej, komunikowania się społecznego, gospodarki narodowej, jak również innych sfer. Jest ona również obszarem kooperacji o charakterze negatywnym. Taki rodzaj aktywności może przejawiać się pod czterema postaciami, a mianowicie[32]:

- cyberinwigilacji polegającej na zaostrzonej kontroli społeczeństwa przy wykorzystaniu narzędzi teleinformatycznych w krajach o ustroju autorytarnym i totalitarnym;
- cyberprzestępczości, która przejawiać się może w wykorzystaniu cyberprzestrzeni do celów kryminalnych, szczególnie w odniesieniu do przestępczości zorganizowanej i mającej charakter ekonomiczny;
- cyberterroryzmu, który polega na wykorzystywaniu cyberprzestrzeni do prowadzenia działań terrorystycznych;
- cyberwojny polegającej na wykorzystaniu cyberprzestrzeni jako czwartego (poza ziemią, morzem i powietrzem) wymiaru do prowadzenia działań o charakterze wojennym.

[31] S. Bąbas, P. Kowalski, *Bezpieczeństwo w warunkach zmian społecznych, cywilizacyjnych i kulturowych*, Wyższa Szkoła Handlowa im. Króla Stefana Batorego, Piotrków Trybunalski 2014, s. 436.
[32] P. Sienkiewicz, *Terroryzm w cyberprzestrzeni*, Warszawa 2009, s. 71.

Z cyberprzestrzenią związana jest cyberprzestępczość, którą nazywa się także przestępczością internetową. Pod tym pojęciem kryją się zabronione prawnie działania, które dokonywane są przy pomocy komputerów w sieci internetowej albo przy pomocy technologii informatycznych. Termin ten został unormowany zarówno w naukach prawnych, jak i w dziedzinie zajmującej się bezpieczeństwem teleinformatycznym. Można przyjąć, że cyberprzestępczość odnosi się do trzech kategorii przestępstw, a mianowicie[33]:

- przestępstw o charakterze tradycyjnym, które popełniane są z wykorzystaniem sieci oraz systemów informatycznych;
- publikowania nielegalnych treści;
- pozostałych przestępstw typowych dla sieci elektronicznej.

Zgodnie z D.E. Denning „cyberterroryzm jest konwergencją cyberprzestrzeni i terroryzmu. Dotyczy nielegalnych ataków i gróźb ataków przeciwko komputerom, sieciom komputerowym i informacjom przechowywanym w nich, by zastraszyć lub wymusić na rządzie lub społeczeństwie polityczne lub społeczne cele. By zakwalifikować atak jako cyberterroryzm powinien on skutkować przemocą przeciwko ludziom lub mieniu lub przynajmniej wyrządzić wystarczające szkody, by stwarzać strach”[34].

Istnieje możliwość wyróżnienia obszarów w szczególności narażonych na ataki cyberterrorystyczne. Wskazać należy na[35]:

- systemy wojskowe – przechowujące informacje na temat położenia satelitów, rozlokowania wojsk i sprzętu, dane dotyczące prowadzonych badań nad nowymi typami broni czy też nowoczesnymi systemami wykorzystywanymi do łączności i komunikacji; liczba ataków na tego rodzaju systemy zauważalna była zwłaszcza podczas trwania zimnej wojny, a ich sprawcami byli agenci innych wywiadów;
- systemy przedsiębiorstw – magazynujące dane ważne z punktu widzenia prowadzenia działalności przez daną firmę; zaliczyć do nich należy np. informacje na temat rezerwacji, klientów, technologii, z których przedsiębiorstwo korzysta; atakami na tego rodzaju infrastrukturę mogą

[33] W. Filipowski, *Internet – przestępcza gałąź gospodarki*, „Prokuratura” 2007, nr 1, s. 79.
[34] J. Kisielnicki, *MIS. Systemy informatyczne zarządzania*, Placet, Warszawa 2008, s. 121.
[35] M. Jędrzejewski, *Analiza systemowa zjawiska infoterroryzmu*, Wyd. AON, Warszawa 2002, s. 32.

zajmować się pracownicy albo byli pracownicy współpracujący z konkurencją lub też chcący dokonać zemsty na byłym pracodawcy;

- systemy tworzące infrastrukturę krytyczną państwa – do infrastruktury krytycznej państwa zalicza się te systemy, które odnoszą się do funkcjonowania całego państwa, np. systemy bankowo-finansowe, energetyczne, telekomunikacyjne, dostarczania wody, transportu, system służb podejmujących działania w sytuacjach wyjątkowych; w tego rodzaju systemach gromadzone są dane, które są istotne z punktu widzenia bezpieczeństwa całego kraju; ataki na systemy infrastruktury krytycznej państwa są najczęściej dokonywane przez pracowników takich systemów, ale również przez terrorystów.

Cyberkonflikty to konflikty cybernetyczne, działania prowadzone w sieciach komputerowych. Ich celem jest uszkodzenie fizycznych elementów infrastruktury państwa (szczególnie narażona jest tutaj infrastruktura krytyczna). Cyberprzestępczość jest zjawiskiem zagrażającym dobru chronionemu prawem, które może okazać się groźne zarówno dla osób fizycznych, jak i dla całej infrastruktury publicznej, charakteryzując się efektywnością i szerokim spektrum działań cyberprzestępców[36].

Jednakże najgroźniejszym zjawiskiem w cyberprzestrzeni jest aktualnie cyberterroryzm, czyli działania: mające na celu próbę ataku lub atak na sieci, systemy informacyjne; powodujące zniszczenie infrastruktury państwa bądź też próby zastraszenia poszczególnych rządów i społeczeństw; wykorzystujące zdobycze technologii informacyjnej wyrządzającej szkody. Najczęściej atakowane są rządowe strony internetowe, infrastruktura bankowa oraz infrastruktura krytyczna.

Można wyróżnić dwa rodzaje ataków cyberterrorystycznych, przy czym jest możliwość ich wzajemnego uzupełniania się, jak również mogą one stanowić samodzielną akcję albo część większej kampanii, a są to[37]: atak, który ma miejsce w cyberprzestrzeni, atak fizyczny na systemy informacyjne.

[36] M. Wódka, *Wyzwania dla bezpieczeństwa informacyjnego w Polsce i Unii Europejskiej*, [w:] *Bezpieczeństwo informacyjne w XXI wieku*, red. M. Kubiak, S. Topolewski, Pracownia Wydawnicza WH UPH, Siedlce-Warszawa 2016, s. 168.
[37] Tamże, s. 11.

Bez względu na rodzaj cyberataki mogą powodować zachwianie stabilności gospodarki kraju, a nawet całego świata. W odniesieniu do ataku fizycznego – terroryści w obrębie cyberprzestrzeni przeprowadzają działania, które ułatwiają lub pozorują uderzenie w rzeczywistym świecie. W takim przypadku nie jest konieczne posiadanie wiedzy informatycznej, ponieważ możliwe jest użycie tradycyjnych środków, do których zalicza się materiały wybuchowe. Ważne jest posiadanie wiedzy na temat tego, w które miejsce może być skierowane uderzenie.

Działania cyberprzestępcze mogą wywierać istotny wpływ na bezpieczeństwo państwa, jego struktur oraz społeczeństwa. Do takich zagrożeń w tym obszarze możemy zaliczyć m.in.: hacking komputerowy, podsłuch, sabotaż, szpiegostwo przemysłowe i polityczne, bezprawne niszczenie informacji, fałszerstwo, oszustwo, kradzież danych, blokowanie dostępu do usług. Cyberprzestępstwa przynoszą grupom przestępczym ogromne zyski zmniejszające dochody przedsiębiorstw, które w nieodpowiedni sposób chronią swoje dane (np. ze względów oszczędnościowych).

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej stanowi, że jednym z priorytetów jest „zapewnienie bezpieczeństwa funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni. „Szczególnie ważna jest: współpraca i koordynacja działań ochronnych z przedmiotami sektora prywatnego – przede wszystkim finansowego, energetycznego, transportowego, telekomunikacyjnego i opieki zdrowotnej – prowadzenie działań o charakterze prewencyjnym i profilaktycznym w odniesieniu do zagrożeń w cyberprzestrzeni; wypracowanie i stosowanie właściwych procedur komunikacji społecznej w tym zakresie; rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni i zapobieganie im oraz ściganie ich sprawców; prowadzenie walki informacyjnej w cyberprzestrzeni; współpraca sojusznicza, także na poziomie działalności operacyjnej służącej do aktywnego zwalczania cyberprzestępstw, w tym wymiany doświadczeń i dobrych praktyk w celu podnoszenia skuteczności i efektywności działań krajowych”[38].

[38] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, s. 24-35.

Infrastruktura krytyczna

Z punktu widzenia cyberterroryzmu najskuteczniejsze są ataki przeprowadzane na systemy należące do infrastruktury krytycznej państwa. Wynika to z faktu, że tego rodzaju ataki powodują najdotkliwsze skutki, co z kolei jest celem działania terrorystów. Dążą oni do osiągnięcia jak najszerszych negatywnych skutków, które dotkną możliwie jak największą liczbę ludności cywilnej. Badacze tematu twierdzą, że już pojawienie się symptomów wystąpienia ataku cyberterrorystycznego powoduje uruchomienie procedur, jakie są niezbędne do zapobieżenia takiemu atakowi. W związku z tym należy zdefiniować potencjalne cele, które są narażone na ataki w pierwszej kolejności[39].

Ustawa o zarządzaniu kryzysowym[40] stanowi, że należy przez to rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy:

- zaopatrzenia w energię, surowce energetyczne i paliwa;
- łączności;
- sieci teleinformatycznych;
- finansowe;
- zaopatrzenia w żywność;
- zaopatrzenia w wodę;
- ochrony zdrowia;
- transportowe;
- ratownicze;
- zapewniające ciągłość działania administracji publicznej;
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

[39] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa we współczesnym świecie*, Aspra, Warszawa 2003, s. 79.
[40] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. Nr 89, poz. 590 ze zm.).

Ze statystyk na temat ochrony infrastruktury krytycznej Stanów Zjednoczonych wynika, że podmioty działające w sieci zlokalizowanej na terenie Arabii Saudyjskiej, Indonezji i Pakistanu podejmowały wielokrotne próby sprawdzania systemów amerykańskich zabezpieczeń sieci komunikacyjnych i systemów alarmowych, jak również sieci energetycznych, wodociągów i elektrowni atomowych. Pokazuje to, że ochrona infrastruktury krytycznej każdego państwa powinna być priorytetem działań związanych z bezpieczeństwem całego państwa. W czasach cyfryzacji bezpieczeństwo cybernetyczne stanowi ważny aspekt funkcjonowania każdego kraju.

Zwykle mówi się o atakach na węzły telekomunikacyjne, teleinformatyczne oraz informacyjne – zaburzenie ich funkcjonowania ma na celu wywołanie w społeczeństwie rozruchów, paniki, strachu, lęku, dezintegracji, poczucia niepewności i zagrożenia.

Do krytycznej infrastruktury telekomunikacyjnej zakwalifikowano w szczególności:

- systemy i sieci telekomunikacyjne obsługujące określony region (państwo, mniejsze jednostki terytorialne);
- sieci teleinformatyczne, telekomunikacyjne, które są niezbędne do prawidłowego, statutowego wykonywania zadań przez organy administracji publicznej (rządowej i samorządowej);
- sieci teleinformatyczne, telekomunikacyjne służące wymianie danych w siłach zbrojnych;
- rejestry państwowe w warstwie aplikacyjnej[41].

Natomiast w kwestii infrastruktury teleinformatycznej na działanie ataków cyberterrorystycznych są szczególnie narażone:

- stacje bazowe i satelitarne;
- miejsca przebiegu telekomunikacyjnych linii międzycentralowych oraz elementarnych linii komunikacyjnych;
- różne obiekty telekomunikacyjne, np. stacje czołowe, węzły dostępowe, wyniesione koncentratory itp.;
- centrale telekomunikacyjne obsługujące instytucje państwowe, urzędy oraz organizacje, których zadaniem jest likwidacja wszelakich zagrożeń;

[41] Tamże, s. 28.

- miejsca posiadające serwery zarządzające danymi, systemami i kluczowymi bazami wykorzystywanymi przez administrację publiczną (PESEL, Regon, CEPIK, Kataster, rejestry sądowe, rejestry państwowe i in.);
- centra zarządzania i utrzymania infrastruktury telekomunikacyjnej[42].

Jak wynika z powyższego zestawienia, na ataki cyberterrorystyczne są najczęściej narażone systemy komputerowe wykorzystywane przez instytucje państwowe, których sprawne funkcjonowanie ma ogromne znaczenie dla porządku publicznego oraz codziennego życia obywateli. Obszary zainteresowania cyberprzestępców nie są wybierane przypadkowo, gdyż – uderzając w infrastrukturę państwową – wyrządzają szkodę wszystkim członkom społeczeństw, którzy z owej infrastruktury korzystają. Z tego powodu tak istotna jest ochrona owej infrastruktury przed destrukcyjnym wpływem cyberterrorystów.

Ochrona infrastruktury krytycznej to zespół przedsięwzięć organizacyjnych realizowanych w celu zapewnienia funkcjonowania lub szybkiego odtwarzania infrastruktury krytycznej na wypadek zagrożeń, w tym awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

Prawną podstawę tych działań stanowi ustawa o zarządzaniu kryzysowym, która wraz z rozporządzeniami wykonawczymi Rady Ministrów określającymi: sposób realizacji obowiązków i współpracy w zakresie Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK)[43], strukturę, sposób tworzenia oraz aktualizowania planów ochrony infrastruktury krytycznej[44], dostarcza formalnych narzędzi do identyfikacji infrastruktury krytycznej i stworzenia warunków do poprawy jej bezpieczeństwa. Wymienione przepisy prawa zdefiniowały podstawowe obowiązki podmiotów zaangażowanych w ochronę infrastruktury krytycznej oraz relacje pomiędzy nimi w ramach współpracy w realizacji NPOIK i przygotowania planów ochrony infrastruktury krytycznej.

[42] Tamże.

[43] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. Nr 83, poz. 541).

[44] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. Nr 83, poz. 542).

Zagrożenia ze strony obcych służb specjalnych

Bezpieczeństwo informacji zależy przede wszystkim od jakości ich ochrony. Jednakże należy mieć świadomość, że zapewnienie nawet najwyższego poziomu bezpieczeństwa nie zlikwiduje zagrożeń, jakie stwarzają obce służby specjalne i organizacje terrorystyczne. Dlatego też jednym z kluczowych zadań ustawowych, jakie należy uwzględnić w systemie ochrony informacji niejawnych, jest rozpoznawanie zagrożeń wywiadowczych i terrorystycznych.

Szczególnym zagrożeniem informacyjnym dotyczącym bezpieczeństwa państwa jest szpiegostwo. Zasługuje ono na wyjątkowe potraktowanie chociażby z dwóch względów, tj. trudności w jego wykrywaniu oraz szkód, jakie mogą powstać w zakresie bezpieczeństwa państwa.

Szpiegostwo, w ujęciu leksykalnym, oznacza działanie przestępcze dokonywane na szkodę określonego państwa, polegające na podjęciu pracy na rzecz obcego wywiadu, a zwłaszcza na zbieraniu i przekazywaniu informacji obcemu wywiadowi lub na ich gromadzeniu i przechowywaniu w celu przekazania obcemu wywiadowi. Natomiast szpiegiem jest osoba zdobywająca i przekazująca obcemu państwu informacje stanowiące tajemnicę państwową lub wojskową[45].

Służby wywiadowcze każdego państwa najczęściej swoją uwagę koncentrują na siłach zbrojnych innego państwa. Ma to swoje uzasadnienie, gdyż na ogół to wojsko jako pierwsze wykorzystuje wszelkiego rodzaju innowacje i zdobycze naukowo-techniczne. No i oczywiście stanowi najistotniejszy element systemu obrony i bezpieczeństwa państwa. Z tego też względu właśnie w wojsku przetwarza się najwięcej informacji niejawnych, tych najistotniejszych z punktu widzenia obronności państwa.

Ze względu na obszary zainteresowań możemy mówić o wywiadzie wojskowym, ekonomicznym, politycznym (tu mieści się terroryzm), naukowym, komputerowym (elektronicznym).

- Szpiegostwo wchodzi w skład działań wywiadowczych, którymi zajmują się służby informacyjne, a do ich zadań należy:
  - rozpoznawanie potencjałów gospodarczych i obronnych oraz administracji i szczebli decyzyjnych innych państw;

[45] P. Thiem, *Ochrona informacji niejawnych. Materiały do szkolenia pracowników*, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 2003, s. 10.

- zbieranie danych o istotnych osobach i instytucjach;
- organizowanie aktów dywersji, werbowanie agentów, manipulowanie informacyjne i wprowadzenie potencjalnego obiektu działań w błąd;
- ochrona własnego państwa i jego podmiotów przed oddziaływaniem informacyjnym przeciwnika.

Kolejnym wyzwaniem, z którym muszą się zmierzyć poszczególne państwa, jest wykorzystywanie Internetu do celów wywiadowczych, a zwłaszcza szpiegostwa gospodarczego. Stosowanie różnego rodzaju urządzeń podsłuchowych oraz rejestratorów obrazu przez niepowołane do tego osoby stało się zjawiskiem zagrażającym zarówno firmom prywatnym, jak i instytucjom państwowym. Szczególną aktywność w tym zakresie przejawia tzw. szpiegostwo korporacyjne.

Wywiad jest instytucją, wychodzącą z działaniami na zewnątrz, której celem jest uzyskiwanie informacji dla kierowniczych organów państwa, danej struktury, która nim kieruje.

- Swoje cele wywiad realizuje poprzez:
  - tzw. „biały wywiad" – informacje zdobywane przez analizę oficjalnych dokumentów (prasy, radia, telewizji, wydawnictw książkowych, Internetu, biuletynów wewnętrznych, jawnych dokumentów, zwłaszcza rządowych, sądowych
    i innych rejestrów urzędowych, dokumentacji technicznej, patentowej, wyników badań opinii społecznej itd.) są zasadniczym źródłem pozyskiwania wiedzy, wynika z tego szczególna ranga właściwej ochrony informacji, zwłaszcza wrażliwych;
  - agenturę – sieć osób tajnie współpracujących ze służbą wywiadu, których celem jest zdobywanie, potwierdzanie i pogłębianie informacji;
  - środki techniczne – podsłuch telefoniczny, zewnętrzny podsłuch obiektu, podgląd (filmowanie i fotografowanie), kontrola korespondencji, tajna rewizja, włamania do sieci komputerowej itp.

- Zainteresowania wywiadu koncentrują się głównie na:
  - ośrodkach decyzyjnych (poprzez pozyskiwanie informacji i plasowanie tzw. agentury wpływu);
  - węzłach informacyjnych (poprzez przejęcie informacji i możliwość jej deformacji);

- ośrodkach (organach) opiniotwórczych, obiektach militarnych, strategicznych i wrażliwych dla danego systemu;
- obiektach i służbach specjalnych;
- siłach zbrojnych.

- Wywiad w szczególny sposób interesuje się osobami, instytucjami, obiektami, które:
  - posiadają dostęp do ważnych informacji (np. planów mobilizacyjnych, operacyjnych, programów naukowo-badawczych, strategicznych przedsięwzięć gospodarczych) lub ze względu na możliwości (np. przebieg kariery zawodowej, posiadane wpływy, rangę polityczną itp.), że w przyszłości mogą być wpływowe ze względu na pełnienie służby czy pracy w ważnych instytucjach;
  - ze względu na możliwości mogą oddziaływać na kreowanie sprzyjających sytuacji;
  - mogą być wykorzystane w procesie tworzenia bazy do działania;
  - mogą być wykorzystane do konkretnych – ważnych przedsięwzięć wywiadowczych;
  - obiekty, na które ukierunkowane jest działanie wywiadowcze – zgodne z celem działania[46].

- Zagrożenia wywiadowcze, terrorystyczne oraz ze strony przestępczości zorganizowanej (metody działania) to:
  - wykorzystywanie najsłabszych elementów w systemie ochrony (państwa, jednostki organizacyjnej, instytucji, obiektu);
  - maskowanie działalności – praca z pozycji innego państwa, organizacji międzynarodowych, ukrywanie celu działania;
  - wykorzystywanie różnic ideologicznych, religijnych, społecznych – głównie dysproporcji w stopie życia ludności (materialne dobra).

W celu zabezpieczenia się przed szpiegostwem w strukturach państwowych tworzone są służby specjalne (tzw. kontrwywiad) zajmujące się rozpoznawaniem obcych wywiadów, ochroną własnych tajemnic państwowych,

[46] B. Jakubus, M. Ryszkowski, dz. cyt., s. 11-17.

zwalczaniem dywersji, sabotażu i innych zagrożeń związanych z działalnością zagranicznych służb.

Trudno precyzyjnie wskazać, które elementy systemu politycznego i obszary działalności społecznej są w kręgu zainteresowania służb specjalnych. Natomiast można to uczynić w stosunku do metod oraz sposobów ich prowadzenia, gdyż są one podobne do wykorzystywanych przez inne służby wywiadowcze na świecie.

Zasoby te składają się z następujących elementów:

- „akredytowany personel dyplomatyczny w Polsce, w tym rezydenci wywiadu funkcjonujący w ambasadach;
- pracownicy służb specjalnych wykonujący zadania wywiadowcze pod przykryciem różnych podmiotów gospodarczych, stowarzyszeń i fundacji;
- przypuszcza się, że dogodnym miejscem prowadzenia tej działalności są regiony graniczące z Rzeczpospolitą, a szczególnie Obwód Kaliningradzki.

Prowadzenie tego typu działań pokazuje m.in. fakt wydalenia w 2000 r. dziewięciu dyplomatów rosyjskich za prowadzenie działań niezgodnych ze statutem dyplomaty (szpiegostwo)”[47].

Przeciwdziałanie zagrożeniom

Bezpieczeństwo informacji jest to dziedzina, której znaczenie w ostatnim czasie gwałtownie rośnie. Jest to jednocześnie dziedzina tak stara, jak sam człowiek, który od zarania swojego istnienia był skazany na zdobywanie informacji (np. na temat tego, gdzie znajdują się zasoby pożywienia i wody), jej ocenę (np. czy członek plemienia, który podał taką informację, jest wiarygodny i czy ta informacja może być przydatna) oraz jej ochronę (np. przez tworzenie kręgów „wtajemniczonych” wojowników, szamanów, jej utrwalanie, najpierw w przekazach ustnych, a potem pisemnych). Zatem informacja i działania mające na celu jej wykorzystanie i ochronę towarzyszyły człowiekowi od zawsze, ale w ostatnich latach wraz z szybszym rozwojem techniki i związanymi z tym zmianami cywilizacyjnymi, nabrały szczególnego znaczenia.

[47] M. Minkina, M. Niedbała, *Zagrożenia wywiadowcze dla Rzeczypospolitej Polskiej*, [w:] *Postęp w inżynierii bezpieczeństwa*, red. K.A. Skibniewska, M. Lutostański, Wyd. UWM, Olsztyn 2015, s. 46.

Każde demokratyczne państwo dbając o własne bezpieczeństwo, a więc i bezpieczeństwo obywateli, chroni swoje tajemnice, szanuje prywatność życia i zapewnia ochronę tajemnic zawodowych oraz handlowych[48]. Demokratyzacja życia społecznego wymusza istnienie określonego zasobu informacji objętego szczególną ochroną i – w konsekwencji – dostępnego wyłącznie ściśle określonemu gronu osób, które zostało upoważnione do ich posiadania. Ochrona takich informacji jest jednym z podstawowych zadań państwa i jego wyspecjalizowanych agend. Funkcjonowanie państwa, a więc i jego życia społecznego, nie jest możliwe bez utrzymania w tajemnicy określonych informacji dotyczących jego strategii działania, obrotu gospodarczego, działalności zawodowej osób oraz ich życia prywatnego.

Znaczenie ochrony informacji znalazło odzwierciedlenie m.in. w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2014 r., w której stwierdzono, że: „bezpieczeństwo informacyjne, w tym ochrona informacji niejawnych, to jeden z najważniejszych obszarów funkcjonowania systemu bezpieczeństwa państwa.

Strategiczne zadania w tym zakresie obejmują: zapewnienie bezpieczeństwa informacyjnego państwa poprzez zapobieganie uzyskaniu nieuprawnionego dostępu do informacji niejawnych i ich ujawnieniu; zapewnienie personalnego, technicznego i fizycznego bezpieczeństwa informacji niejawnych; akredytację systemów teleinformatycznych służących przetwarzaniu tych informacji; zapewnienie realizacji funkcji krajowej władzy bezpieczeństwa w celu umożliwienia międzynarodowej wymiany informacji”[49]. „Ważnym zadaniem jest też ciągłe dostosowywanie rozwiązań prawnych, proceduralnych, fizycznych i technicznych do pojawiających się zagrożeń dla przechowywania, przetwarzania i wymiany informacji niejawnych. W tym kontekście istotne znaczenie dla ochrony systemów teleinformatycznych ma rozwój i implementacja narodowych rozwiązań kryptografii”[50].

Zapewnienie bezpieczeństwa informacji jest procesem złożonym i uzależnionym od szeregu czynników, tj.: od umiejętnego zarządzania bezpieczeństwem poszczególnych rodzajów informacji, poziomu świadomości pracowników

[48] M. Polok, *Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym*, WP LexisNexis, Warszawa 2006, s. 10.
[49] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, s. 35.
[50] Tamże, s. 50.

dopuszczonych do przetwarzania informacji oraz odpowiednio dobranych rozwiązań organizacyjno-technicznych. Należy również mieć świadomość, że bezpieczeństwo jest procesem ciągłym, w związku z tym należy udoskonalać mechanizmy zapewniające skuteczną ochronę bezpieczeństwu informacyjnemu.

Szczególnie w ostatnich latach obserwujemy zagrożenia, które nabierają szczególnego i coraz większego znaczenia i związane są z rozwojem techniki. Można zatem postawić tezę, że w przyszłości zagrożenia informacyjne będą miały zasadnicze znaczenie dla bezpieczeństwa państwa i społeczeństwa. Ranga zagrożeń informacyjnych będzie wzrastała wraz ze wzrostem zastosowań dla technik informatycznych.

Na każdym poziomie zarządzania bezpieczeństwem informacji zasadniczym celem jest niedopuszczenie do ich utraty, ujawnienia czy modyfikacji. Należy mieć również na uwadze, aby przyjęte rozwiązania organizacyjno-prawne nie utrudniały czy wręcz uniemożliwiały przepływu informacji.

Zasadniczym elementem niedopuszczenia do przeistoczenia się zagrożeń w niebezpieczeństwo jest właściwa diagnoza zagrożeń. Niski poziom świadomości tych zagrożeń oraz słabe przygotowanie ochronne i obronne społeczeństwa może wykorzystać potencjalny przeciwnik poprzez nieuprawnione korzystanie z dostępu do informacji. Ponadto ochrona informacji i ochrona przed zagrożeniami, o których wiedza jest niepełna, nie będzie skuteczną.

Zatem informacje podlegające ochronie winny być udostępnione wyłącznie osobie uprawnionej, zgodnie z obowiązującymi przepisami i wymogami w tym zakresie. Muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie. Muszą być odpowiednio chronione, z zastosowaniem środków bezpieczeństwa osobowego, fizycznego i technicznego.

Bibliografia

Adamczyk K., Sawicka-Nagańska D., *Operacje informacyjne, wybór terminów, główne założenia*, „Myśl Wojskowa", nr 6 (641), listopad-grudzień 2005.

Bania K., *Analiza zagrożeń telekomunikacyjnych sektora publicznego,* [w:] *Bezpieczeństwo w telekomunikacji i teleinformatyce*, red. J. Strzelczyk, BBN, Warszawa 2007.

Barczyk A., Sydoruk T., *Bezpieczeństwo systemów informacyjnych zarządzania*, Bellona, Warszawa 2003.

Bąbas S., Kowalski P., *Bezpieczeństwo w warunkach zmian społecznych, cywilizacyjnych i kulturowych*, Wyższa Szkoła Handlowa im. Króla Stefana Batorego, Piotrków Trybunalski 2014.

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego,* Wyd. A. Marszałek, Toruń 2006.

Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa we współczesnym świecie*, Aspra, Warszawa 2003.

Filipowski W., *Internet – przestępcza gałąź gospodarki*, „Prokuratura" 2007, nr 1.

Herman M., *Potęga wywiadu*, Bellona, Warszawa 2002.

Hildreth S.A., *Cyberwarfare. CRS Report for Congress*, Washington 2001.

Janczak J., Nowak A., *Bezpieczeństwo informacyjne. Wybrane problemy*, Wyd. AON, Warszawa 2013.

Jakubus B., Ryszkowski M., *Ochrona informacji niejawnych*, Wyd. Projekt, Warszawa 2001.

Jędrzejewski M., *Analiza systemowa zjawiska infoterroryzmu*, Wyd. AON, Warszawa 2002.

Kaufmann F.X., *Koncepcja socjologii religii*, ZW Nomos, Kraków 2006.

Kisielnicki J., *MIS. Systemy informatyczne zarządzania*, Placet, Warszawa 2008

Korycki S., *System bezpieczeństwa Polski*, Wyd. AON, Warszawa 1994.

Koziej S., *Teoria sztuki wojennej*, Bellona, Warszawa 2011.

Leksykon wiedzy wojskowej, red. Marian Laprus, Wyd. MON, Warszawa 1979.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wyd. A. Marszałek, Toruń 2008.

Liedel K., *Cyberbezpieczeństwo – wyzwanie przyszłości. Działania społeczności międzynarodowej*, [w:] *Bezpieczeństwo XXI wieku. Asymetryczny świat*, red. K. Liedel, P. Piasecki, T.R. Aleksandrowicz, Difin, Warszawa 2011.

Liderman K., *Bezpieczeństwo informacyjne*, PWN, Warszawa 2012.

Minkina M., Niedbała M., *Zagrożenia wywiadowcze dla Rzeczypospolitej Polskiej*, [w:] *Postęp w inżynierii bezpieczeństwa*, red. K.A. Skibniewska, M. Lutostański, Wyd. UWM, Olsztyn 2015.

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

Pańkowska M., *Zarządzanie zasobami informatycznymi*, Difin, Warszawa 2001.

Polok M., *Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym*, WP LexisNexis, Warszawa 2006.

Potejko P., *Bezpieczeństwo informacyjne,* [w:] *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Aspra, Warszawa 2000.

Sienkiewicz P., *Bezpieczeństwo informacji – wspólne dobro dla racji stanu, bezpieczeństwa i obronności kraju, firm i obywateli*, [w:] *Ochrona informacji niejawnych i biznesowych*, Materiały IV Kongresu, Katowice 2008.

Sienkiewicz P., *Terroryzm w cyberprzestrzeni*, Warszawa 2009.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.

Sutton R.J., *Bezpieczeństwo telekomunikacji*, WKŁ, Warszawa 2004.

Thiem P., *Ochrona informacji niejawnych. Materiały do szkolenia pracowników*, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 2003.

Wróblewski R., *Wybrane problemy diagnozy bezpieczeństwa narodowego*, „Zeszyty Naukowe AON" 1991, nr 3/4.

Zięba R., *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych,* [w:] *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, red. B. Bobrow, E. Halizak, R. Zięba, Scholar, Warszawa 1997.

Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Abrys, Kraków 2000.

Information security threats

Summary: Since the dawn of time, information has been an important element in ensuring security and development for both individuals and the state. Recently, its role and importance has been growing rapidly. It takes the form of not only data, but also knowledge and skills. Nowadays, the vast majority of countries with entities of social life and organizations depend on access to information that determines their development and position on the market. Additionally, the vast majority of citizens owns, disposes and processes messages, information, materials (documents), which, for various reasons, should not be generally available. This applies to information resulting from the nature of work as well as the broadly understood private sphere (correspondence, banks, offices, schools, universities, health care facilities, etc.). Due to its role and importance, it is exposed to many different threats. Therefore, the most important task and responsibility of the government and its specialized services in this field is to protect this information. It can be ensured by a properly organized and efficiently functioning system, which will guarantee restrictions on the access of persons, especially to sensitive information, on its proper processing, as well as the use of appropriate and sufficient physical and ICT security measures.
Keywords: *information, threats, prevention, security*

TOMASZ STEFANIUK
ORCID: 0000-0001-5769-8735
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych

Bezpieczeństwo informacji w świadczeniu pracy zdalnej

Istota i miejsce pracy zdalnej we współczesnym świecie

Telepraca to stosunkowo nowa forma wykonywania obowiązków wynikających ze stosunku pracy. Ma ona swoje podłoże w wielu zjawiskach zachodzących we współczesnym świecie, zmieniających uwarunkowania funkcjonowania organizacji w przeciągu ostatnich lat. Gospodarka globalna i dynamiczny jej rozwój wpłynął na zmiany w komunikacji, konkurencji i współpracy pomiędzy instytucjami, podmiotami rynkowymi czy pojedynczymi osobami. Chęć uzyskania trwałej przewagi konkurencyjnej często narzuca konieczność podejmowania przez firmę współpracy z innymi podmiotami rynkowymi na różnych poziomach[1]. Coraz częściej cały zespół pracowników danego przedsiębiorstwa nie jest w stanie podołać zadaniom, jakie zostały już wyznaczone. Konieczna jest współpraca międzyorganizacyjna, tworzenie zespołów złożonych ze specjalistów wielu współpracujących ze sobą instytucji.

Tymczasem rozwój technologii teleinformatycznych umożliwił elektroniczne formy komunikacji i wymiany oraz współdzielenia danych, które otworzyły nowe możliwości podejmowania pracy uniezależnionej od odległości geograficznej. Do powyższego obrazu należy jeszcze dołożyć ogromną nieprzewidywalność otoczenia i zachodzących przemian: konflikty etniczne i religijne, zmiany ustrojowe,

[1] A. Maik, A. Godzisz, *Istota i pojęcie organizacji sieciowej*, [w:] „Studia i Materiały. Miscellanea Oeconomicae" 2013, r. 17, nr 2, s. 336.

kryzysy ekonomiczne, coraz częściej występujące stany klęski żywiołowej, czy wreszcie szybki postęp technologiczny, umożliwiający powstawanie cyfrowych produktów i będące jego konsekwencją krótkie cykle życia produktów i usług. M. Trziszka wskazuje na następujące procesy implikujące rozwój telepracy[2]:

- rozwój komputerów i powstałych z nich komputerów osobistych;
- rozwój sieci komputerowych;
- rozwój środków telekomunikacji;
- rozwój systemów zarządzania przedsiębiorstwem (klasy ERP);
- rozwój nowych koncepcji zarządzania, w tym idei outsourcingu, offsourcingu oraz modelu kosztów ABC;
- digitalizacja wielu dóbr materialnych oraz powstanie nowych, niematerialnych rynków dóbr i usług.

Polskie prawo definiuje telepracę w artykule 675 Kodeksu pracy jako pracę wykonywaną regularnie poza zakładem pracy, z wykorzystaniem środków komunikacji elektronicznej w rozumieniu przepisów o świadczeniu usług drogą elektroniczną[3]. Powyższy zapis pozwala na wyodrębnienie następujących istotnych cech telepracy[4]:

- regularność świadczenia pracy w formie telepracy;
- wykonywanie pracy poza zakładem pracy;
- wykorzystywanie środków komunikacji elektronicznej w rozumieniu przepisów o świadczeniu usług drogą elektroniczną;
- przekazywanie pracodawcy wyników pracy, w szczególności za pośrednictwem środków komunikacji elektronicznej.

Telepraca może być świadczona zarówno na podstawie zwykłej umowy o pracę lub kontraktu, jak również w ramach własnej działalności gospodarczej. Rzadko stanowi ona jedyną formę pracy danej osoby – zazwyczaj jest ona łączona z klasyczną pracą w siedzibie organizacji. Oczywiście proporcje czasu telepracy do pracy lokalnej bywają różne: od okazjonalnej, gdy pracownik jedynie ze względu na wyjątkową sytuację osobistą lub zewnętrzną (jak w przypadku epidemii

[2] M. Trziszka, *Model organizacji i zarządzania systemem pracy zdalnej w branży IT*, Rozprawa doktorska, Wyd. PP, Poznań 2019, s. 9.

[3] Art. 675 § 1. ustawy z dnia 24 sierpnia 2007 r. o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw (Dz.U. z 2007 r. Nr 181, poz. 1288).

[4] S. Wrycza, *Informatyka ekonomiczna: podręcznik akademicki*, PWE, Warszawa 2010, s. 100.

koronawirusa) kontaktuje się drogami elektronicznymi ze współpracownikami, po stałe świadczenie tej formy pracy, gdzie telepraca systematycznie stanowi większą część czasu pracy danej osoby.

Telepraca kojarzy się głównie z pracą świadczoną z domu. Jednak miejscem tej formy pracy może być również lokal pracodawcy, z którego telepracownik obsługuje klientów firmy czy telecentrum (biuro wyposażone w komputery z szybkim dostępem do Internetu) dzielone przez wielu pracodawców w celu redukcji kosztów lub prowadzone przez lokalną administrację w celu tworzenia miejsc pracy w regionie[5]. Niezależnie od miejsca jej świadczenia Kodeks pracy zobowiązuje pracodawcę do:

- wyposażenia telepracownika w sprzęt, który jest niezbędny do wykonywania przez niego pracy w systemie zdalnym;
- ubezpieczenia danego sprzętu;
- pokrycia ewentualnych kosztów, które są związane z instalacją, serwisem, eksploatacją i konserwacją sprzętu;
- zapewnienia telepracownikowi pomocy technicznej, jak i niezbędnych szkoleń w zakresie obsługi danego sprzętu.

Oczywiście powyższe ustalenia mogą przebiegać inaczej, gdyż przede wszystkim są regulowane przez umowę pomiędzy pracodawcą i telepracownikiem[6].

W przypadku gdy telepracownik do pracy udostępnia własny sprzęt, wówczas ma prawo do ekwiwalentu pieniężnego. Jeśli chodzi o jego wysokość, to ustala się ją w porozumieniu. Pracodawca zachowuje też kontrolę nad wykonywaniem przez swojego pracownika obowiązków, jednak niezbędna jest tutaj zgoda osoby kontrolowanej[7].

Telepraca przynosi korzyści zarówno dla pracodawcy, pracownika, jak również gospodarki i środowiska. Brak konieczności wspólnego przebywania w pracy, czy też fakt, iż dojazdy do pracy, stają się zbędne (lub są zdecydowanie

[5] A. Szewczak, *Telepraca – szansą czy zagrożeniem na rynku pracy?*, Wyd. Hogben, Szczecin 2002, s. 43.

[6] Ustawa z dnia 24 sierpnia 2007 r. o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw (Dz.U. z 2007 r. Nr 181, poz. 1288), art. 6711 § 1.

[7] K. Karbownik, *Korzyści i zagrożenia wynikające z zatrudnienia pracowników w formie telepracy*, „Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie" 2015, nr 20, s. 165.

rzadsze), pozytywnie wpływa na wiele kwestii: możliwość pozyskania specjalistów, obniżenie kosztów pracy, wzrost wydajności pracy czy ochronę środowiska.

Brak geograficznego ograniczenia przy angażowaniu specjalistów do współpracy daje możliwość rekrutacji najbardziej utalentowanych pracowników na świecie[8]. Z drugiej strony telepraca umożliwia zatrudnienie osobom biernym zawodowo, które w tradycyjnej formie pracy prawdopodobnie nigdy nie uzyskałyby zatrudnienia.

Kolejną zaletą pracy zdalnej, uznawaną bardzo często w literaturze za najważniejszą, jest możliwość znacznego obniżenia kosztów, zarówno po stronie organizacji, jak również pracowników[9]. Obniżenie kosztów prowadzenia działalności gospodarczej jest szczególnie ważne w okresie kryzysu – z którym, według opinii większości ekonomistów, będziemy mieli do czynienia w najbliższym czasie. J. Fort[10] twierdzi, że coraz więcej firm rozważa zastąpienie spotkań bezpośrednich w siedzibie firmy wideokonferencjami lub wręcz zamykanie biur i umożliwienie pracownikom zdalnej pracy w domu. Wszystko to oczywiście w celu obniżenia kosztów. Oszczędności płynące z takiej formy pracy wynikają przede wszystkim z niższych kosztów wynajęcia biura. Jak podaje J. Nilles[11], firmy lub instytucje rządowe zatrudniające dużą liczbę pracowników pracujących w domu, mogą łatwo uzyskać nawet do 33% oszczędności powierzchni biurowej[12]. Gdyby wykorzystano także fakt, że pracownicy przez część czasu nie korzystają z miejsc parkingowych, i gdyby zostały one przydzielone innym osobom lub były przez nie wykorzystywane, miesięczne oszczędności wynosiłyby mniej więcej jedną czwartą miesięcznego kosztu parkingu.

[8] B.J. Bergiel, E.B. Bergiel, P.W. Balsmeier, *Nature of virtual teams: a summary of their advantages and disadvantages* [w:] "Management Research News", Vol. 31 No. 2, Emerald Group Publishing Limited, United Kingdom, Bingley 2008, s. 105.

[9] T. Stefaniuk, *Komunikacja w zespole wirtualnym*, Difin, Warszawa 2014, s. 76.

[10] C. Morris, *7 ways to make working from home easier during the coronavirus pandemic*, https://fortune.com/2020/03/12/working-from-home-coronavirus-remote-work-telecommuting-wfh-covid-19/ [dostęp 24.05.2020].

[11] J. Nilles, *Telepraca, strategie kierowania wirtualną załogą*, WNT, Warszawa 2003, s. 185-186.

[12] AT&T, na przykład, szacuje, że oszczędności wynikające z ograniczenia powierzchni biurowej dzięki telepracy wynoszą 2000 USD rocznie na osobę za: "Harvard Business Review", maj-czerwiec 1998, s. 128.

Brak konieczności korzystania z dojazdów do pracy, to znaczne ograniczenie kosztów po stronie telepracowników[13]. Łączny zaoszczędzony na dojazdach do pracy czas w ciągu miesiąca może sięgać od 30 do 50 godzin.

Ograniczenie dojazdów do pracy w konsekwencji stosowania telepracy prowadzi również do zmniejszenia emisji spalin silnikowych, na co zwraca uwagę opublikowana w maju 2019 r. prognoza OECD dotycząca długookresowych perspektyw rozwoju transportu na świecie[14]. Upowszechnienie telepracy może zmniejszyć ruch pasażerów w miastach z 3% do 30%[15].

Spośród innych czynników pozwalających na zmniejszenie kosztów w wyniku stosowania zespołów wirtualnych wymienić należy także spadek fluktuacji, mniejszą ilość zwolnień chorobowych czy jednodniowych urlopów. Dla przykładu ARO Call Centre (Kansas City) zredukowało wskaźnik rotacji z 60% do 4% w ciągu roku, po tym jak osiemdziesięciu pięciu ze stu pracowników mogło pracować w domu[16]. Badanie przeprowadzone przez Telework American Association w 1999 r. pokazało, że osoby pracujące w domu rzadziej korzystają ze zwolnień chorobowych. Również w przypadkach nagłych spraw osobistych lub złego samopoczucia zwykli pracownicy najczęściej biorą cały dzień wolny, natomiast osoby pracujące w formie zdalnej wracają do pracy krótko po załatwieniu bieżących spraw[17]. Ponadto taka forma pracy eliminuje konieczność zwolnienia się z pracy, gdy firma przenosi się w inne miejsce. Cenieni pracownicy mogą być zatrzymani w charakterze pracowników elastycznych, jeśli nie chcą (nie mogą) się przeprowadzić.

[13] Zakładając, że telepracownik pracuje przeciętnie trzy dni w tygodniu w domu, zastępując jazdę samochodem tam i z powrotem na odległość 50 km i przy założeniu przeciętnego zużycia 8 litrów benzyny na 100 km, oszczędność w ciągu miesiąca wyniesie 96 litrów benzyny, co przy cenie 4.50 zł/litr daje miesięcznie 432 zł oszczędności. Do tego należy doliczyć także wydatki na odpowiednią „biurową" prezencję, lunch itp. (na podstawie własnych obliczeń). Warto pamiętać także o czasie zaoszczędzonym na dojazdach do pracy, który w ciągu miesiąca może sięgać od 30 do 50 godzin. Według szacunków dyrektora działu rozwiązań biznesowych firmy IBM, oszczędności wynikające z ograniczenia kosztów podróży i strat czasu z nimi związanych wynoszą 50 milionów dolarów, za: R. Baskerville, J. Nandhakumar, *Activating and perpetuating virtual teams*, Transactions on Professional Communication 2007, Vol. 50 No. 1, s. 20.

[14] ITF Transport Outlook 2019, https://www.oecd-ilibrary.org/transport/itf-transport-outlook-2019_transp_outlook-en-2019-en [dostęp 6.05.2020].

[15] Telepraca na odsiecz środowisku, https://www.obserwatorfinansowy.pl/bez-kategorii/rotator/telepraca-na-odsiecz-srodowisku/ [dostęp 8.03.2020].

[16] Swansea University, http://www.swan.ac.uk/psychology/patra [dostęp 19.11.2011].

[17] B. Kozłowska, J. Królikowski, P. Szczęsny, *Telepraca – podręcznik dla gminnych centrów informacji*, PARP, Warszawa 2008, s. 36.

Inną, niezwykle ważną korzyścią zdalnych form pracy, jest znaczne zwiększenie jej wydajności. Praca w domu może przynieść łączny wzrost wydajności od 10 do 60%[18]. J. Nilles, prowadząc badania nad telepracą, wykazał, iż średni wzrost wydajności osób pracujących w domu, wynikający z ich samooceny, wynosi 30%[19]. Natomiast według oceny kierowników zmiany wydajność tych osób wynosiła średnio 22%. Jak wynika z badań Uniwersytetu Stanforda, osoby pracujące z domu mogą osiągać o 13% lepsze wyniki niż ich koledzy siedzący w biurze[20].

Powyższe zalety telepracy sprawiają, że coraz więcej firm oferuje pracownikom możliwość pracy zdalnej, przy czym sytuacja kształtuje się odmiennie w zależności od kraju. Według raportu OECD ponad 51% pracowników w Danii deklaruje, że doświadczyła telepracy. Najbardziej zbliżona do Danii jest pod tym względem Finlandia (46,8% zatrudnionych czasami tak pracuje) oraz Szwecja (45,8%). Największy udział pracowników stale wykonujących telepracę posiadają takie kraje, jak Holandia (33,4%), Szwecja (30,6%) i Luksemburg (27,4%). Według badania aktywności ekonomicznej ludności udział pracowników najemnych pracujących z domu w 2018 r., w grupie wiekowej od 20 do 64 lat, wyniósł w Polsce 7,8%[21]. W każdym z powyższych przykładów widoczny jest wzrost znaczenia telepracy, a w przypadku Polski liczba telepracowników w roku 2018 zwiększyła się o 20% w stosunku do roku poprzedniego[22].

Sytuacja diametralnie zmieniła się na początku roku 2020 w związku z wybuchem epidemii koronawirusa wywołującego COVID-19. Przyjęta przez Sejm RP 2 marca 2020 r. specustawa ws. koronawirusa przewidywała, że pracodawca może zlecić pracownikowi pracę zdalną. W chwili pisania niniejszego rozdziału trudno oszacować, ile firm się na to zdecyduje, ale około 2,5 miliona Polaków jest zatrudnionych w branżach, które mają taką możliwość[23].

[18] Tamże, s. 37.

[19] J. Nilles, *Telepraca*..., dz. cyt., s. 179-186.

[20] M. Duszczyk, *Koronawirus wygania Polaków na telepracę. Czas wirtualnych biur*, https://cyfrowa.rp.pl/it/45191-koronawirus-wygania-polakow-na-teleprace-czas-wirtualnych-biur [dostęp 12.08.2020].

[21] Telepraca na odsiecz środowisku, https://www.obserwatorfinansowy.pl/bez-kategorii/rotator/telepraca-na-odsiecz-srodowisku/ [dostęp 8.03.2020].

[22] *Rocznik statystyczny Pracy 2019*, red. D. Rozkrut i in., GUS, Warszawa 2020, s. 120.

[23] Praca zdalna: 5 najważniejszych zasad. Z powodu koronawirusa w Polsce przybywa osób pracujących z domu, https://alebank.pl/praca-zdalna-5-najwazniejszych-zasad-z-powodu-koronawirusa-w-polsce-przybywa-osob-pracujacych-z-domu/ [dostęp 29.03.2020].

Badania przeprowadzone przez GfK Polonia zrealizowane w dniach 20-23 marca 2020 r. (trzy tygodnie po wprowadzeniu specustawy) wskazały, że 17% pracowników może i pracuje zdalnie (co stanowi ponad 2,8 miliona pracowników), a ponad 50% normalnie, jak zwykle przed epidemią, jeździ do pracy. Pozostała część pracowników (33%) została zmuszona do zrezygnowania ze świadczenia pracy na skutek: zawieszenia działalności przez firmę (8%), przebywania na przymusowym urlopie wypoczynkowym (5%), ze względu na konieczność opieki nad dziećmi – z uwagi na zamknięte szkoły czy przedszkola (4%) bądź z innych powodów[24].

Dodatkowo, w konsekwencji zamknięcia szkół i uczelni, w obliczu epidemii, w domach pozostało 4,5 miliona uczniów[25], 300 tys., studentów[26] oraz prawie 700 tys. nauczycieli[27] świadczących zdalne nauczanie.

Oczywiście telepraca nie posiada samych zalet. Niesie ona ze sobą ryzyka związane z występowaniem braku zaufania, rywalizacji i trudności z kontrolą efektów pracy, negatywnym wpływem na życie rodzinne, pracoholizmem i uzależnieniem od Internetu czy też problemów z bezpieczeństwem informacji i systemów teleinformatycznych.

Zagrożenia dla bezpieczeństwa informacji w pracy zdalnej oraz ich następstwa

Specyfika telepracy implikuje zależność od technologii teleinformatycznych, co prowadzi do szczególnej wrażliwości na zakłócenia dostępności informacji oraz problemy związane z ich integralnością. Ponadto poza siedzibą organizacji zdecydowanie łatwiej o utratę poufności danych, a rozdzielenie geograficzne telepracowników sprawia, iż jakakolwiek forma porozumiewania się pomiędzy

[24] G. Ułan, Tylko 17% pracowników w Polsce pracuje zdalnie, ponad połowa nadal jeździ do pracy jak zwykle, https://antyweb.pl/tylko-17-pracownikow-w-polsce-pracuje-zdalnie/ [dostęp 5.04.2020].

[25] Ilu jest uczniów w Polsce? https://www.zadluzenia.com/ilu-jest-uczniow-w-polsce/ [dostęp 4.04.2020].

[26] Potocka J., Studenci wracają na uczelnie. Dziś początek roku akademickiego 2019/2020 https://www.rmf24.pl/tylko-w-rmf24/joanna-potocka/redaktor/news-studenci-wracaja-na-uczelnie-dzis-poczatek-roku-akademickieg,nId,3233364 [dostęp 30.03.2020].

[27] Ilu jest nauczycieli w Polsce? https://www.zadluzenia.com/liczba-nauczycieli-w-polsce/ [dostęp 2.04.2020].

nimi jest możliwa tylko dzięki narzędziom teleinformatycznym. Dlatego, w przypadku świadczenia pracy zdalnie, wystąpienie incydentu naruszającego bezpieczeństwo informacji powoduje m.in. zakłócenie procedur, czego skutkiem może być brak możliwości świadczenia pracy lub zmniejszenie jej skuteczności. Dodatkowo incydenty bezpieczeństwa informacji mogą spowodować wiele innych, negatywnych konsekwencji, takich jak[28]:

- bezpośrednie straty finansowe poprzez oszustwa i kradzież informacji;
- straty finansowe będące następstwem kar oraz procesów sądowych (np. z tytułu naruszenia wolności i praw z tytułu utraty danych osobowych);
- spadek wartości dla akcjonariuszy;
- utrata reputacji powodująca dewaluację marki;
- wydatki na uszkodzone, skradzione lub utracone w wyniku incydentów aktywa bezpieczeństwa informacji;
- utrata przewagi konkurencyjnej;
- spadek rentowności.

Pierwszą kwestią, o której należy pamiętać, jest fakt, że większość domów – będących podstawowym miejscem pracy telepracowników – nie posiada takich zabezpieczeń fizycznych jak siedziba organizacji. Miejsce pracy może nie zapewniać ochrony przetwarzanych dokumentów przed utratą poufności. W niektórych przypadkach trudno o wydzielenie odpowiedniej przestrzeni, tak aby osoby postronne nie miały dostępu do dokumentów, nad którymi aktualnie prowadzona jest praca. Zdecydowanie gorsze są zabezpieczenia antywłamaniowe w porównaniu z tymi stosowanymi w siedzibie firmy: nie ma szafek zamykanych atestowanymi zamkami, alarmów, monitoringu czy osobowej kontroli wejść i wyjść itd. W efekcie nikt nie jest w stanie skontrolować, jakie osoby będzie zapraszać do domu telepracownik, z kim będzie rozmawiać i komu będzie pokazywać poufne dane ze swojego komputera. Telepracownicy w swoich domach nie posiadają gaśnic, wykrywaczy dymu czy planów ewakuacyjnych.

Co istotne, praca poza siedzibą firmy – zazwyczaj w domu – to przede wszystkim brak sieciowej infrastruktury informatycznej. Pracownicy, którzy

[28] M. Ratajczyk-Mrozek, A.I. Adamik, M. Najda-Janoszka, P. Wróbel, T. Stefaniuk, R. Niedbał, *Koncepcje zarządzania zorientowane na współdziałanie i wspomagające je narzędzia informatyczne*, TNOiK, Dom Organizatora, Toruń 2016, s. 94-95.

wykonują swoje obowiązki zdalnie, są podłączeni do sieci domowych, które nie są w żaden sposób sprawdzone przez ekspertów ds. cyberbezpieczeństwa. Najczęściej one również nie są zabezpieczone w odpowiedni sposób. Co więcej występuje ryzyko, że mogą się w nich znajdować urządzenia niezabezpieczone, podatne na zagrożenia, jak np. elementy Internetu rzeczy (inteligentne kamerki, telewizory, kuchnie, bramy garażowe itp.). Umożliwia to łatwiejsze włamanie się do sieci, w której przetwarzane są służbowe informacje. Dzięki temu przestępcy mogą podsłuchiwać i przechwytywać informacje, które najczęściej będą wysyłane w formie niezaszyfrowanego tekstu[29].

Geograficzne rozproszenie pracowników zdalnych rodzi wymagania co do dostępności informacji i wiedzy poza siedzibą organizacji. Istnieje wiele sposobów zapewnienia dostępności informacji telepracownikom. Może to być przekazanie istotnych danych na pamięciowych urządzeniach przenośnych, zapewnienie zdalnego dostępu do danych przechowywanych w sieciowej infrastrukturze organizacji bądź ich przechowywania w zewnętrznej chmurze (cloud computing). Każde z nich rodzi poważne zagrożenia dla bezpieczeństwa.

Przenośne nośniki danych wynoszone poza siedzibę organizacji mogą być łatwo zgubione lub skradzione. Jak pokazują badania przeprowadzone przez Kingston Technology w 2016 r., aż 70% przedsiębiorstw nagminnie gubi nośniki pamięci. Warto dodać, że często znajdują się tam kluczowe dla organizacji dane, szczegóły realizowanych projektów, a także dane osobowe. To może się okazać bardzo kosztowne dla firm, pracowników oraz osób, których dane były na dyskach. Wg badań przeprowadzonych przez firmę Kingston prawie 24% osób przyznało, że pamięci USB w firmie nie są w żaden sposób zabezpieczane, a co więcej ponad połowa decydentów (kadra kierownicza) w firmach przyznaje się do utraty pamięci USB z ważnymi danymi[30]. Dane tracone są najczęściej z powodu uszkodzeń pamięci USB (61,2%) oraz zgubienia (31,1%) czy kradzieży pamięci USB (3,0%). Aż w 4,1% przypadków ankietowani nie mają pewności co do przyczyny utraty danych lub jest ona nieznana. Nie dość, że pamięć USB łatwo jest utracić, to w dodatku pracownicy nie zgłaszają tego typu zdarzeń w swojej firmie. Co

[29] A. Kozłowski, *Bezpieczna praca zdalna*, https://www.cyberdefence24.pl/bezpieczna-praca-zdalna [dostęp 3.04.2020].

[30] Pamięć USB – używasz prywatnie lub służbowo? Przeczytaj!!!, https://blogspeclab.pl/pamiec-usb-uzywasz-prywatnie-lub-sluzbowo-przeczytaj/ [dostęp 28.03.2020].

gorsza, dane w podręcznej pamięci najczęściej nie są zaszyfrowane ani chronione hasłem. Szyfrowanie sprzętowe zastosowane jest tylko w 21% przypadków. Szyfrowanie programowe – w 37% przypadków. Należy pamiętać, że niezabezpieczone pamięci stwarzają ryzyko nie tylko opisanego powyżej wycieku danych, ale również niebezpieczeństwa infekcji szyfrującej (ransomware) lub innego ataku wirusowego (nie mówiąc o oprogramowaniu szpiegującym backdoor).

Według ankiety firmy Apricorn 8. na 10. pracowników używa w pracy obcych napędów, np. otrzymanych na eventach branżowych[31]. W przypadku telepracowników korzystanie z prywatnych nośników pamięci jest trudne do zweryfikowania, stąd i skala ryzyka jest większa. Zespół CERT.GOV.PL informuje o ciągłym wzroście aktywności szkodliwego oprogramowania wyspecjalizowanego w rozprzestrzenianiu się za pomocą wymiennych nośników pamięci (pendrive'y, karty pamięci, zewnętrzne dyski twarde). Dotyczy to w szczególności przenośnych pamięci typu flash USB, które są najpopularniejszym medium przenoszenia danych[32].

Inne rozwiązanie – zapewnienie telepracownikom zdalnego dostępu do zasobów sieciowych (danych lub aplikacji) otwierają organizację na różnorodne zagrożenia cyberbezpieczeństwa. Aby ustanowić połączenia zdalne, organizacje często używają wirtualnej sieci prywatnej (Virtual Private Network – VPN), w celu umożliwienia użytkownikom interakcji z ich systemami. Jednak sieci VPN można porównać z jednej strony do drzwi frontowych, które umożliwiają uprawnionym użytkownikom dostęp do danych, a z drugiej strony – do tylnych drzwi, którymi osoby bez uprawnień mogą dostać się do krytycznych danych i aplikacji. W związku z tym połączenia VPN są często wykorzystywane do uzyskania nieautoryzowanego dostępu do systemów, przyciągając uwagę hackerów. Analiza danych dotyczących incydentów wykazuje, że prawie każde poważne naruszenie bezpieczeństwa IT w ciągu ostatnich kilku lat w Polsce wiązało się z pewnym sposobem nieautoryzowanego dostępu zdalnego. 86% menedżerów uważa, że naruszenia danych są bardziej prawdopodobne, gdy pracownicy pracują zdalnie[33].

[31] 8 praktyk dla bezpiecznego zarządzania nośnikami danych, https://logsystem.pl/blog/8-praktyk-dla-bezpiecznego-zarzadzania-nosnikami-danych/ [dostęp 3.04.2020].

[32] CSIRT: Nośniki USB- zapobieganie zagrożeniom, https://www.csirt.gov.pl/cer/wiadomosci/zagrozenia-i-podatnosc/110,Nosniki-USB-zapobieganie-zagrozeniom.html [dostęp 3.04.2020].

[33] T. Smug, *Niebezpieczeństwa związane z VPN i jak zminimalizować zagrożenia zdalnego dostępu za pomocą PAM?*, https://emspartner.pl/beyondtrust/niebezpieczenstwa-zwiazane-z-vpn-i-jak-zminimalizowac-zagrozenia-zdalnego-dostepu-za-pomoca-pam/ [dostęp 6.04.2020].

Trzecim, wcześniej wymienionym, rozwiązaniem udostępniania danych telepracownikom jest technologia przetwarzania w chmurze (cloud computing), która stała się jednym z coraz częściej stosowanych rozwiązań w wielu obszarach biznesowych[34]. Organizacja, korzystająca z takiej usługi, swoje zasoby wiedzy przechowuje na zewnętrznych serwerach, do których częściowy dostęp przydziela telepracownikom.

Pomimo wielu zalet takiego rozwiązania, organizacja godzi się na przynajmniej częściową utratę kontroli nad danymi oraz sposobami ich zabezpieczenia. Przechowywanie danych na zewnętrznych serwerach sprawia, że są one narażone na wyciek lub utratę, a ponadto łatwiejsze staje się przejęcie konta albo aplikacji przez osoby nieuprawnione. Pojawiają się problemy z kompatybilnością wspólnie używanych narzędzi, serwery przeciążają się, zabezpieczenia interfejsów są niedostateczne[35]. Według międzynarodowego badania, w którym wzięło udział 676 praktyków bezpieczeństwa informacji, to właśnie zwiększająca się ilość usług cloud computing została uznana za jedno z największych obecnie zagrożeń dla organizacji w dziedzinie bezpieczeństwa informacji, przy czym odsetek respondentów, którzy zidentyfikowali wykorzystanie zasobów cloud computing jako główny problem wzrósł w przeciągu roku z 28% do 44%[36].

Według Cloud Security Alliance największe zagrożenia dla danych w chmurze są następujące[37]:

1) naruszenie danych (kradzieże, oglądanie lub używanie przez osobę do tego nieupoważnioną);
2) niedostateczna identyfikacja tożsamości i zarządzanie dostępem;
3) niebezpieczne interfejsy API;
4) luki w systemie;
5) przejęcie konta;
6) ataki od wewnątrz (malicious insiders);
7) zaawansowane długotrwałe ataki (APT);
8) utrata danych;

[34] PWC, 2016 *W obronie cyfrowych granic, czyli 5 rad, aby realnie wzmocnić ochronę firmy przed Cyber ryzykiem*, s. 16, https://www.pwc.pl/pl/pdf/raport-pwc-gsiss-cyberzagrozenia-2016.pdf [dostęp 26.11.2016].

[35] M. Hołyński, *Bezpieczeństwo w Chmurach*, „Elektronika" 2012, vol. 53, nr 8, s. 119.

[36] 2014 State of Endpoint Risk Report, Ponemon Institute LLC, Traverse City 2014, s. 4.

[37] Cloud Security Alliance*, Top Threats in 2016*, https://cloudsecurityalliance.org/group/top-threats/ [dostęp 12.11.2016].

9) brak należytej staranności przy wyborze odpowiedniej technologii;
10) nadużywanie oraz niefrasobliwe korzystanie z usług Cloud.

Wystąpienie incydentu dotyczącego wiedzy przechowywanej w chmurze skutkować może utratą reputacji, wyższymi kosztami i potencjalnie nawet likwidacją firmy[38].

Kolejnym następstwem pracy zdalnej jest konieczność zapewnienia sprzętu komputerowego telepracownikom i realizowana jest na dwa sposoby:

1) korzystanie ze sprzętu służbowego w domu;
2) praca na prywatnym komputerze.

Obydwa przypadki niosą za sobą negatywne konsekwencje dla bezpieczeństwa informacji. Z jednej strony praca na służbowym sprzęcie poza siedzibą organizacji stwarza większe ryzyko jego kradzieży (choćby podczas transportu). Łatwiej w przestrzeni prywatnej o dostęp osób trzecich do urządzeń służbowych lub o celowe ich udostępnienie (np. domownikom). Jak wynika z przeprowadzonych badań, około 50% wszystkich pracowników deklaruje, że z ich firmowego laptopa korzysta rodzina[39]. Dodatkowe ryzyka mogą stwarzać dzieci czy nawet zwierzęta, które mogą przez przypadek zalać firmowy sprzęt lub go uszkodzić, ale również omyłkowo wysłać e-maila służbowego czy wprowadzić modyfikacje w dokumentacji. W środowisku domowym służbowe komputery nie posiadają osłony firewall, a często pozbawione są także aktualizacji programów antywirusowych.

Z drugiej strony korzystanie z komputerów prywatnych to jeszcze większe zagrożenie dla bezpieczeństwa informacji. Bardzo często urządzenia prywatne pozbawione są większości zabezpieczeń stosowanych tradycyjnie w sprzęcie firmowym. Nie posiadają one kont zabezpieczonych hasłami, aktualnych programów antywirusowych czy ograniczeń ruchu sieciowym (np. firewall). Dodatkowo częściej są zainfekowane wirusami. Podczas prywatnego wykorzystywania tych urządzeń pracownicy lub ich domownicy wchodzić mogą na niebezpieczne strony internetowe lub instalować niebezpieczne aplikacje, sprowadzając ryzyko na dane służbowe i systemy wewnątrz firmy, z którymi telepracownik będzie się łączył z prywatnego komputera.

W związku z powyższym transfer plików pomiędzy sprzętem służbowym i prywatnym niesie za sobą poważne ryzyko naruszeń i ataków hackerskich, a jak

[38] Tamże, s. 4.
[39] Infowatch, http://www.InfoWatch.com [dostęp 4.02.2010].

wynika z prowadzonych badań, do takiego transferu przyznaje się 46% pracowników zdalnych[40].

Coraz częściej do komunikacji z innymi pracownikami lub do pracy w sieci służbowej wykorzystywane są również prywatne smartfony i tablety. Trend powyższy nazwany jest BYOD (Bring Your Own Device). Specyfikacja współczesnych urządzeń mobilnych umożliwia pracownikom dostęp do sieci korporacyjnej i biznesowych aplikacji z dowolnego miejsca. W konsekwencji duża ilość poufnych informacji firmowych jest zatem narażonych na utratę lub kradzież. Jak łatwo się domyśleć, crackerzy chętnie wykorzystują fakt, że coraz więcej urządzeń łączy się z globalną siecią. Dla samego systemu Android, tylko w drugim kwartale 2018 r., specjaliści odnotowywali pojawianie się nowych zagrożeń co 7 sekund. Natomiast w pierwszej połowie roku 2018 naliczono ponad 2 miliony przykładów złośliwego oprogramowania działającego w systemie stworzonym przez Google'a [41].

Pomimo że smartfony i tablety są wszechobecnym narzędziem pracy telepracowników, a informacje o zagrożeniach z nimi związanych są obecne w czołówkach serwisów informacyjnych, to organizacje nie spieszą się z wprowadzaniem zabezpieczeń mających przeciwdziałać zagrożeniom ze strony urządzeń przenośnych[42].

Analogiczne ryzyka, jak w przypadku korzystania z urządzeń teleinformatycznych, istnieją podczas wykorzystywania prywatnych nośników informacji. Według analizy przeprowadzonej w 2016 r. przez Kaspersky Lab ICS Cert, przenośne pamięci masowe są drugim z najczęstszych źródeł wnikania złośliwego oprogramowania. Podłączając prywatne przenośne urządzenie do komputera służbowego, możemy przenieść do niego (lub nawet do całej infrastruktury IT) np. złośliwy kod znajdujący się na pendrivie. Jego źródłem są zwykle zainfekowane, pobierane z sieci pliki (zwłaszcza pornografia)[43]. Inną kwestią istotną dla bezpieczeństwa

[40] A. Kozłowski, *Bezpieczna...*, dz. cyt.

[41] D. Długosz, *Nowy wirus na Androida pojawia się co 7 sekund. Tak źle jeszcze nie było*. https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/nowy-wirus-na-androida-pojawia-sie-co-7-sekund-tak-zle-jeszcze-nie-bylo/s68yx49 [dostęp 5.04.2020].

[42] Jedynie nieco ponad połowa organizacji na świecie (54%) wdrożyło strategię bezpieczeństwa dla urządzeń przenośnych. Źródło: *The Global State of Information Security® Survey 2015*, PWC, s. 25.

[43] Dekra, Nie używaj prywatnych pamięci przenośnych w pracy, https://hi-in.facebook.com/DEKRAwPolsce/photos/dlaczego-nie-powiniene%C5%9B-u%C5%BCywa%C4%87-prywatnych-pendrive%C3%B3w-na-komputerach-s%C5%82u%C5%BCbowych-%EF%B8%8F/2753828461301721/ [dostęp 6.04.2020].

danych w pracy zdalnej jest fakt, iż osoba pracująca w domu, pozbawiona jest bezpośredniego wsparcia ze strony administratora czy specjalisty bezpieczeństwa informacji. W takiej sytuacji łatwiej o zachowania niezgodne z polityką bezpieczeństwa firmy bądź o zwykłą pomyłkę. Nie mając w pobliżu siebie kolegów czy przełożonych, trudniej jest wykryć potencjalny atak przy użyciu socjotechniki – phishing. Jak pokazuje przypadek epidemii koronawirusa, powszechna praca zdalna jest łatwo wykorzystywana przez cyberprzestępców do licznych wyłudzeń lub podszywania się pod inne instytucje.

Już od wielu lat wszystkie badania poświęcone bezpieczeństwu informacji wskazują na człowieka jako głównego sprawcę incydentów zagrażających bezpieczeństwu informacji. Należy zauważyć, że aż 70% wszystkich nadużyć w roku 2014 było popełnionych przez pracowników organizacji (z czego 48% przez obecnych, a 22% przez byłych pracowników)[44]. Jednak w większości przypadków pracownicy są wykorzystywani jedynie jako środek do przenoszenia złośliwego oprogramowania czy jako obiekt ataku phishingowego i wykorzystującego socjotechnikę, stając się w ten sposób narzędziem w ręku rzeczywistych sprawców. Zdecydowanie łatwiej bowiem cyberprzestępcom wykorzystać naiwność człowieka niż złamać coraz to doskonalsze zabezpieczenia sprzętowo-programowe. Takich pracowników można podzielić na trzy kategorie: beztroskich i niedoświadczonych, wprowadzonych w błąd lub padających ofiarą ataków typu: inżynieria społeczna.

Bardzo często pracownicy wykonują lwią część pracy cyberprzestępców, stosując np. te same loginy i hasła w różnych serwisach, które nie są równie dobrze zabezpieczone. Wystarczy więc, że włamywacz wydobędzie informacje z bazy danych, z tego teoretycznie nieistotnego portalu, aby chwilę później, wykorzystując zdobyte dane, zalogować się do skrzynki pocztowej lub wykraść dane znajdujące się na firmowym dysku wirtualnym.

Jest to szczególnie istotne w pracy zdalnej, w której pracownicy nie mogą liczyć na szybkie wsparcie ze strony administratora czy serwisanta w miejscu swojej pracy. Rzadkością są również szkolenia dla wirtualnych pracowników dotyczące zagrożeń bezpieczeństwa informacji. W efekcie 70% ekspertów w dziedzinie bezpieczeństwa uważa, że pracownicy zdalni stanowią większe zagrożenie niż pracownicy wykonujący swe obowiązki w siedzibie pracodawcy[45].

[44] Tamże, s. 16.
[45] A. Kozłowski, *Bezpieczna*..., dz. cyt.

Zestawienie głównych zagrożeń dla bezpieczeństwa informacji wynikających ze specyfiki pracy zdalnej przedstawiono w tabeli 1.

Tabela 1. Zagrożenia w obszarze bezpieczeństwa informacji w pracy zdalnej

Cechy pracy zdalnej	Zagrożenie dla bezpieczeństwa informacji
Brak wydzielonego stanowiska pracy	- przeglądanie lub kopiowanie danych przez osoby trzecie - kradzież danych - modyfikacja danych
Brak adekwatnych zabezpieczeń fizycznych	- kradzież danych - kopiowanie danych
Stała obecność osób trzecich (domowników)	- ryzyko nieuprawnionego dostępu do danych - usunięcie danych - modyfikacja danych
Brak wsparcia ze strony administratora	- zwiększone ryzyko ataków phishingowych - błędna reakcja na incydenty bezpieczeństwa - dłuższy brak dostępu do danych w przypadku incydentu bezpieczeństwa
Korzystanie ze służbowych urządzeń w domu	- kradzież urządzeń - ryzyko nieuprawnionego dostępu do danych - ryzyko uszkodzenia sprzętu
Korzystanie z prywatnych urządzeń w celach służbowych	- nieautoryzowany dostęp do danych - zainfekowanie plików zawierających informacje służbowe - zainfekowanie systemów informatycznych organizacji
Praca w domowej sieci internetowej	- przechwycenie informacji / podsłuch informacyjny - włamanie się do sieci organizacji
Korzystanie ze służbowych nośników danych	- kradzież nośnika - nieautoryzowany dostęp do danych
Korzystanie z prywatnych nośników danych	- utrata danych - nieautoryzowany dostęp do danych - zainfekowanie plików zawierających informacje służbowe - zainfekowanie systemów informatycznych organizacji - ataki hackerskie na systemy informatyczne organizacji
Dostęp do danych w chmurze	- naruszenie danych (kradzież, wgląd w dane) - ataki hackerskie - brak dostępu do danych
Korzystanie z wirtualnej sieci prywatnej (Virtual Private Network – VPN)	- ataki hackerskie na systemy informatyczne organizacji

Źródło: opracowanie własne.

Ochrona informacji w organizacji pracy zdalnej

Z perspektywy bezpieczeństwa informacyjnego w pracy zdalnej optymalnym rozwiązaniem jest posiadanie przez organizację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), który kompleksowo obejmuje wszystkie obszary zagrożeń i sposoby przeciwdziałania im. Wdrożenie SZBI jest obligatoryjne w organizacjach, w których istnieje konieczność zachowania zgodności ze standardami, wytycznymi branżowymi takimi jak SOX, Basel II czy Cobit oraz zgodności z przepisami prawa, co szczególnie dotyczy podmiotów publicznych podlegających Ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących działania publiczne[46]. Jednak rosnąca świadomość w zakresie potrzeby ochrony informacji, szczególnie tych dotyczących know-how, danych osobowych czy też danych klientów sprawiają, że po SZBI coraz częściej sięgają organizacje chcące uchodzić w oczach swoich klientów za bezpiecznych i wiarygodnych partnerów.

Tworzenie i modyfikacja systemu zabezpieczeń oparte na cyklicznej analizie ryzyka – charakterystyczne dla SZBI – są szczególnie istotne podczas pracy zdalnej, zależnej od technologii teleinformatycznych. Z kolei kompletność podejścia oznacza zajęcie się całą organizacją i wszystkimi procesami przetwarzania informacji. SZBI oparty o normę PN ISO/IEC 27001 obejmuje m.in. takie obszary istotne z perspektywy bezpieczeństwa informacji, a kluczowe dla pracy zdalnej, jak:[47]

- polityka stosowania urządzeń mobilnych;
- telepraca;
- dostęp do sieci i usług sieciowych;
- zarządzanie dostępem użytkowników;
- uświadamianie, kształcenie i szkolenie z zakresu bezpieczeństwa informacji;
- przekazywanie nośników informacji;
- bezpieczeństwo sprzętu i aktywów poza siedzibą;
- bezpieczeństwo komunikacji i przesyłania informacji drogą elektroniczną;

[46] Są one zobowiązane do wdrożenia zasad zarządzania bezpieczeństwem informacji, co wynika z Rozporządzenia 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.

[47] PN ISO/IEC 27001:2014-12- *Systemy zarządzania bezpieczeństwem informacji – wymagania*, s. 16-27.

- ochrona przed szkodliwym oprogramowaniem;
- zarządzanie usługami świadczonymi przez dostawców;
- zgłaszanie incydent;
- zapewnienie ciągłości działania;
- zapewnianie zgodności z prawem.

Oczywiście zabezpieczenia w poszczególnych obszarach są opisane w normie na dużym poziomie ogólności. Każda organizacja w oparciu o zapisy normy tworzy zestaw procedur opisujących szczegółowy sposób postępowania w powyższych obszarach uwzględniający specyfikę danej organizacji.

Jeśli w danej organizacji nie funkcjonuje SZBI, zasady dotyczące bezpiecznej pracy zdalnej powinny zostać opracowane oddzielnie i uwzględniać następujące kwestie:

1) Zaopatrzenie telepracownika w komputer służbowy zabezpieczony wcześniej przez administratora w: system antywirusowy, firewall, konto zabezpieczone hasłem, ustawione blokowanie komputera po pewnym krótkim czasie bezczynności. W przypadku niemożności skorzystania z komputera służbowego – komputer prywatny powinien zostać poddany takiemu samemu reżimowi bezpieczeństwa jak sprzęt służbowy.
2) Zaopatrzenie telepracownika w szyfrowane służbowe dyski przenośne.
3) Opracowanie zasad bezpiecznego łączenia się ze służbową infrastrukturą informatyczną z wykorzystaniem szyfrowanych metod łączenia.
4) Wprowadzenie zakazu zapisywania na prywatnych nośnikach informacji i prywatnych komputerach jakichkolwiek plików z danymi wrażliwymi (dane osobowe, informacje niejawne lub inne istotne z punktu organizacji dane).
5) Opracowanie zasad bezpiecznego korzystania z poczty elektronicznej, zawierających min:
   a) zakaz korzystania z systemu poczty elektronicznej dla celów prywatnych oraz z adresów prywatnych do celów służbowych;
   b) nakaz szyfrowania informacji wrażliwych, a szczególnie danych osobowych przed wysłaniem.
6) Opracowanie zasad przechowywania dokumentów w przestrzeni domowej.
7) Politykę haseł dostępu (określającą ich siłę, częstotliwość zmian czy sposoby przechowywania).

8) Pomoc techniczną telepracownikom.
9) Sposób postępowania w przypadku wykrycia incydentu bezpieczeństwa informacji.

Należy równocześnie pamiętać, że samo opracowanie odpowiednich zasad i procedur działania nie sprawi, że będą one stosowane. Każdy incydent naruszenia bezpieczeństwa informacji w organizacji jest mniej lub bardziej zależny nie tylko od zapisanych procedur czy technologii, ale przede wszystkim od ludzi. Niewłaściwe postępowanie lub brak działania ze strony pracowników prowadzi do większości incydentów związanych z bezpieczeństwem informacji. W związku z powyższym telepracownicy muszą być zaznajomieni z obowiązującymi procedurami i rozumieć konsekwencje swoich zachowań. Dlatego nieodzowną częścią organizacji pracy zdalnej muszą stanowić szkolenia, które nie tylko zwiększają wiedzę na temat bezpieczeństwa informacji, ale przede wszystkim posiadają istotny wpływ na faktyczne zachowania pracowników w tym obszarze[48].

Podsumowanie

Praca zdalna ze swej istoty jest uzależniona od wykorzystania systemów teleinformatycznych. Technologie te umożliwiają dostęp do niezbędnych informacji i wiedzy, wspólne podejmowanie decyzji, przesyłanie efektów pracy, konsultacje czy dyskusje. Jednym słowem pozwalają na realizację zadań. Charakterystyka tej formy pracy sprawia, że pojawiają się w niej nowe – liczne – zagrożenia dla bezpieczeństwa informacji. Z kolei wystąpienie incydentu bezpieczeństwa informacji powoduje zakłócenia procedur i procesów bądź uniemożliwia ich realizację, a w efekcie zmniejsza skuteczność całej organizacji.

W konsekwencji zasadne wydaje się wdrożenie w organizacjach stosujących pracę zdalną systemu zarządzania bezpieczeństwem informacji. W przypadku niewielkich podmiotów zawiłe procedury i działania SZBI mogą wydawać się zbyt zbiurokratyzowane czy wręcz zbędne. Jednak z perspektywy potencjalnych kosztów, wynikających z naruszenia bezpieczeństwa informacji, posiadanie zasad bezpieczeństwa pracy zdalnej staje się koniecznością.

[48] T. Stefaniuk, *Training in shaping employee information security awareness*, "Entrepreneurship and Sustainability Issues" 2020, No. 7 (3), s. 1843.

Bibliografia

8 praktyk dla bezpiecznego zarządzania nośnikami danych, https://logsystem.pl/blog/8-praktyk-dla-bezpiecznego-zarzadzania-nosnikami-danych/ [dostęp 3.04.2020].

2014 State of Endpoint Risk Report, Ponemon Institute LLC, Traverse City 2014.

Baskerville R., Nandhakumar J., Activating and perpetuating virtual teams, [w:] Transactions on Professional Communication 2007, Vol. 50, No.1.

Bergiel B.J., Bergiel E.B., Balsmeier P.W., *Nature of virtual teams: a summary of their advantages and disadvantages,* [w:] "Management Research News", Vol. 31, No. 2, Emerald Group Publishing Limited, United Kingdom, Bingley 2008.

Cloud Security Alliance, *Top Threats in 2016*, https://cloudsecurityalliance.org/group/top-threats/ [dostęp 12.11.2016].

CSIRT: Nośniki USB- zapobieganie zagrożeniom, https://www.csirt.gov.pl/cer/wiadomosci/zagrozenia-i-podatnosc/110,Nosniki-USB-zapobieganie-zagrozeniom.html [dostęp 3.04.2020].

Dekra, *Nie używaj prywatnych pamięci przenośnych w pracy*, https://hi-in.facebook.com/DEKRAwPolsce/photos/dlaczego-nie-powiniene%C5%9B-u%C5%BCywa%C4%87-prywatnych-pendrive%C3%B3w-na-komputerach-s%C5%82u%C5%BCbowych-%EF%B8%8F/2753828461301721/ [dostęp 6.04.2020].

Długosz D., *Nowy wirus na Androida pojawia się co 7 sekund. Tak źle jeszcze nie było*, https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/nowy-wirus-na-androida-pojawia-sie-co-7-sekund-tak-zle-jeszcze-nie-bylo/s68yx49 [dostęp 5.04.2020].

Duszczyk M., Koronawirus wygania Polaków na telepracę. Czas wirtualnych biur, https://cyfrowa.rp.pl/it/45191-koronawirus-wygania-polakow-na-teleprace-czas-wirtualnych-biur [dostęp 5.04.2020].

GfK Corona Mood, *Dynamika zachowań konsumenckich na rynkach FMCG, dóbr trwałych i usług finansowych*, https://www.gfk.com/pl/aktualnosci/press-release/polowa-respondentow-51-proc-deklaruje-ze-chodzi-do-pracy-jak-zwykle/, https://antyweb.pl/tylko-17-pracownikow-w-polsce-pracuje-zdalnie/ [dostęp 5.04.2020].

"Harvard Business Review", maj-czerwiec 1998, s. 128.

Hołyński M., *Bezpieczeństwo w Chmurach*, „Elektronika" 2012, vol. 53, nr 8, s. 119.

Ilu jest nauczycieli w Polsce?, https://www.zadluzenia.com/liczba-nauczycieli-w-polsce/ [dostęp 04.04.2020].

Ilu jest uczniów w Polsce?, https://www.zadluzenia.com/ilu-jest-uczniow-w-polsce/ [dostęp 4.04.2020].

Infowatch, http://www.InfoWatch.com [dostęp 4.02.2010].

ITF Transport Outlook 2019, https://www.oecd-ilibrary.org/transport/itf-transport-outlook-2019_transp_outlook-en-2019-en [dostęp 6.05.2020].

Karbownik K., *Korzyści i zagrożenia wynikające z zatrudnienia pracowników w formie telepracy*, „Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie" 2015, nr 20.

Kozłowska B., Królikowski J., Szczęsny P., *Telepraca – podręcznik dla gminnych centrów informacji*, PARP, Warszawa 2008.

Kozłowski A., *Bezpieczna praca zdalna*, https://www.cyberdefence24.pl/bezpieczna-praca-zdalna [dostęp 3.04.2020].

Maik A., Godzisz A., *Istota i pojęcie organizacji sieciowej*, [w:] „Studia i Materiały. Miscellanea Oeconomicae" 2013, r. 17, nr 2.

Morris C., *7 ways to make working from home easier during the coronavirus pandemic,* https://fortune.com/2020/03/12/working-from-home-coronavirus-remote-work-tele-commuting-wfh-covid-19/ [dostęp 24.05.2020].

Nilles J., *Telepraca, strategie kierowania wirtualną załogą*, WNT, Warszawa 2003.

Pamięć USB – używasz prywatnie lub służbowo? Przeczytaj!!!, https://blogspec-lab.pl/pamiec-usb-uzywasz-prywatnie-lub-sluzbowo-przeczytaj/ [dostęp 28.03.2020].

PN ISO/IEC 27001:2014-12-2014 – *Systemy zarządzania bezpieczeństwem informacji – wymagania*.

Potocka J., *Studenci wracają na uczelnie. Dziś początek roku akademickiego 2019/2020*, https://www.rmf24.pl/tylko-w-rmf24/joanna-potocka/redaktor/news-studenci-wra-caja-na-uczelnie-dzis-poczatek-roku-akademickieg,nId,3233364 [dostęp 30.03.2020].

Praca zdalna: 5 najważniejszych zasad. Z powodu koronawirusa w Polsce przybywa osób pracujących z domu, https://alebank.pl/praca-zdalna-5-najwazniejszych-zasad-z-powodu-koronawirusa-w-polsce-przybywa-osob-pracujacych-z-domu/ [dostęp 29.03.2020].

PWC, 2016, *W obronie cyfrowych granic, czyli 5 rad, aby realnie wzmocnić ochronę firmy przed Cyberryzykiem*, https://www.pwc.pl/pl/pdf/raport-pwc-gsiss-cyberzagroz-enia-2016.pdf [dostęp 26.11.2016].

Ratajczyk-Mrozek M., Adamik A.I., Najda-Janoszka M., Wróbel P., Stefaniuk T., Nie-dbał R., *Koncepcje zarządzania zorientowane na współdziałanie i wspomagające je narzędzia informatyczne*, TNOiK, Dom Organizatora, Toruń 2016.

Rocznik statystyczny pracy 2019, GUS, Warszawa 2020, s. 120.

Smug T., *Niebezpieczeństwa związane z VPN i jak zminimalizować zagrożenia zdalnego dostępu za pomocą PAM?*, https://emspartner.pl/beyondtrust/niebezpieczenstwa-zwiazane-z-vpn-i-jak-zminimalizowac-zagrozenia-zdalnego-dostepu-za-pomoca-pam/ [dostęp 6.04.2020].

Stefaniuk T., *Komunikacja w zespole wirtualnym*, Difin, Warszawa 2014.

Stefaniuk T., *Training in shaping employee information security awareness*, „Entrepreneurship and Sustainability Issues" 2020, nr 7 (3).

Swansea University, http://www.swan.ac.uk/psychology/patra [dostęp 19.11.2011].

Szewczak A., *Telepraca – szansą czy zagrożeniem na rynku pracy*? Wyd. Hogben, Szczecin 2002.

Telepraca na odsiecz środowisku, https://www.obserwatorfinansowy.pl/bez-kategorii/rotator/telepraca-na-odsiecz-srodowisku/ [dostęp 8.03.2020].

The Global State of Information Security® Survey 2015, PWC.

Trziszka M., *Model organizacji i zarządzania systemem pracy zdalnej w branży IT*, Rozprawa doktorska, Wyd. PP, Poznań 2019.

Ustawa z dnia 24 sierpnia 2007 r. o zmianie ustawy – Kodeks pracy (Dz.U. z 2007 r. Nr 181, poz. 1288).

Wrycza S., *Informatyka ekonomiczna: podręcznik akademicki*, PWE, Warszawa 2010.

Information security in the provision of remote work

Summary: Remote work, also referred to as teleworking, involves performing tasks entrusted by the employer to be performed outside the company headquarters - usually at home. It has many advantages both from the employee's and employer's perspective. As the teleworker moves outside the parent company's headquarters, the information and IT systems necessary to do the work move. This results in a much easier materialization of information security threats. This chapter presents the essence and advantages of remote work and the main threats to information security resulting from the specifics of this form of employment. Attention was also paid to key issues related to the security of information and ICT systems.
Keywords: *information security, remote work, teleworking, information security management system (ISMS)*

Część druga

MARIA HAPUNIK
Komenda Wojewódzka Policji w Białymstoku

Zakres uprawnień służb państwowych do przetwarzania informacji w celu zapobiegania przestępstwom i ich zwalczania na przykładzie Policji

Zwalczanie zagrożeń bezpieczeństwa i zapobieganie im wymaga zastosowania przez współczesne państwo mechanizmów ochrony informacji. Działania takie przebiegają dwutorowo. Z jednej strony chroniona jest wiedza służb państwowych, która jest nieustannie zdobywana i służyć ma szeroko rozumianemu zagwarantowaniu bezpieczeństwa czy zwalczaniu przestępczości. Z drugiej strony państwo tworzy nowe gwarancje ochrony prywatności obywateli. Ciążące na ustawodawcy zobowiązanie zagwarantowania praw oraz wolności sprowadza się do zakazu nadmiernej ingerencji, dotyczy to przede wszystkim niejawnego pozyskiwania informacji, jak również na umożliwieniu swobodnego korzystania z tych wolności. Nie ulega wątpliwości, że to właśnie równowaga pomiędzy tymi gwarancjami buduje poczucie bezpieczeństwa w państwie. Wiadomo jednak, że jawność i prywatność często pozostają w konflikcie. Zarówno rozwój technologiczny, przykładowo związany z rewolucją elektroniczną, jak i przemiany społeczne są tak dynamiczne, że próg „niezbędnych" ograniczeń prywatności rzeczywiście jest trudny do określenia w dłuższej perspektywie czasowej.

Ochronę prywatności gwarantują przepisy ustawy zasadniczej, nie zaznacza się w nich jednak wprost ograniczeń, które wynikają z tytułu jawności. Artykuł 49 Konstytucji RP określa wolność i ochronę komunikowania się, w artykule 50 – „zapewnia się nienaruszalność mieszkania". Konstytucja ogranicza

rodzaj pozyskiwanych, gromadzonych i udostępnianych przez organy państwowe informacji – nie można tego czynić w stosunku do „innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym", ponadto do ich ujawnienia może zobowiązywać wyłącznie ustawa. Stwierdzenie, co oznacza „niezbędne", jest trudne przy podejmowaniu prób interpretacyjnych.

W 2018 r. w Polsce doszło do istotnych zmian w ramach regulacji prawnych dotyczących ochrony informacji oraz danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Warto na początku zwrócić uwagę na regulacje, które miały bezpośredni wpływ na obecny kształt sytemu prawnego Unii Europejskiej w tym zakresie. Organizacją, która jako pierwsza wypracowała porozumienie w zakresie ochrony danych osobowych, jest Rada Europejska. Była to Konwencja Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r.[1] Powyższa Konwencja reguluje omawiany obszar wraz z Protokołem dodatkowym o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczącym organów nadzoru i transgranicznych przepływów danych, sporządzonym w Strasburgu dnia 8 listopada 2001 r.[2] oraz Protokołem zmieniającym Konwencję Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonym w Strasburgu dnia 10 października 2018 r. Ustawa z dnia 16 października 2019 r. o ratyfikacji Protokołu zmieniającego Konwencję Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonego w Strasburgu dnia 10 października 2018 r.[3] obowiązuje od grudnia 2019 r. Prezydent RP podpisał ustawę 8 listopada 2019 r. Konwencja nr 108 została opracowana pod auspicjami Rady Europy jako pierwsza umowa międzynarodowa dotycząca ochrony danych osobowych w kontekście przestrzegania prawa do prywatności. Wprowadziła ona mechanizmy ochrony osób przed naruszeniami, jakie mogą mieć miejsce w związku z gromadzeniem i automatycznym przetwarzaniem danych osobowych oraz uregulowała kwestię przepływu danych osobowych przez granice państw. Polska stała się jej stroną 1 września 2002 r.[4] Fenomenalny rozwój technologii oraz zmiany w systemach

[1] Dz.U. z 2003 r., poz. 25.
[2] Dz.U. z 2006 r., poz. 15.
[3] Dz.U. z 2019 r., poz. 2284.
[4] https://uodo.gov.pl/pl/454 [dostęp 22.02.2020].

prawnych w odniesieniu do ochrony danych osobowych zdeterminowały istotne modernizacje w tekście konwencji nr 108. Wzmocnione zostały w niej m.in. standardy ochrony związane z przetwarzaniem danych ze względów bezpieczeństwa narodowego ze wskazaniem niezależnej oraz skutecznej kontroli i nadzoru w tym obszarze. Powyższe regulacje mają szeroki zakres podmiotowy i przedmiotowy, normujący system ochrony danych osobowych, również tych przetwarzanych przez organy ścigania i wymiar sprawiedliwości. Należy zwrócić jednak uwagę na przepis art. 9 ust. 1 oraz art. 11 konwencji nr 108, które dopuszczają wprowadzenie odstępstw od zasad ogólnych na rzecz utrzymania bezpieczeństwa publicznego oraz zwalczania przestępczości, jak również wyłączeń dla prowadzonych postępowań karnych. Podwaliny prawnej ochrony autonomii informacyjnej jednostki w systemie europejskim ukształtowała Konwencja o ochronie praw człowieka i podstawowych wolności z 4 listopada 1950 r.[5] Przepisem, który reguluje prawo do prywatności, do poszanowania życia prywatnego i rodzinnego, jak również prawo do ochrony danych osobowych, jest art. 8 Konwencji.

Poza umowami międzynarodowymi wiążącymi państwa – strony tych umów – duże znaczenie miały również rezolucje (zalecenia) Komitetu Ministrów, z których niektóre dotyczą również ochrony danych osobowych[6]. Należy postrzegać ich jako zespołu wytycznych stanowiących punkt odniesienia dla ustawodawcy tworzącego prawo krajowe i w szczególności dla krajowych organów stosujących prawo, które posługują się nimi przy dokonywaniu wykładni prawa krajowego[7]. W omawianej tematyce najbardziej istotna wydaje się Rekomendacja R (87)15 o ochronie danych osobowych wykorzystywanych w sektorze policji z dnia 17 września 1987 r., która dotyczy przetwarzania danych w systemie informatycznym (kraje członkowskie mają prawo rozszerzyć te ochronę na dane przetwarzane ręcznie). W 2018 r. komitet konsultacyjny, pracujący nad zmianami w konwencji nr 108, opracował praktyczny przewodnik w sprawie wykorzystywania danych osobowych w sektorze policji[8]. Rekomendację kilkukrotnie oceniano pod

[5] Dz.U. z 1993 r., poz. 284 ze zm.

[6] *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, red. A. Grzelak, Wyd. C.H.Beck, Warszawa 2019, s. 8.

[7] Tamże.

[8] Zob. dokument z dnia 15 lutego 2018 r. T-PD(2018)01, Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data,

kątem jej modernizacji, jednak uznano, że nie ma potrzeby wprowadzania do niej znaczących zmian. Według omawianego zalecenia dane zbierane na potrzeby policji powinny być ograniczone w niezbędnym zakresie w celu zapobiegania konkretnemu niebezpieczeństwu bądź zwalczania konkretnego przestępstwa. Ponadto zwrócono uwagę na konieczności oddzielenia zbiorów danych opartych na faktach od danych, które opierają się na subiektywnych opiniach i indywidualnych ocenach. W rekomendacji istnieje również zalecenie, aby przetwarzanie danych osobowych w Policji nadzorował niezależny organ.

Rozwój systemu ochrony danych osobowych w Unii Europejskiej (wcześniej Wspólnoty Europejskiej) był ograniczony ze względu na jej strukturę oraz odmienności systemu prawnego. Regulacje tego obszaru w zakresie współpracy sądowej i policyjnej obejmował filar III, natomiast przetwarzanie danych osobowych zostało uregulowane w obszarze podlegającym zasadom I filaru Unii Europejskiej, które wynikały z dyrektywy ogólnej w sprawie ochrony danych (dyrektywa 95/46/WE). Od momentu jej przyjęcia ukształtowało się całe acquis: prawodawstwo [można w tym miejscu wymienić dyrektywy szczegółowe, regulujące problematykę ochrony danych w szczególnych obszarach, jak np. dyrektywę 2000/31/WE Parlamentu Europejskiego i Rady z 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)[9], czy chociażby dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)][10], przez instytucje [Grupa Robocza 29 (obecnie to Europejska Rada Ochrony Danych – EROD)] czy też Europejski Inspektor Ochrony Danych (EIOD)], zostało też wypracowane orzecznictwo Trybunału Sprawiedliwości[11]. Nie należy pomijać regulacji odnoszących się do Systemu Informacyjnego Schengen drugiej generacji (SIS II)[12], europejskiego nakazu

Practical guide on the use of personal data in the police sector, https://rm.coe.int/practical-guide-use-of-personal-data-in-the-police-sector/1680789a74 [dostęp 24.02.2020].

[9] Dz.Urz. UE L 178 z 17.07.2000 r., s. 1.

[10] Dz.Urz. UE L 201 z 31.07.2002 r. ze zm., s. 37.

[11] *Ustawa o ochronie…*, red. A. Grzelak, dz. cyt., s. 10.

[12] Rozporządzenie (WE) nr 1987/2006 – utworzenie, funkcjonowanie i użytkowanie Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz. UE L 381 z 28.12.2006 r.), s. 4, Decyzja

aresztowania (ENA)[13], Europolu[14], Eurojustu[15] czy dyrektywy PNR[16]. W 2008 r. przyjęta została Decyzja ramowa Rady 2008/977/WSiSW z 27.11.2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych[17]. Akt prawny regulował zasady przetwarzania danych osobowych w relacjach transgranicznych pomiędzy państwami Unii Europejskiej. Dyrektywa nie regulowała form przetwarzania danych, miała ogólny charakter, pomimo innych pierwotnych założeń powstałych w obliczu potrzeb wprowadzenia znowelizowanych regulacji jako odpowiedzi na nowe metody przetwarzania i nowe formy współpracy pomiędzy organami UE. Omawiana dyrektywa w Polsce została implementowana Ustawą z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi[18], znacząco zmienioną po wejściu w życie Ustawy z dnia 10 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[19].

Wejście w życie w dniu 1 grudnia 2009 r. Traktatu z Lizbony[20] pozwoliło państwom członkowskim na bardziej równomierny rozwój współpracy w dziedzinie zarówno systemu ochrony, jak i dostępu uprawnionych służb do informacji i danych osobowych. Należy zwrócić uwagę, że to dzięki zniesieniu struktury

2007/533/WSiSW – utworzenie, funkcjonowanie i użytkowanie Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz. UE L 205 z 07.08.2007 r.), s. 63.

[13] Decyzja ramowa Rady z dn. 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między Państwami Członkowskimi (Dz.Urz. WE L 190 z 18.7.2002 r.), s. 1.

[14] Konwencja sporządzona na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie ustanowienia Europejskiego Urzędu Policji (Konwencja o Europolu), sporządzona w Brukseli dnia 26 lipca 1995 r. (Dz.U. z 2005 r. Nr 29, poz. 243).

[15] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1727 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) oraz zastąpienia i uchylenia decyzji Rady 2002/187/WSiSW (Dz.Urz. UE L 295 z 21.11.2018 r.), s. 138.

[16] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.Urz. UE L 119 z 4 maja 2016 r.), s. 3.

[17] Dz.Urz. UE L 350 z 30.12.2008 r., s. 60.

[18] Dz.U. z 2018 r., poz. 484 ze zm.

[19] Dz.U. z 2019 r., poz. 125.

[20] Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską (Dz.Urz. C 306 z 17.12.2007 r.).

trójfilarowej ustanowiona została jedna wspólna podstawa dla ochrony danych osobowych. System filarowy został zastąpiony jednolitym reżimem prawnym, Unia uzyskała osobowość prawną. Do Traktatu o funkcjonowaniu Unii Europejskiej[21] wprowadzony został art. 16, który zagwarantował zmiany systemowe w omawianym obszarze, przede wszystkim ustanawiając indywidualne prawo podmiotu danych do ochrony jego danych osobowych. Wejście w życie Traktatu z Lizbony spowodowało nadanie statusu prawa pierwotnego Karcie Praw Podstawowych Unii Europejskiej (dalej: KPP), przyznano jej charakter prawnie wiążący. KPP została proklamowana w Nicei w dniu 7 grudnia 2000 r. Po wejściu w życie Traktatu z Lizbony jej pierwotną wersję poddano redakcji, a następnie została ona ponownie uchwalona przez Komisję Europejską, Radę i Parlament Europejski. Postanowienia dotyczące ochrony autonomii informacyjnej jednostki zawarte są w art. 7 i 8 KPP. Prawo do ochrony danych osobowych jest niezmiennie związane z prawem do poszanowania życia prywatnego ustanowionym w art. 7 KPP. Treść art. 8 KPP oparta jest – jak wynika z objaśnień Sekretariatu Konwencji redagującej KPP – na tekście art. 16 TFUE, Dyrektywie 95/46/WE, art. 8 EKPCz oraz konwencji nr 108[22]. Jednocześnie stwierdza się tam dość lakonicznie, że Dyrektywa 95/46/WE i Rozporządzenie (WE) 45/2001 „zawierają warunki i ograniczenia stosowane w wykonywaniu prawa do ochrony danych osobowych”[23]. Wspomniane powyżej artykuły 8 KPP oraz 16 TFUE stanowiły podstawę prawną do przyjęcia nowych norm w zakresie ochrony danych osobowych, dotyczących współpracy policyjnej i sądowej w sprawach karnych. Komisja, przygotowując projekt dyrektywy, w związku z treścią deklaracji nr 21[24], miała do wyboru dwie opcje: albo mogła przedstawić jeden, spójny, ustanawiający standardy tekst, który będzie określał zasady ogólne przetwarzania danych w UE, albo – odmiennie – kontynuować rozróżnienie między podejściem ogólnym a podejściem szczególnym dla spraw związanych z bezpieczeństwem wewnętrznym i zwalczaniem

[21] Dz.Urz. UE 2016 C 202, s. 1.

[22] A. Gajda, *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace” / OW SGH 2014, nr 4, s. 77.

[23] Tamże.

[24] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”, COM(2010)609 final.

przestępczości[25]. Komisja zdecydowała się na drugi wybór ze względu na szczególny charakter regulowanego obszaru. Przemawiały za tym różne potrzeby, w tym przechowywanie danych przez długi czas, konieczność porównywania i analizowania posiadanych danych z napływającymi, czy zagwarantowanie braku dostępu do informacji określonej grupie osób do danych na swój temat, np. osobom podejrzanym. Ponadto uregulowanie zasad ochrony danych osobowych w dwóch aktach prawnych – rozporządzeniu i dyrektywie – uwzględniło zwiększony margines swobody państw członkowskich UE w kształtowaniu regulacji dotyczących funkcjonowania organów państwowych zwalczających przestępczość. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW[26] uchwalona została w tym samym dniu, razem z RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[27]. Termin implementacji dyrektywy został wyznaczony na 5 maja 2016 r., lecz polski ustawodawca nie dotrzymał tego terminu, uchwalając ustawę o ochronie danych osobowych przetwarzanych w związku ze zwalczaniem i zapobieganiem przestępczości w dniu 14.12.2018 r[28].

Transpozycja dyrektywy 2016/680 nie mogła polegać wyłącznie na uchwaleniu powyższej ustawy, koniecznym było wprowadzenie licznych zmian w przepisach sektorowych. W rozdziale 9 ustawy o ochronie danych osobowych przetwarzanych w związku ze zwalczaniem i zapobieganiem przestępczości zawarto przepisy zmieniające 42 ustawy. W większości zmienianych ustaw dostosowuje się legislacyjnie przepisy do zmian w zakresie funkcjonowania Prezesa

[25] *Ustawa o ochronie…*, red. A. Grzelak, dz. cyt., s. 17-18.
[26] Dz.Urz. UE L 194 z 19.07.2016 r., s. 1.
[27] Dz.Urz. UE L 119 z 04.05.2016 r., s. 1 ze zm.
[28] Dz.U. z 2019 r., poz. 125.

UODO oraz prawidłowych odesłań do aktualnie obowiązujących ustaw[29]. Poza tym jednak uchwalone zmiany dotyczą przede wszystkim wskazania administratora, okresu retencji danych, nadzoru nad przetwarzaniem danych czy wyłączenia stosowania niektórych przepisów RODO[30]. Największy zakres obejmują zmiany w Ustawie z dnia 6 kwietnia 1990 r. o Policji[31], zawarte w art. 58 omawianej ustawy. Znowelizowany został art. 1 ust. 2 pkt 8, który ustanawia podstawowe zadanie Policji do przetwarzania informacji kryminalnych, w tym danych osobowych. Kompetencję tę wprost wymienia art. 20 ust. 1 ustawy o Policji: „W celu realizacji zadań ustawowych Policja jest uprawniona do przetwarzania informacji, w tym danych osobowych, z zachowaniem ograniczeń wynikających z art. 19 (zarządzenie kontroli operacyjnej)".

Przetwarzanie informacji, w tym danych osobowych, może odbywać się za pomocą środków technicznych, zakres danych określa art. 14 ust. 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Policja ma prawo przetwarzać dane osobowe, o których mowa w art. 9 i 10 RODO, wyłączając dane dotyczące kodu genetycznego. Omawiana ustawa dodaje przepisy, które pozwalają Policji w ramach wykonywanych czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych i administracyjno-porządkowych (art. 15 ust. 1 pkt 5a) obserwować i rejestrować przy użyciu środków technicznych obrazy zdarzeń w miejscach publicznych, a w przypadku czynności operacyjno-rozpoznawczych i administracyjno-porządkowych podejmowanych na podstawie ustawy – także i dźwięk towarzyszący tym zdarzeniom (art. 15 ust. 1 pkt 5b[32]). Policjanci mogą obserwować i rejestrować przy użyciu środków technicznych obraz lub dźwięk w trakcie interwencji w miejscach innych niż publiczne, podczas prowadzenia działań kontrterrorystycznych oraz wspierania działań jednostek organizacyjnych Policji przez służbę kontrterrorystyczną w warunkach szczególnego zagrożenia lub wymagających użycia specjalistycznych sił i środków oraz specjalistycznej taktyki działań, a także w policyjnych środkach transportu. Okres przechowywania danych, uzyskanych podczas

[29] *Ustawa o ochronie*..., red. A. Grzelak, dz. cyt., s. 511.
[30] Tamże.
[31] Dz.U. z 2020 r., poz. 360.
[32] Art. 58 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r., poz. 125).

wykonywania czynności, o których mowa w art. 15 ust. 1 pkt 5a i 5 b ustawy o Policji, to co najmniej 30 dni, nie dłużej jednak niż 60 dni od dnia ich zarejestrowania. Informacje uzyskane podczas czynności operacyjno-rozpoznawczych podlegają zniszczeniu po okresie przechowywania do 60 dni, z tym, że termin przechowywania liczy się od dnia zakończenia tych czynności. Kolejna istotna zmiana to nadanie uprawnienia do pobierania i udostępniania danych telekomunikacyjnych, pocztowych i internetowych także organom ścigania państw członkowskich UE i innych państw, agencjom UE, które zajmują się zapobieganiem i zwalczaniem przestępczości oraz Międzynarodowej Organizacji Policji Kryminalnej – Interpolu, na ich wniosek, jeżeli następuje to w celu wykrywania przestępstw oraz ścigania ich sprawców, ratowania zdrowia lub życia ludzkiego albo poszukiwania osób zaginionych (art. 20 c ust. 8 ustawy o Policji).

Efektywne wypełnianie zadań ustawowych w zakresie zapobiegania i zwalczania przestępczości przez Policję jest zależne od możliwości dysponowania przez tę służbę odpowiednim zasobem informacji. Trzon uprawnień Policji stanowią przepisy art. 15 oraz 19-21nb. Szczególnym uprawnieniem Policji jest prowadzenie czynności operacyjno-rozpoznawczych, które poprzedzają co do zasady postępowanie przygotowawcze, gdy stanowią podstawę do jego wszczęcia, jak również często prowadzone są równolegle do tego postępowania. Czynności te można prowadzić także po umorzeniu postępowania przygotowawczego na podstawie przepisu art. 325f §2 k.p.ksgj.pl (niewykrycie sprawców).

Czynności operacyjno-rozpoznawcze umocowane są ustawą o Policji oraz w niejawnym zarządzeniu nr pf – 1 Komendanta Głównego Policji z dnia 3 stycznia 2019 r. w sprawie metod i form wykonywanych przez Policję czynności operacyjno-rozpoznawczych (niepublikowane). Prawo podejmowania czynności operacyjno-rozpoznawczych przysługuje Policji na podstawie art. 14 ust. 1 ustawy o Policji: „W granicach swych zadań Policja wykonuje czynności: operacyjno-rozpoznawcze, dochodzeniowo-śledcze i administracyjno-porządkowe w celu: rozpoznawania, zapobiegania i wykrywania przestępstw, przestępstw skarbowych i wykroczeń; poszukiwania osób ukrywających się przed organami ścigania lub wymiaru sprawiedliwości, zwanych dalej »osobami poszukiwanymi«; poszukiwania osób, które na skutek wystąpienia zdarzenia uniemożliwiającego ustalenie miejsca ich pobytu należy odnaleźć w celu zapewnienia ochrony ich życia, zdrowia lub wolności, zwanych dalej »osobami zaginionymi«".

Do ustawowo uregulowanych czynności operacyjno-rozpoznawczych zaliczyć należy przepisy art. 19 ust. 1 – kontrola operacyjna, art. 19a – zakup kontrolowany, kontrolowane wręczenie lub przyjęcie korzyści i sprzedaż kontrolowana, art. 19b – przesyłka niejawnie nadzorowana oraz art. 20c – żądanie od przedsiębiorców telekomunikacyjnych danych retencyjnych. Do uregulowanych w ustawie o Policji czynności operacyjno-rozpoznawczych zaliczyć trzeba także wykorzystanie dokumentów legalizacyjnych – art. 20a oraz art. 22 – współpraca z osobami niebędącymi policjantami, udzielającymi pomocy Policji.

Pozyskiwanie przez nieuprawnione osoby (czy to ze służb wywiadowczych innego państwa, czy grup przestępczych) informacji, które mają wpływ na bezpieczeństwo danego państwa (czyli jego niepodległość, suwerenność oraz pozycję na arenie międzynarodowej), może mieć daleko idące konsekwencje[33]. Dlatego, by zachować stabilność państwa i dawać poczucie bezpieczeństwa obywatelom, najważniejszym obowiązkiem rządu jest ochrona informacji[34]. Współcześnie informacja przekazywana jest niezwykle szybko i w dodatku do nieograniczonej liczby odbiorców. Nowe normy prawne chroniące informację powstają z opóźnieniem w stosunku do rozwoju technologii informacyjno-komunikacyjnych. Obecnie zasoby informacji chronione są szczególnie w kontekście podejmowania decyzji algorytmicznych, które są istotne w związku z rozwojem w krajach rozwiniętych sztucznej inteligencji. W stosunku do obywateli źródłami zagrożenia są cyberprzestępcy zajmujący się „kradzieżą" cudzej tożsamości czy firmy profilujące konsumentów. Nie ustaje również dyskusja kontestująca legalne działania służb państwowych wykorzystujących potencjał ICT[35] do swoich potrzeb. Niedopuszczalne jest, by służby państwowe działały na szkodę obywateli, dlatego tak ważna jest kwestia kontroli ich działalności i nadzoru nad nimi.

Informacja jest zatem produktem cennym, chronionym zarówno systemami fizycznymi jak i teleinformatycznymi. Państwo rozszerza normy prawne zabezpieczające prywatność obywateli, jednak skuteczna walka z szeroko pojętymi zagrożeniami wymaga dostępu służb państwowych do tajemnic. Wkraczanie w strefę wolności i praw człowieka jest możliwe wyłącznie na podstawie ustaw kompetencyjnych poszczególnych służb państwowych oraz ich niejawnych instrukcji.

[33] S. Topolewski, *Ochrona informacji niejawnych w Siłach Zbrojnych Rzeczypospolitej Polskiej*, Wyd. Nauk. UPH, Siedlce 2017, s. 353.
[34] Tamże.
[35] ICT – technologie informacyjno-komunikacyjne.

W Dokumencie roboczym nr 1 w sprawie amerykańskich i unijnych programów nadzoru oraz ich wpływu na podstawowe prawa obywateli UE stwierdza się, że „postęp techniczny jest jednym z czynników mających wpływ na zasadniczą zmianę modelu działania i praktyk służb specjalnych, które odeszły od tradycyjnej koncepcji ukierunkowanego nadzoru, stanowiącego konieczny i proporcjonalny środek zwalczania terroryzmu, i skierowały się ku systemom nadzoru prowadzonego na skalę masową”[36]. Zdaniem autorki nie jest możliwe zapobieganie i zwalczanie zagrożeń bez szerokich uprawnień służb państwowych, szczególnie biorąc pod uwagę rozwój cyberprzestrzeni. Skuteczność służb nie jest możliwa bez odpowiednich norm prawnych, narzędzi oraz specjalistycznie wykształconej kadry. W Polsce istnieje przestrzeń w działaniu państwa, którą powinna zapełnić służba specjalna do prowadzenia wywiadu zarówno CYBER HUMINT, jak i SIGINT. Według doniesień prasowych[37] jest szansa, aby taka służba specjalna, zajmująca się wywiadem elektronicznym i cyberbezpieczeństwem kraju, powstała. Współcześnie służby państwowe gromadzą i wykorzystują informacje nie tylko przedstawiające wartość dowodową w prowadzonych postępowaniach. W ramach proaktywnych strategii, prowadzonych w związku z działaniami kontr- i antyterrorystycznymi czy ze zwalczaniem przestępczości zorganizowanej dane zbierane są prewencyjnie. Oczywiście dyskusja na temat równoważenia działań inwigilacyjnych i chroniących prywatność obywateli jest potrzebna. To dzięki protestom, m.in. organizacji pozarządowych, służby państwowe są poddane koniecznej w państwie demokratycznym kontroli społecznej.

Bibliografia

Akty prawne

Decyzja 2007/533/WSiSW – utworzenie, funkcjonowanie i użytkowanie Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz. UE L 205 z 07.08.2007 r.).

Decyzja ramowa Rady 2008/977/WSiSW z 27.11.2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.Urz. UE L 350 z 30.12.2008 r.).

[36] Parlament Europejski, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, Sprawozdawca Claude Moraes, 11.12.2013 r. (DT\1012434PL.doc), s. 2.

[37] https://forsal.pl/artykuly/906998,nowa-sluzba-specjalna-w-polsce-wywiad-elektroniczny-nasluch-radioelektroniczny-program-pis.html [dostęp 28.03.2020].

Decyzja ramowa Rady z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między Państwami Członkowskimi (Dz.Urz. WE L 190 z 18.7.2002 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 194 z 19.07.2016 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.Urz. UE L 119 z 4 maja 2016 r.).

Konwencja Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r.

Konwencja sporządzona na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie ustanowienia Europejskiego Urzędu Policji (Konwencja o Europolu), sporządzona w Brukseli dnia 26 lipca 1995 r. (Dz.U. z 2005 r. Nr 29, poz. 243).

Protokół dodatkowy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych, sporządzony w Strasburgu 8 listopada 2001 r. (Dz.U. z 2006 r., poz. 15).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016 r. ze zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1727 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) oraz zastąpienia i uchylenia decyzji Rady 2002/187/WSiSW (Dz.Urz. UE L 295 z 21.11.2018 r.).

Rozporządzenie (WE) nr 1987/2006 – utworzenie, funkcjonowanie i użytkowanie Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz. UE L 381 z 28.12.2006 r.).

Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE z 2016 r. C 202).

Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie 13 grudnia 2007 (Dz.Urz. UE z 2007 r. C 306/1).

Ustawa z dnia 16 października 2019 r. o ratyfikacji Protokołu zmieniającego Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonego w Strasburgu dnia 10 października 2018 r. (Dz.U. z 2019 r., poz. 2284).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2020 r., poz. 360).

Ustawa z dnia 10 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r., poz. 125).

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

Ustawa z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz.U. z 2018 r., poz. 484 ze zm.).

Dokumenty

Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data – Practical guide on the use of personal data in the police sector, dokument z dnia 15 lutego 2018 r. T-PD(2018)01, https://rm.coe.int/practical-guide-use-of-personal-data-in-the-police-sector/16807 89a74.

Dokument roboczy nr 1 w sprawie amerykańskich i unijnych programów nadzoru oraz ich wpływu na podstawowe prawa obywateli UE Parlament Europejski, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, Sprawozdawca Claude Moraes, 11.12.2013 r. (DT\1012434PL.doc).

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", COM(2010)609 final.

Opracowania

Gajda A., *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace" / OW SGH 2014, nr 4.

Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz, red. A. Grzelak, Wyd. C.H. Beck, Warszawa 2019.

Topolewski S., *Ochrona informacji niejawnych w Siłach Zbrojnych Rzeczypospolitej Polskiej*, Wyd. Nauk. UPH, Siedlce 2017.

Źródła internetowe

https://forsal.pl/artykuly/906998,nowa-sluzba-specjalna-w-polsce-wywiad-elektroniczny-nasluch-radioelektroniczny-program-pis.html [dostęp 28.03.2020].

https://uodo.gov.pl/pl/454 [dostęp 22.02.2020].

https://rm.coe.int/practical-guide-use-of-personal-data-in-the-police-sector/1680789a74 [dostęp 24.02.2020].

The scope of powers of law enforcement to process information in order to determine and fight crime

Summary: The purpose of this article is to present normative elements concerning national law enforcement information processing, including personal data, to prevent and combat crime. Legal acts regulating information processing in activities of state services are discussed, using the Police as a case study. The author tries to underline the necessity of surveillance activities undertaken by state services in situations of largely understood threats prevention.

Keywords: *security, personal data protection, data processing by police, crime prevention, police intelligence operations*

JOWITA SOBCZAK

Akademia Finansów i Biznesu Vistula

Obowiązek zgłaszania naruszeń ochrony danych osobowych w jednostkach organizacyjnych

Ostatnie zmiany legislacyjne w obszarze ochrony danych osobowych pokazały, że ochrona danych to dla wielu podmiotów priorytet w prowadzeniu działalności gospodarczej. Przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („ogólne rozporządzenie o ochronie danych osobowych", „RODO") obligują wszystkie jednostki organizacyjne, które przetwarzają dane osobowe, do ochrony tych danych oraz ustanawiania odpowiednich zabezpieczeń określonych w powyższym rozporządzeniu.

Obowiązek zgłaszania naruszeń organowi nadzorczemu, czyli Prezesowi Urzędu Ochrony Danych Osobowych (PUODO), został wprowadzony na mocy przepisów ogólnego rozporządzenia o ochronie danych osobowych, które weszło w życie 25 maja 2018 r. Naruszenia ochrony danych osobowych przez wiele lat były skrupulatnie utrzymywane w tajemnicy przez jednostki organizacyjne, w których takie naruszenie wystąpiło (nie istniał obowiązek ich ujawniania). Wyjątek stanowili przedsiębiorcy usług telekomunikacyjnych, którzy w świetle przepisów prawa telekomunikacyjnego zobligowani byli, w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, powiadomić o tym właściwy organ

do spraw ochrony danych osobowych[1], a także abonenta lub użytkownika końcowego, w przypadku którego tajemnica danych została naruszona.

Przepisy art. 33 ogólnego rozporządzenia o ochronie danych zobligowały wszystkie podmioty przetwarzające dane osobowe do zgłaszania przypadków naruszenia ochrony danych osobowych, w tym praw i wolności osób, których dane dotyczą, do organu nadzorczego (PUODO). Istotne jest, aby administratorzy danych[2] w procesie związanym ze zgłaszaniem naruszenia ochrony danych posiadali odpowiednie narzędzia umożliwiające im szybką reakcję na zdarzenie, zarówno wobec organu nadzorczego jak i osób, których dane dotyczą. W celu zapewnienia działania bez zbędnej zwłoki jednostki organizacyjne powinny opracować i wdrożyć procedury postępowania na wypadek wystąpienia naruszenia ochrony danych, które mogą znacznie usprawnić i przyspieszyć działania w przypadku wykrycia takiego naruszenia.

Pojęcie naruszenia ochrony danych osobowych

Przepisy ogólnego rozporządzenia o ochronie danych osobowych wprowadzają legalną definicję pojęcia „naruszenie ochrony danych osobowych". Termin ten zgodnie z art. 4 pkt 12 RODO oznacza „przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych". Oznacza to, że naruszenia mogą odnieść się do różnych czynności przetwarzania danych, a w szczególności ich przechowywania bądź przesyłania[3]. Naruszenie może być rodzajem incydentu bezpieczeństwa. Jednocześnie P. Fajgielski wyjaśnia, że naruszenie bezpieczeństwa można uznać

[1] Przed 25 maja 2018 r. organem do spraw ochrony danych osobowych był Generalny Inspektor Ochrony Danych Osobowych.

[2] Zgodnie z art. 4 pkt 7 RODO administrator danych oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

[3] P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Wyd. C.H.Beck, Warszawa 2018, s. 508.

za naruszenie danych osobowych[4]. Warto przypomnieć, że incydentem bezpieczeństwa, zgodnie z normą ISO/IEC 27001[5], będzie pojedyncze zdarzenie lub seria niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. Przepisy ogólnego rozporządzenia o ochronie danych osobowych mają zastosowanie wyłącznie w sytuacji, gdy dochodzi do naruszenia ochrony danych osobowych. Wystąpienie takiego naruszenia prowadzi do sytuacji, w której podmiot nie jest w stanie zapewnić zgodności z zasadami dotyczącymi przetwarzania danych osobowych określonymi w art. 5 RODO. Pozwala to odróżnić incydent bezpieczeństwa od zdarzenia skutkującego naruszeniem ochrony danych osobowych[6]. Naruszenie ochrony danych musi spełniać łącznie trzy przesłanki:

1) dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez jednostkę organizacyjną, której dotyczy naruszenie;
2) skutkiem naruszenia może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych;
3) naruszenie jest skutkiem złamania zasad bezpieczeństwa danych osobowych.

Grupa Robocza Artykuł 29[7] w Wytycznych dotyczących zgłaszania naruszeń ochrony danych osobowych[8] wyróżnia trzy typy naruszeń ochrony danych:

[4] P. Fajgielski, *Informowanie o naruszeniu ochrony danych osobowych w świetle przepisów ogólnego rozporządzenia o ochronie danych*, „Monitor Prawniczy" 2016, nr 20, 2016.
[5] PN-EN ISO/IEC 27001:2017 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.
[6] Zob. także: Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250 rev.01), s. 6.
[7] Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołana została na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych jako niezależny podmiot o charakterze doradczym. Grupa ta została rozwiązana 25 maja 2018 r., a w jej miejsce została powołana Europejska Rada Ochrony Danych.
[8] Tamże, s. 7.

1) Naruszenie poufności danych – występuje w przypadku nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Przykładowo naruszeniem takim będzie umożliwienie osobie nieuprawnionej wglądu do dokumentów zawierających dane osobowe.
2) Naruszenie integralności danych – dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych, np. pracownik zmienia imiona klientów w systemie informatycznym przetwarzającym.
3) Naruszenie dostępności danych – dochodzi do przypadkowej lub nieuprawnionej utraty dostępu do danych osobowych lub zniszczenia danych osobowych. Przykładem utraty dostępności będzie sytuacja, w której doszło do przypadkowego usunięcia danych albo ich usunięcia przez nieuprawnioną osobę, jeżeli doprowadziło ono do trwałej utraty lub zniszczenia tych danych. Do utraty dostępności może dojść również wskutek awarii systemu zasilania lub zainfekowania systemu informatycznego/oprogramowania „złośliwym" oprogramowaniem.

Warto podkreślić, że – w zależności od okoliczności – naruszenie może dotyczyć jednocześnie poufności, integralności i dostępności danych, a także dowolnego połączenia dwóch spośród tych trzech kategorii naruszeń.

Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu

Obowiązek zgłaszania naruszeń ochrony danych osobowych wynika z przepisów ogólnego rozporządzenie o ochronie danych, który w art. 33 określa, że „w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu […] chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych".

Stwierdzenie wystąpienia naruszenia bezpieczeństwa danych osobowych następuje w momencie, w którym administrator uzyskuje wystarczającą wiedzę potwierdzającą tego typu zdarzenie. Warto podkreślić, że administrator danych nie zawsze może zgłosić naruszenie w wyznaczonym terminie. Dokonanie zgłoszenia z opóźnieniem, czyli po upływie 72 godzin, może być w niektórych

przypadkach akceptowane przez organ nadzorczy (PUODO), ale podmiot zgłaszający naruszenie musi dołączyć stosowne wyjaśnienie przyczyn i okoliczności takiego opóźnienia.

Po stwierdzeniu naruszenia administrator danych powinien ocenić prawdopodobne ryzyko, na jakie narażone są osoby fizyczne, aby ustalić, czy w danym przypadku zastosowanie ma wymóg zgłoszenia takiego naruszenia, a także aby określić działania, które należy podjąć, aby zaradzić temu naruszeniu. Dlatego bardzo ważne jest, aby administrator danych posiadał odpowiednią dokumentację wewnętrzną, np. procedury dotyczące zgłaszania naruszeń. Zgodnie z zaleceniami Prezesa Urzędu Ochrony Danych Osobowych taka procedura powinna zawierać:

- cel, w jakim procedura została opracowana;
- zakres jej stosowania;
- katalog ewentualnych potencjalnych zagrożeń i naruszeń, które mogą się pojawić w danej jednostce organizacyjnej;
- opis etapów zarządzania naruszeniami;
- opis postępowania personelu administratora danych w przypadku wystąpienia naruszenia ochrony danych osobowych[9].

Administrator danych powinien zapoznać z tą procedurą personel oraz wszystkie inne osoby zaangażowane w przetwarzanie danych w jednostce organizacyjnej, np. podczas szkolenia z zakresu ochrony danych. Pracownicy powinni wiedzieć komu i w jakich okolicznościach należy zgłaszać zdarzenie naruszenia ochrony danych osobowych oraz jak mają postępować w takiej sytuacji. Dlatego też administrator danych powinien ustanowić wewnętrzne zasady wykrywania naruszenia i zaradzenia mu. Zgodnie z motywem 87 ogólnego rozporządzenia o ochronie danych administrator danych powinien upewnić się, czy zastosował wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by móc możliwie jak najszybciej stwierdzić naruszenie ochrony danych osobowych i w wyznaczonym terminie (72 godziny) poinformować organ nadzorczy (PUODO) oraz, jeśli zajdzie taka potrzeba, osobę, której dane dotyczą. To, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem

[9] Zob. także: Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, Urząd Ochrony Danych Osobowych, wersja 1.0, czerwiec 2019, s. 5.

w szczególności charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą. Takie zawiadomienie może skutkować interwencją Prezesa Urzędu Ochrony Danych Osobowych.

W sytuacji, kiedy administrator danych przeprowadził już stosowną analizę w celu ustalenia okoliczności naruszenia ochrony danych osobowych, dokonuje zgłoszenia na formularzu określonym przez PUODO, który dostępny jest na stronie internetowej tego organu. Tak jak wskazano wyżej, kluczowa dla każdego zgłoszenia naruszenia jest ochrona praw i wolności osób, których dane dotyczą, dlatego niezwykle ważny jest szybki czas reakcji administratora danych na zdarzenie. Warto podkreślić, że przepisy ogólnego rozporządzenia o ochronie danych osobowych przewidują dwa rodzaje obowiązków związanych ze zgłaszaniem naruszeń ochrony danych osobowych:

- zgłoszenie przez administratora danych organowi nadzorczemu;
- zgłoszenie przez podmiot przetwarzający[10] administratorowi danych.

Oznacza to, że podmiot, który przetwarza dane osobowe na zlecenie administratora danych (np. podmiot prowadzący obsługę księgową administratora, usługi archiwum czy usługi IT), po stwierdzeniu naruszenia bezpieczeństwa danych osobowych bez zbędnej zwłoki zobligowany jest zgłosić takie naruszenie administratorowi danych. Dotyczy to także dostawców usług chmurowych, którzy bardzo często korzystają z serwerów położonych w wielu krajach, w tym w państwach trzecich[11]. Ogólne rozporządzenie o ochronie danych zobowiązuje podmiot przetwarzający do wspierania administratora danych w realizacji obowiązku zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych, np. poprzez udzielenie dostępnych mu w danej sprawie informacji. Dlatego bardzo ważnym elementem umowy z podmiotem przetwarzającym, który będzie wykonywał zadania związane z przetwarzaniem danych na rzecz administratora danych, są odpowiednio skonstruowane zabezpieczenia prawne w umowie dotyczące

[10] Zgodnie z art. 4 pkt 8 RODO przez podmiot przetwarzający należy rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

[11] Zob. także: J. Sobczak, *Realizacja usługi przetwarzania danych osobowych w chmurze obliczeniowej*, [w:] *Informacje prawnie chronione – wybrane zagadnienia*, red. S. Topolewski, Wyd. Nauk. UPH, Sieldce, 2019, s. 121.

zgłaszania naruszeń ochrony danych przez podmiot przetwarzający: tak, aby administrator danych mógł wywiązać się z obowiązku na nim spoczywającym w zakresie zgłoszenia naruszania do PUODO w terminie przewidzianym w ogólnym rozporządzeniu o ochronie danych, tj. 72 godzin po stwierdzeniu naruszenia. Najczęściej zastrzeżenia dotyczące terminu zgłaszania naruszeń ochrony danych osobowych przez podmiot przetwarzający wskazane są w umowie powierzenia, o której mowa w art. 28 RODO. Bowiem w przypadku, gdy administrator danych zdecyduje się na powierzenie przetwarzania danych osobowych, zobligowany jest podjąć odpowiednie zabezpieczenia, m.in. zawrzeć stosowna umowę powierzenia z podmiotem. Umowa powierzenia przetwarzania powinna zawierać w szczególności:

1) przedmiot przetwarzania – będzie on powiązany z realizacją przedmiotu umowy głównej zawartej pomiędzy administratorem danych a podmiotem przetwarzającym, np. outsourcing działań marketingowych, gdy dla ich wykonania konieczne jest przetwarzanie danych osobowych;
2) czas trwania przetwarzania – co do zasady powiązany z realizacją przedmiotu umowy;
3) charakter przetwarzania;
4) cel przetwarzania – określenie, dlaczego podmiot przetwarzający ma przetwarzać dane osobowe w imieniu administratora;
5) kategorię danych osobowych – wymienienie, jakie konkretnie dane osobowe będą podlegały powierzeniu przy uwzględnieniu podziału na dane zwykłe (przykładowo wymienione w art. 4 pkt 1 RODO) oraz dane szczególnych kategorii (katalog zawarty w art. 9 ust. 1 RODO);
6) kategorię osób, których dane dotyczą – sprecyzowanie grupy osób, których dane zostały powierzone do przetwarzania, np. dane klientów, dane pracowników.

Praktycznym rozwiązaniem w przypadku obowiązku zgłaszania naruszeń ochrony danych osobowych przez podmiot przetwarzający jest opracowanie przez administratora odpowiedniej procedury, która może stanowić załącznik do umowy. Przepisy dotyczące obowiązku zgłaszania naruszeń ochrony danych przez podmiot przetwarzający mogą być z praktycznego i prawnego punkt widzenia niewystarczające. Jeżeli podmiot przetwarzający świadczy usługi na rzecz kilku administratorów, a naruszenie wywiera wpływ na wszystkich z nich, podmiot

przetwarzający będzie zobowiązany do zgłoszenia wystąpienia wspomnianego naruszenia każdemu z tych administratorów. Warto podkreślić, że zasady zgłaszania naruszeń przez podmiot przetwarzający powinny być dostarczone i przekazane wszystkim osobom zaangażowanym w realizację umowy. Administratorzy danych oraz podmioty przetwarzające powinni propagować kulturę ochrony danych osobowych w organizacjach oraz przeprowadzać regularne szkolenia w tym zakresie.

Grupa Robocza Artykuł 29 w swoich Wytycznych dotyczących zgłaszania naruszeń ochrony danych osobowych przedstawiła propozycje postępowania w przypadku zaistnienia naruszenia ochrony danych osobowych. Według niej poniższe zasady powinny być uwzględniane we wszystkich przypadkach wystąpienia naruszeń:

1) Informacje na temat wszystkich zdarzeń powiązanych z ochroną danych powinny być przekazywane w szczególności osobom, którym powierzono zadanie reagowania na naruszenia.
2) Należy wyznaczyć w jednostce organizacyjnej osobę odpowiedzialną za ustalanie zaistnienia naruszenia i dokonania oceny poziomu ryzyka.
3) Ocena ryzyka dla osób fizycznych związana z danym naruszeniem powinna być przekazywana odpowiednim komórkom organizacyjnym w ramach danej organizacji.
4) W razie konieczności (po dokonaniu oceny) należy zgłosić dane naruszenie organowi nadzorczemu (podmiot przetwarzający zgłasza je do administratora danych) oraz w przypadku zaistnienia przesłanki należy poinformować o naruszeniu osoby fizyczne, których naruszenie dotyczy.
5) Administrator powinien podjąć działania mające na celu ograniczenie skali naruszenia i przywrócenie stanu sprzed wystąpienia naruszenia.
6) Informacje na temat naruszenia powinny być udokumentowane[12].

W przypadku konieczności zgłoszenia naruszenia ochrony danych do organu nadzorczego administrator danych powinien w szczególności zawrzeć w nim opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać:

[12] Zob. także: Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250 rev.01), s. 8.

- kategorię i przybliżoną liczbę osób, których dane dotyczą;
- kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opis możliwych konsekwencji naruszenia ochrony danych osobowych;
- opis środków zastosowanych w procesie obsługi naruszenia ochrony danych osobowych, w tym środków, które – w stosownych przypadkach – mają służyć zminimalizowaniu jego ewentualnych, negatywnych skutków.

Według danych przekazanych przez Prezesa Urzędu Ochrony Danych Osobowych administratorzy bardzo często popełniają błędy w takim zgłoszeniu naruszenia, co utrudnia i wydłuża pracę tego organu. Najczęściej występującymi błędami podczas zgłaszania naruszeń ochrony danych osobowych są w szczególności:

- błędna liczba osób, których dane dotyczą;
- podanie niewłaściwej kategorii danych;
- wskazanie niewłaściwego poziomu ryzyka;
- podanie niewłaściwego czasu zaistnienia naruszenia.

Ponadto, zgodnie z art. 33 ust. 3 ogólnego rozporządzenia o ochronie danych, administrator powinien w zgłoszeniu podać tylko kategorie danych osobowych, których dotyczy naruszenie. Kategoriami danych będą np. imię, nazwisko, adres zamieszkania, adres e-mail, numer PESEL, dane dotyczące zdrowia, dane dotyczące wykształcenia itp. Niewłaściwą praktyką jest podawanie w takim zgłoszeniu konkretnych imion, nazwisk czy adresów zamieszkania osób, których dane dotyczą[13]. Wątpliwości pojawiają się także przy interpretacji terminu „kategoria osób". RODO nie określa definicji kategorii osób, których dane dotyczą. Grupa Robocza Artykuł 29 zaproponowała, aby kategorie osób, których dane dotyczą, obejmowały różnego rodzaju osoby fizyczne których dotyczy naruszenie danych osobowych, np. pracownicy, klienci, współpracownicy itp.

[13] Komunikat Prezesa Urzędu Ochrony Danych Osobowych, www.uodo.gov.pl [dostęp 12.02.2020].

Warto podkreślić, że brak dostępu do szczegółowych informacji nie może stanowić podstawy do niezgłoszenia naruszenia danych osobowych w terminie wymaganym przez ogólne rozporządzenie o ochronie danych osobowych. Jeżeli informacji o naruszeniu nie da się udzielić w tym samym czasie, można ich udzielać sukcesywnie PUODO, lecz bez zbędnej zwłoki. Różne kategorie naruszenia mogą bowiem wiązać się z koniecznością przekazania dodatkowych informacji, aby w pełni wyjaśnić okoliczności danej sprawy.

Grupa Robocza Artykuł 29 zaleca, aby w momencie, w którym administrator danych po raz pierwszy zgłasza naruszenie Prezesowi Urzędu Ochrony Danych Osobowych, poinformował również ten organ o tym, że nie dysponuje jeszcze wszystkimi wymaganymi informacjami, oraz że przekaże bardziej szczegółowe dane na późniejszym etapie, bez zbędnej zwłoki, po otrzymaniu takich informacji[14]. Organ nadzorczy powinien ustalić z administratorem sposób i termin przekazania tych dodatkowych informacji. Nie uniemożliwia to administratorowi udzielania dodatkowych informacji na dowolnym innym etapie, w przypadku gdy uzyska wiedzę o dalszych istotnych okolicznościach faktycznych związanych z naruszeniem, które powinny zostać przekazane organowi nadzorczemu.

Warto zaznaczyć, że sam fakt wystąpienia naruszenia ochrony danych osobowych nie stanowi przesłanki do zgłoszenia takiego naruszenia do PUODO. Bowiem, tak jak zaznaczono w art. 33 ust. 1 RODO, dotyczy to naruszeń praw lub wolności osób fizycznych. Oznacza to, że natychmiast po stwierdzeniu naruszenia administrator danych musi nie tylko dążyć do ograniczenia negatywnych skutków zdarzenia (naruszenia), lecz również ocenić ryzyko, które może powstać w wyniku tego naruszenia dla osób, których dane dotyczą. Przykładowo naruszeniem, które nie będzie wymagało zgłoszenia organowi nadzorczemu, jest zagubienie przez pracownika bezpiecznie zaszyfrowanego komputera przenośnego (laptopa). Bowiem ryzyko zapoznania się przez osoby nieuprawnione z danymi zawartymi na tym dysku komputera przenośnego jest w tej sytuacji niskie.

Należy pamiętać, że bez względu na to, czy należy zgłosić dane naruszenie organowi nadzorczemu, czy też nie, administrator danych jest zobowiązany do dokumentowania wszystkich naruszeń danych osobowych. Dokumentacja

[14] Zob. także: Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250 rev.01), s. 9.

powinna być prowadzona w taki sposób, by pozwalała organowi nadzorczemu na weryfikowanie przestrzegania obowiązków dotyczących zgłaszania naruszeń. Dokumentacja powinna zawierać co najmniej:

- informacje o okolicznościach naruszenia;
- skutki naruszenia;
- podjęte działania zaradcze.

Brak wypełnienia obowiązków w zakresie prowadzenia dokumentacji stanowi przesłankę do zastosowania wobec podmiotu administracyjnej kary pieniężnej w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa w wysokości do 2% jego całkowitego rocznego światowego obrotu (z poprzedniego roku obrotowego).

Zawiadamianie osoby o naruszeniu ochrony jej danych osobowych

W sytuacji, w której naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator danych – oprócz zgłoszenia do PUODO – zobligowany jest bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie ma na celu przede wszystkim dostarczenie szczegółowych informacji na temat działań zapobiegawczych, które osoby fizyczne powinny podjąć, aby uchronić się przed wszelkimi negatywnymi skutkami naruszenia. Administrator danych powinien dołożyć wszelkich starań, by zawiadomienie było zredagowane z użyciem przejrzystego i zrozumiałego języka dla osób, których dane dotyczą. Prezes Urzędu Ochrony Danych Osobowych, powołując się na wytyczne Grupy Roboczej Artykuł 29, zaleca, aby sformułowania kierowane do podmiotu danych były przekazem bezpośrednim. Należy wybrać taką formę zawiadomienia, by osoba fizyczna miała możliwość zapoznania się z jego treścią, np. wiadomość e-mail, SMS, korespondencja[15]. Zawiadomienie powinno zostać dostarczone osobie, której dane dotyczą, w możliwie najkrótszym czasie.

Zgodnie z RODO zawiadomienie osoby fizycznej nie jest wymagane w następujących przypadkach:

[15] Prezes Urzędu Ochrony Danych Osobowych, www.uodo.gov.pl [dostęp 15.02.2020].

1. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, np. szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym.
2. Administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane zostały naruszone.
3. Zawiadomienie wymagałoby niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób. W zakresie publicznego komunikatu należy przyjąć, iż powinien on zawierać takie elementy jak charakter naruszenia, opisany jasnym i prostym językiem oraz zawierać informacje o zastosowanych środkach zaradczych[16].

Kluczowe dla organizacji jest wdrożenie odpowiednich środków technicznych i organizacyjnych zapobiegających możliwym naruszeniom ochrony danych.

Zawiadomienie o naruszeniu ochrony danych osób fizycznych powinno zawierać w szczególności:

1) opis charakteru naruszenia (np. przedstawienie okoliczności wystąpienia naruszenia);
2) imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych (jeżeli został on wyznaczony) lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3) opis możliwych konsekwencji naruszenia ochrony danych osobowych (np. możliwość zaciągnięcia zobowiązań finansowych);
4) opis środków zastosowanych i proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych lub zminimalizowania jego ewentualnych, negatywnych skutków.

Istotne jest, aby informacje przekazane osobie fizycznej, dotyczące naruszenia, były dla niej zrozumiałe w zakresie charakteru naruszenia oraz wiedzy na temat postępowania, aby się zabezpieczyć.

[16] Zob. także: P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Wyd. C.H.Beck, Warszawa 2018, s. 519.

Najczęściej występujące naruszenia danych osobowych

Zgodnie z danymi podanymi w sprawozdaniu z działalności Prezesa Urzędu Ochrony Danych Osobowych za 2018 rok[17] zakres przedmiotowy naruszeń ochrony danych osobowych zgłaszanych przez administratorów danych z sektora publicznego obejmował najczęściej nieprawidłowości w przetwarzaniu danych osobowych dotyczące:

1. Udostępnienia danych osobowych nieuprawnionym osobom w związku z wysyłaniem poczty elektronicznej. Naruszenie powstawało wskutek błędu pracowników. Administratorzy podejmowali działania mające na celu zdyscyplinowanie pracowników, przeprowadzali dodatkowe szkolenia, dokonywali przeglądu procedur, wykonywali audyty bezpieczeństwa. Warto zaznaczyć, że w takim przypadku, co do zasady, konieczne jest poinformowanie osób fizycznych o naruszeniu[18].
2. Udostępnienia danych w trybie dostępu do informacji publicznej, w wyniku nieprawidłowej anonimizacji danych, w tym w Biuletynie Informacji Publicznej. Naruszenia powstawały głównie wskutek niedopatrzenia pracowników zajmujących się anonimizacją danych. Administratorzy dokonywali przeglądu procedur oraz deklarowali wprowadzenie dodatkowych procedur (np. dodatkowe sprawdzanie dokumentów przez innego pracownika pod kątem anonimizacji dokumentów).
3. Zniszczenia/zagubienia/kradzieży dokumentacji bądź innych nośników (telefon, smartfon, komputer przenośny) zawierających dane osobowe. Administratorzy podejmowali działania mające na celu ustalenie przyczyn zagubienia korespondencji czy weryfikację umów zawartych z operatorem pocztowym. Sam fakt utraty danych osobowych w wyniku zagubienia czy kradzieży urządzeń lub nośników nie musi prowadzić do naruszenia praw lub wolności osób, których dane dotyczą, jeżeli administrator

[17] Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w 2018 r., www.uodo.gov.pl [dostęp 12.02.2020].

[18] Zob. Decyzja (ZWAD.405.154.2018) Prezesa Urzędu Ochrony Danych Osobowych z dnia 21 grudnia 2018 r. nakazująca ubezpieczycielowi ponowne zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych i wskazanie jej możliwych konsekwencji zdarzenia, a także powiadomienie jej o podjętych działaniach zaradczych i proponowanych środkach, które osoba ta może zastosować, by zminimalizować ewentualne negatywne skutki naruszenia.

zastosował skuteczne, adekwatne środki zabezpieczenia. Przykładowo, w celu eliminowania naruszeń, administrator danych powinien:

- ograniczyć ilość dokumentacji wynoszonej poza obszar obiektu administratora danych do niezbędnego minimum;
- tam, gdzie jest to możliwe, przewozić dokumentację w formie elektronicznej (na zaszyfrowanych urządzeniach informatycznych).

4. Naruszenia związane z udostępnieniem danych osobowych (np. zaświadczeń), które zawierały informacje o innych, osobom nieuprawnionym lub petentom urzędów. Najczęściej naruszenia wynikały z błędów pracowników urzędów. Administratorzy podejmowali działania podobne jak w poprzednich przypadkach, tj. mające na celu zdyscyplinowanie pracowników.
5. Naruszenia polegające na złamaniu zabezpieczeń systemu informatycznego, które skutkowało zablokowaniem dostępu do plików, całego komputera lub wewnętrznej sieci intranetowej przez złośliwe oprogramowanie typu ransomware. Administratorzy odzyskiwali dostęp do danych na podstawie kopii zapasowych baz danych wykonywanych automatycznie.

Z kolei informacje dotyczące najczęściej zgłaszanych naruszeń w sektorze prywatnym dotyczyły podobnych działań jak w sektorze publicznym, jednak dodatkowo można wyszczególnić:

1) lukę bezpieczeństwa w systemie informatycznym pozwalającą na uzyskanie nieuprawnionego dostępu do danych osobowych;
2) przesłanie newslettera z błędnie skonstruowanego skryptu z adresów e-mail do wszystkich odbiorców;
3) omyłkowe udostepnienie w trakcie rozmowy telefonicznej danych innego klienta przez pracownika call center;
4) ataki hackerskie, mające na celu uzyskanie nieuprawnionego dostępu do bazy danych klientów, sklepów internetowych w celu wysyłki phishingowych wiadomości SMS i wyłudzenia danych dostępowych do konta bankowego.

W przypadku naruszenia polegającego na udostępnieniu danych osobowych nieuprawnionym osobom w związku z wysyłką poczty elektronicznej, jeśli już doszło do takiego naruszenia, administrator danych powinien w szczególności:

- wprowadzić procedury kontroli poprawności adresu przy wysyłce dokumentów zawierających dane osobowe;
- przed wysyłką dokumentów weryfikować poprawność adresu z klientem.

Natomiast w przypadku niewłaściwej anonimizacji danych osobowych administrator danych powinien w szczególności:

- przeprowadzać regularne szkolenia dla personelu z zakresu ochrony danych;
- wprowadzić szczegółowe instrukcje postępowania z dokumentami zawierającymi dane osobowe, w tym – sposobów anonimizacji danych;
- wprowadzić wewnętrzne procedury regulujące przechowywanie archiwalnych dokumentów oraz ich późniejsze niszczenie.

Administratorzy powinni dokonywać szczegółowej analizy przypadków naruszeń ochrony danych osobowych, bowiem nie wszystkie będą wymagały zgłoszenia do organu nadzorczego. Jednocześnie istotne jest, by administratorzy danych potrafili prawidłowo i sprawnie reagować na już występujące naruszenia, aby możliwie ograniczyć negatywny wpływ na ochronę praw i wolności osób fizycznych.

Analiza występujących naruszeń ochrony danych

Według Prezesa Urzędu Ochrony Danych Osobowych brak przeprowadzenia prawidłowej oceny ryzyka naruszenia praw lub wolności osób fizycznych jest jednym z podstawowych błędów, które popełniają administratorzy danych. Zgodnie bowiem z zaleceniami zawartymi w motywach 75 i 76 RODO podczas oceny ryzyka zasadniczo należy wziąć pod uwagę zarówno prawdopodobieństwo, jak i powagę ryzyka naruszenia praw lub wolności osób, których dane dotyczą. Należy podkreślić, że podczas oceny ryzyka naruszenia praw i wolności osób fizycznych powstałego w wyniku wystąpienia naruszenia bardzo często administratorzy danych koncentrują się na innych (niż ochrona praw i wolności podmiotu danych) obszarach, np. zabezpieczaniu danych. Oceniając ryzyko dla osób fizycznych, będące wynikiem naruszenia, administrator powinien uwzględnić zatem konkretne okoliczności naruszenia, w tym wagę potencjalnego wpływu i prawdopodobieństwo jego wystąpienia. Grupa Robocza Artykuł 29 zaleca zatem, aby w trakcie oceny brano pod uwagę następujące kryteria[19]:

1) rodzaj naruszenia, np. konsekwencje naruszenia dla osoby fizycznej w przypadku naruszenia integralności;
2) charakter, wrażliwość i ilość danych osobowych;

[19] Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250 rev.01), s. 28-30.

3) łatwość identyfikacji osób fizycznych;
4) wagę konsekwencji dla osób fizycznych, tj. możliwe szkody, których mogą doznać osoby fizyczne, np. w przypadku, gdy w wyniku naruszenia nastąpi kradzież lub sfałszowanie tożsamości, uszkodzenie ciała, cierpienie psychiczne, upokorzenie lub naruszenie dobrego imienia;
5) cechy szczególne danej osoby fizycznej;
6) cechy szczególne administratora danych;
7) liczbę osób fizycznych, na które wywiera wpływ dane naruszenie.

Mając na uwadze powyższe, administrator danych, dokonując oceny ryzyka, które może powstać w wyniku naruszenia, powinien łącznie uwzględnić wagę potencjalnego wpływu na prawa i wolności osób fizycznych i prawdopodobieństwo jego wystąpienia. Oczywiście ryzyko wzrasta, gdy konsekwencje naruszenia są poważniejsze, jak również wtedy, gdy wzrasta prawdopodobieństwo ich wystąpienia. W przypadku jakichkolwiek wątpliwości administrator powinien zgłosić naruszenie, nawet jeśli taka ostrożność mogłaby się okazać nadmierna. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) opracowała zalecenia dotyczące metod oceny wagi naruszenia[20], które mogą być przydatne administratorom i podmiotom przetwarzającym podczas opracowywania planów działania i zarzadzania w sytuacji wystąpienia naruszenia.

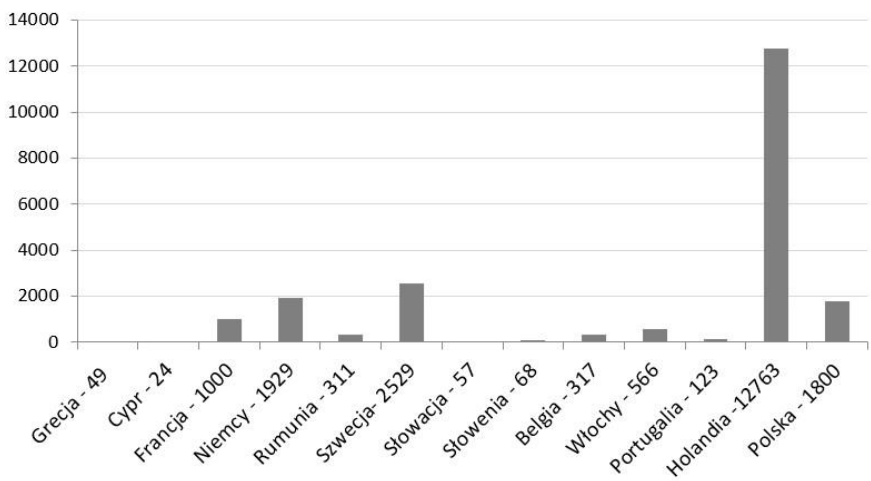
Statystyki zgłoszonych naruszeń ochrony danych

Zgodnie z danymi ze sprawozdania z działalności Prezesa Urzędu Ochrony Danych Osobowych w 2018 r. od 25 maja do 31 grudnia 2018 r. UODO dokonał analizy 2 446 zgłoszeń naruszeń pod kątem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, w tym – 1 882 naruszenia zostały zgłoszone przez podmioty sektora prywatnego, zaś 564 – przez podmioty sektora publicznego[21]. Dla porównania: do irlandzkiego organu nadzorczego wpłynęło w 2018 r. 3 687 zgłoszeń naruszeń ochrony danych osobowych[22], w tym – 2 429

[20] ENISA, Zalecenia dotyczące metod oceny wagi naruszeń ochrony danych osobowych, https://www.enisa.europa.eu/publications/dbn-severity [dostęp 12.02.2020].
[21] Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w 2018 r., www.uodo.gov.pl [dostęp 12.02.2020].
[22] Annual Report 25 may – 31 december 2018, An Coimisium um Chosaint Sonrai, Data Protection Commission, s. 36-38.

z sektora prywatnego, a 1 258 – z sektora publicznego. Natomiast liczba powiadomień o naruszeniu danych otrzymanych przez holenderski organ nadzorczy wyniosła 20 881, w tym najbardziej dotknięte sektory to sektory zdrowia (29% zgłoszonych naruszeń), sektor finansowy (26% zgłoszonych naruszeń) oraz sektor publiczny (17% zgłoszonych naruszeń). 63% przypadków naruszeń, które wpłynęły do holenderskiego organu nadzorczego, dotyczyło danych osobowych wysłanych na niewłaściwy adres e-mail. Pozostałe 37% przypadków dotyczyło utraty danych osobowych (np. zagubienie laptopa lub pamięci USB), hackowania, phishingu lub złośliwego oprogramowania[23].

Według danych opublikowanych przez Komisję Europejską w UE w okresie od 25 maja 2018 r. do 28 stycznia 2019 r. zgłoszono w łącznie 41 502 powiadomień o naruszeniu ochrony danych osobowych. Z rysunku 1 wynika, że liczba zawiadomień o naruszeniach ochrony danych wpływających do poszczególnych organów nadzorczych w krajach Unii Europejskiej jest bardzo zróżnicowana, a najwięcej naruszeń zostało zgłoszonych w Holandii.



Rysunek 1. Całkowita liczba otrzymanych powiadomień o naruszeniu ochrony danych osobowych w okresie od 25 maja 2018 r. do 28 stycznia 2019 r.
Źródło: opracowanie własne na podstawie „GDPR Today", https://www.gdprtoday.org/gdpr-in-numbers-4/ [dostęp 10.02.2020].

[23] Autoriteit, Persoonsgegevens, Meldplicht dataleeken. Overzicht feiten en cijfers 2018, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2019/01/rapportage_datalekken_2018.pdf [dostęp 12.02.2020].

Zgodnie z informacją podaną przez Prezesa Urzędu Ochrony Danych Osobowych do maja 2019 r. administratorzy, realizując obowiązek wynikający z art. 33 ust. 1 ogólnego rozporządzenia o ochronie danych (RODO), zgłosili aż 4 539 naruszeń ochrony danych osobowych. Dwie trzecie notyfikacji pochodziło od administratorów z sektora prywatnego, a jedna trzecia – od administratorów z sektora publicznego. W przypadku sektora prywatnego najwięcej zgłoszeń napłynęło od firm telekomunikacyjnych, ubezpieczeniowych, finansowych, banków oraz służby zdrowia. W sektorze publicznym zawiadomienia o incydentach z danymi osobowymi najczęściej nadsyłały jednostki samorządu terytorialnego, szkoły, przedszkola, żłobki oraz placówki służby zdrowia[24].

Według Komisji Europejskiej w Unii Europejskiej do organów nadzorczych wpłynęło w okresie od 25 maja 2018 r. do maja 2019 r. aż 89 271 zgłoszeń o utracie danych, które mogły spowodować naruszenie praw lub wolności osób fizycznych[25], co pokazuje, że jednostki organizacyjne w Unii Europejskiej są świadome obowiązku związanego ze zgłaszaniem naruszeń ochrony danych.

Wnioski

Naruszenie bezpieczeństwa danych osobowych może potencjalnie spowodować szereg negatywnych skutków dla osób fizycznych, takich jak powstanie uszczerbku fizycznego, szkód majątkowych lub szkód niemajątkowych. Przykładowo mogą one obejmować utratę kontroli nad własnymi danymi osobowymi, ograniczenie praw, dyskryminację, kradzież lub sfałszowanie tożsamości, stratę finansową czy też naruszenie dobrego imienia. Mogą one również wiązać się z wszelkimi innymi znacznymi szkodami gospodarczymi lub społecznymi dla tych osób fizycznych.

Dlatego w art. 33 ogólnego rozporządzenia o ochronie danych osobowych zobligowano administratora danych do zgłoszenia naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, chyba że dane naruszenie nie wiąże się z ryzykiem wywołania takich negatywnych skutków.

[24] Prezes Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl/pl/134/1029 [dostęp 12.02.2020].

[25] The European Data Protection Board, Rapport: "GDPR in numbers", edpb.europa.eu [dostęp 12.02.2020].

Warto podkreślić, że RODO przewiduje odpowiedzialność administracyjną za niezrealizowanie obowiązku zgłaszania naruszeń oraz innych postanowień zawartych w art. 33 RODO. W sytuacji, kiedy administrator danych nie zrealizuje obowiązku zgłoszenia naruszenia ochrony danych organowi nadzorczemu albo osobom, których dane dotyczą, albo zarówno organowi nadzorczemu, jak i osobom, których dane dotyczą, organ nadzorczy może skorzystać z możliwości zastosowania administracyjnej kary pieniężnej. Wartość tej kary może wynosić do 10 000 000 EUR lub do 2% całkowitego rocznego światowego obrotu przedsiębiorstwa (zgodnie z art. 83 ust. 4 lit. a RODO). Należy również pamiętać o tym, że w niektórych przypadkach niewywiązanie się z obowiązku zgłoszenia naruszenia mogłoby doprowadzić do ujawnienia braku albo nieadekwatności istniejących środków bezpieczeństwa. Ponadto wytyczne Grupy Roboczej Art. 29 w sprawie administracyjnych kar stanowią, że: „występowanie kilku różnych naruszeń popełnionych łącznie w konkretnym pojedynczym przypadku oznacza, że organ nadzorczy może nakładać administracyjne kary w sposób, który jest zarazem skuteczny, proporcjonalny i odstraszający na poziomie najpoważniejszego naruszenia". W takim przypadku organ nadzorczy będzie miał również możliwość nakładania kar za niewywiązanie się z obowiązku zgłoszenia naruszenia lub zawiadomienia o wystąpieniu naruszenia, określonego w art. 33 i 34 RODO z jednej strony, oraz za brak (odpowiednich) środków bezpieczeństwa, o których mowa w art. 32 RODO, z drugiej strony. Obydwie te sytuacje traktuje się jako dwa odrębne naruszenia.

Mając na uwadze powyższe przepisy podmioty, które przetwarzają dane osobowe, powinny zastosować odpowiednie środki organizacyjne i techniczne, w tym wdrożyć odpowiednie procedury, które pozwolą im sprawnie i szybko realizować proces ochrony danych osobowych w ich jednostce i w odpowiednim czasie (jeśli wymaga tego sytuacja) zgłosić takie naruszenie organowi nadzorczemu.

Bibliografia

Annual Report 25 may-31 december 2018, An Coimisium um Chosaint Sonrai, Data Protection Commission.

Autoriteit, Persoonsgegevens, Meldplicht dataleeken. Overzicht feiten en cijfers 2018, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2019/01/rapportage_datalekken_2018.pdf.

Decyzja (ZWAD.405.154.2018) Prezesa Urzędu Ochrony Danych Osobowych z dnia 21 grudnia 2018 r. nakazująca ubezpieczycielowi ponowne zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych i wskazanie jej możliwych konsekwencji zdarzenia, a także powiadomienie jej o podjętych działaniach zaradczych i proponowanych środkach, które osoba ta może zastosować, by zminimalizować ewentualne negatywne skutki naruszenia.

ENISA, *Zalecenia dotyczące metod oceny wagi naruszeń ochrony danych osobowych*, https://www.enisa.europa.eu/publications/dbn-severity.

Fajgielski P., *Informowanie o naruszeniu ochrony danych osobowych w świetle przepisów ogólnego rozporządzenia o ochronie danych*, „Monitor Prawniczy" 2016, nr 20.

GDPR Today, GDPR in numbers, www.gdprtoday.org/gdpr-in-numbers.

Litwiński P., Barta P., Kawecki M., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Wyd. C.H.Beck, Warszawa 2018.

PN-EN ISO/IEC 27001:2017 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L z 2016 r. Nr 119/1).

Sobczak J., *Realizacja usługi przetwarzania danych osobowych w chmurze obliczeniowej*, [w:] *Informacje prawnie chronione – wybrane zagadnienia*, red. S. Topolewski, Wyd. Nauk. UPH, Siedlce 2019.

Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w 2018 r., www.uodo.gov.pl.

The European Data Protection Board, Rapport: "GDPR in numbers", edpb.europa.eu.

Wytyczne Grupy Roboczej Artykuł 29 dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250 rev.01).

Obligation to report the breaches of personal data protection in organizational units

Summary: The article explains the process of notification of a personal data breach to the supervisory authority, in accordance with Article 33 of The General Data Protection Regulation (GDPR). The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area. In case (preventive) security measures are breached and personal data is unlawfully processed, the controller must report such a breach to the supervisory authority within 72 hours, and possibly to affected data subjects as well. This is the case unless you can establish that the breach has caused no actual risks for the data subjects or other individuals. The article contains analysis of data breach notifications sent to data protection authorities by companies or other organizations.
Keywords: *GDPR, data protection, notification of a personal, data breach, personal data, supervisory authority*

MONIKA KOPCZYŃSKA

Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych

Przetwarzanie danych osobowych w Straży Granicznej

Tradycja Straży Granicznej

Straż Graniczna (SG) to formacja powołana do życia Ustawą z dnia 12 października 1990 r. o Straży Granicznej[1]. Jej utworzenie było odpowiedzią na zmianę sytuacji polityczno-ustrojowej, która miała miejsce w 1989 r. Nowa rzeczywistość, jak również zmienione warunki funkcjonowania państwa, wymusiły potrzebę nowatorskich sposobów ochrony granic Rzeczypospolitej Polskiej. Takim sposobem Straż Graniczna zastąpiła Wojska Ochrony Pogranicza w sprawowaniu obowiązku ochrony granic, jak również – w kontroli ruchu granicznego. Funkcjonowanie Straży Granicznej rozpoczęło się 16 maja 1991 r.[2] Należy mieć świadomość, iż Straż Graniczna jest spadkobierczynią tradycji Korpusu Ochrony Pogranicza oraz Wojsk Ochrony Pogranicza[3]. Korpus Ochrony Pogranicza realizował swoje zadania od 1924 r., Wojska Ochrony Pogranicza od 1945 r., natomiast od 1991 r. do dnia dzisiejszego funkcjonuje formacja o charakterze policyjnym, jaką jest Straż Graniczna. Zapisy ustawy o Straży Granicznej określają m.in. naczelne zadania tej formacji, uprawnienia i obowiązki funkcjonariuszy SG, przebieg służby w SG czy korpusy i stopnie w Straży Granicznej.

[1] Ustawa z dn. 12 października 1990 r. o Straży Granicznej (Dz.U. Nr 78, poz. 462).
[2] J.R. Truchan, *Wybrane obszary współdziałania Policji i Straży Granicznej w ochronie granicy Polski – zewnętrznej granicy Unii Europejskiej*, Szczytno 2016, s. 52.
[3] *System ochrony granicy państwowej Rzeczypospolitej Polskiej. Stan obecny i prognozy na przyszłość*, red. B. Wiśniewski, R. Jakubczak, Szczytno 2015, s. 15.

Wybrane aspekty działalności Straży Granicznej

Ustawowe zadania, które Straż Graniczna realizuje, wymienione są w art. 1 ust. 2 ww. ustawy[4]. Formacja jest powołana do realizacji niżej wymienionych zadań, do których należą:

1) ochrona granicy państwowej na lądzie i morzu;
2) organizowanie i dokonywanie kontroli ruchu granicznego;
3) zapobieganie i przeciwdziałanie nielegalnej migracji;
4) wydawanie zezwoleń na przekraczanie granicy państwowej, w tym wiz;
5) rozpoznawanie i wykrywanie przestępstw i wykroczeń, zapobieganie im oraz ściganie ich sprawców w zakresie właściwości Straży Granicznej;
6) zapewnienie bezpieczeństwa w komunikacji międzynarodowej i porządku publicznego w zasięgu terytorialnym przejścia granicznego, a w zakresie właściwości Straży Granicznej – także w strefie nadgranicznej;
7) współdziałanie z innymi organami i służbami w zakresie rozpoznawania zagrożeń terroryzmem i przeciwdziałania im;
8) osadzanie i utrzymywanie znaków granicznych na lądzie oraz sporządzanie, aktualizacja i przechowywanie granicznej dokumentacji geodezyjnej i kartograficznej;
9) ochrona nienaruszalności znaków i urządzeń służących do ochrony granicy państwowej;
10) przetwarzanie informacji, w tym danych osobowych, informacji z zakresu ochrony granicy państwowej, kontroli ruchu granicznego, zapobiegania i przeciwdziałania nielegalnej migracji oraz udostępnianie ich sądom, prokuratorom, organom administracji publicznej i innym organom państwowym, uprawnionym do ich otrzymania na podstawie odrębnych ustaw, w zakresie niezbędnym do realizacji ich zadań;
11) nadzór nad eksploatacją polskich obszarów morskich oraz przestrzeganiem przez statki przepisów obowiązujących na tych obszarach;
12) ochrona granicy państwowej w przestrzeni powietrznej Rzeczypospolitej Polskiej przez prowadzenie obserwacji statków powietrznych i obiektów latających, przelatujących przez granicę państwową na małych

[4] Zob. szerz. art. 1, ust. 2 ustawy z dn. 12 października 1990 r. o Straży Granicznej (Dz.U. Nr 78, poz. 462).

wysokościach, oraz informowanie o tych przelotach właściwych jednostek Sił Powietrznych Sił Zbrojnych Rzeczypospolitej Polskiej;

13) zapobieganie transportowaniu, bez zezwolenia wymaganego w myśl odrębnych przepisów, przez granicę państwową odpadów, szkodliwych substancji chemicznych oraz materiałów jądrowych i promieniotwórczych, a także zanieczyszczaniu wód granicznych;
14) zapobieganie przemieszczaniu, bez zezwolenia wymaganego w myśl odrębnych przepisów, przez granicę państwową środków odurzających i substancji psychotropowych oraz broni, amunicji, materiałów wybuchowych i prekursorów materiałów wybuchowych podlegających ograniczeniom;
15) przeprowadzanie kontroli legalności wykonywania pracy przez cudzoziemców, prowadzenia działalności gospodarczej przez cudzoziemców, powierzania wykonywania pracy cudzoziemcom;
16) wykonywanie zadań określonych w innych ustawach.

Ponadto Straż Graniczna realizuje zadania i czynności wynikające z przepisów prawa Unii Europejskiej, umów i porozumień międzynarodowych, na zasadach i w zakresie w nich określonych[5]. Należy w tym miejscu podkreślić, że funkcjonariusze Straży Granicznej wykonują również inne zadania określone w ustawie o SG. Ponadto, realizując ww. zadania, mają pośredni i bezpośredni wpływ na poziom bezpieczeństwa nie tylko Polski, ale również Unii Europejskiej i Strefy Schengen. Ustawowe zadania są realizowane w efektywny sposób. Wynika to zarówno z nieustannego podnoszenia kwalifikacji funkcjonariuszy SG, jak również specjalistycznego wyposażenia, jakim dysponuje Straż Granicza.

Dane osobowe w Straży Granicznej i podstawy prawne przetwarzania tych danych

Formacja, jaką jest Straż Graniczna, przetwarza bardzo dużo informacji, w tym również danych osobowych, na podstawie różnych przepisów. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych

[5] J.R. Truchan, dz. cyt., s. 54.

osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwane dalej RODO, definiuje dane osobowe jako „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (»osobie, której dane dotyczą«); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”[6]. Kolejny zapis ww. rozporządzenia stanowi o zasadach przetwarzania tych danych.

1. Dane osobowe muszą być:
   a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
   b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”);
   c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
   d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
   e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można

[6] Art. 4 pkt. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność")[7].

W związku z powyższym, jeżeli chodzi o kwestie przetwarzania danych osobowych w Straży Granicznej, to ich administratorem jest Komendant Główny Straży Granicznej, natomiast nadzór nad prawidłowym przetwarzaniem danych osobowych w Straży Granicznej sprawuje inspektor ochrony danych – jest nim Dyrektor Biura Ochrony Informacji Komendy Głównej Straży Granicznej. Istotnym jest, iż dane osobowe w Straży Granicznej przetwarza się w konkretnych celach na podstawie obowiązujących przepisów prawa, zawartych umów oraz na podstawie udzielonej zgody. Należy podkreślić, że przetwarzanie danych osobowych przez Straż Graniczną jest nie tylko uprawnieniem, ale często również ustawowym obowiązkiem. Odbiorcami danych osobowych mogą być:

1) organy władzy publicznej oraz podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów powszechnie obowiązującego prawa;
2) inne podmioty, które na podstawie stosownych umów podpisanych ze Strażą Graniczną przetwarzają dane osobowe, których administratorem

[7] Art. 5 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

jest Komendant Główny Straży Granicznej. W tym wypadku Straż Graniczna dokłada starań, aby przetwarzanie danych przez te podmioty odbywało się zgodnie z obowiązującymi przepisami i aby ryzyko naruszenia tych przepisów było jak najmniejsze.

Ponadto dane osobowe mogą być przekazywane do państw trzecich lub organizacji międzynarodowych w uzasadnionych wypadkach, gdy przepisy prawa na to pozwalają. Straż Graniczna bardzo często odmawia przekazania danych osobowych, o które proszą organizacje lub państwa – jest to podyktowane głównie brakiem prawnych możliwości przekazania tych danych. Jeżeli chodzi o czas, przez który dane osobowe będą przechowywane w Straży Granicznej, to są one przechowywane przez czas niezbędny do realizacji celów, dla których zostały zebrane lub przez czas przewidziany w przepisach powszechnie obowiązującego prawa. Należy wskazać prawa, jakie przysługują osobom fizycznym, których dane są przetwarzane przez Straż Graniczną:

1) prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
2) prawo do żądania sprostowania (poprawiania) danych osobowych – w przypadku, gdy dane są nieprawidłowe lub niekompletne;
3) prawo do żądania usunięcia danych osobowych (tzw. prawo do bycia zapomnianym), w przypadku gdy:
   a) dane nie są już niezbędne do celów, dla których były zebrane lub w inny sposób przetwarzane;
   b) zostanie wniesiony sprzeciw wobec przetwarzania danych osobowych;
   c) dane osobowe przetwarzane są niezgodnie z prawem;
   d) dane osobowe muszą być usunięte w celu wywiązania się z obowiązku wynikającego z przepisów prawa;
4) prawo do żądania ograniczenia przetwarzania danych osobowych – w przypadku gdy:
   a) zostanie zakwestionowana prawidłowość danych osobowych;
   b) przetwarzanie danych jest niezgodne z prawem, a następuje sprzeciw usunięcia danych, żądanie w zamian ich ograniczenia;
   c) administrator nie potrzebuje już danych dla swoich celów, ale są one potrzebne do ustalenia, obrony lub dochodzenia roszczeń;

d) zostanie wniesiony sprzeciw wobec przetwarzania danych, do czasu ustalenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstawy sprzeciwu;

5) prawo sprzeciwu wobec przetwarzania danych – w przypadku gdy łącznie spełnione są następujące przesłanki:
   a) zaistnieją przyczyny związane ze szczególną sytuacją, w przypadku przetwarzania danych na podstawie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej przez administratora;
   b) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy osób, których dane są przetwarzane lub podstawowe prawa i wolności wymagające ochrony danych osobowych;
6) jeżeli dane osobowe są przetwarzane na podstawie zgody, w każdej chwili można tę zgodę wycofać, wówczas Straż Graniczna zaprzestanie przetwarzania danych pozyskanych na podstawie zgody.

Należy jednak mieć na uwadze, że Straż Graniczna przetwarza dane osobowe głównie na podstawie prawa. Ponadto istnieje prawo wniesienia skargi do organu nadzorczego właściwego w sprawach ochrony danych osobowych. Przysługuje ono w momencie powzięcia informacji o niezgodnym z prawem przetwarzaniu w Straży Granicznej danych osobowych. Dane osobowe mogą być przetwarzane w sposób zautomatyzowany, jednak nie są one profilowane w zakresie obowiązywania RODO, a decyzje nie są podejmowane automatycznie. Należy podkreślić, iż Straż Graniczna pozyskuje dane osobowe od innych organów państwowych oraz instytucji publicznych i niepublicznych oraz ze źródeł publicznie dostępnych. Pozyskiwanie oraz dalsze przetwarzanie danych osobowych odbywają się na podstawie i w granicach prawa[8].

[8] Szerzej na ten temat: Straż Graniczna, Komenda Główna Straży Granicznej, https://www.strazgraniczna.pl/pl/odo/informacje-ogolne/6642,Klauzula-informacyjna-glowna.html [dostęp 28.10.2019].

Dane osobowe przetwarzane przez Komendę Główną Straży Granicznej

Dane osobowe mogą być przetwarzane przez Służbę Graniczną także w celu **przeprowadzenia naboru do pracy lub służby**. Mogą być przekazywane tylko uprawnionym podmiotom na podstawie przepisów prawa. Ponadto nie są one przekazywane do państw trzecich. Wyżej wymienione dane osobowe są przechowywane przez czas niezbędny do realizacji naboru do służby i pracy. Po zakończeniu procesu naboru, dane osobowe osób, które nie zostały przyjęte do służby lub pracy, bądź z innych przyczyn proces wobec nich został przerwany, są usuwane. Natomiast dane osób przyjętych do służby lub pracy będą przetwarzane jako dane funkcjonariuszy lub pracowników Straży Granicznej. Prawa osób fizycznych, których dane osobowe są przetwarzane, prawo wniesienia skargi do organu nadzorczego, profilowanie oraz sposób pozyskiwania tych danych są identyczne, jak te w odniesieniu do osób fizycznych[9].

Dane osobowe są również **przetwarzane podczas odbywania praktyk studenckich** w Komendzie Głównej SG. Przetwarza się je w celu zrealizowania praktyk studenckich. Są one przechowywane przez czas niezbędny do realizacji praktyk studenckich, a po ich zakończeniu jeszcze przez 5 lat. Natomiast prawa osób fizycznych, których dane osobowe są przetwarzane, prawo wniesienia skargi do organu nadzorczego, profilowanie oraz sposób pozyskiwania tych danych są identyczne, jak te w odniesieniu do osób fizycznych[10].

Dane osobowe przetwarzane w ramach **kontaktów z rzecznikiem prasowym** Komendanta Głównego Straży Granicznej są przetwarzane w celu umożliwienia kontaktu z rzecznikiem prasowym Komendanta Głównego Straży Granicznej, w szczególności w celu odpowiedzi na pytania, wysyłania informacji prasowych, zaproszeń na konferencje i wydarzenia. Wyżej wymienione dane osobowe nie są przekazywane poza Straż Graniczną ani do państw trzecich. Są one przechowywane do czasu cofnięcia zgody na przetwarzanie danych osobowych w celach kontaktu z rzecznikiem prasowym lub do czasu wyrażenia sprzeciwu wobec przetwarzania

[9] Szerzej na ten temat: Straż Graniczna, Komenda Główna Straży Granicznej, https://www.straz-graniczna.pl/pl/odo/informacje-ogolne/6642,Klauzula-informacyjna-glowna.html [dostęp 28.10.2019].

[10] Szerzej na ten temat: Straż Graniczna, Komenda Główna Straży Granicznej, https://www.straz-graniczna.pl/pl/odo/dane-osobowe-przetwarza-2/6651,Dane-osobowe-podczas-odbywania-praktyk-studenckich.html [dostęp 31.10.2019].

danych osobowych w tym celu. Straż Graniczna, w zakresie kontaktów z rzecznikiem prasowym, nie pozyskuje danych osobowych od innych organów państwowych oraz instytucji publicznych i niepublicznych ani ze źródeł publicznie dostępnych. W tym przypadku również prawa osób fizycznych, których dane osobowe są przetwarzane, prawo wniesienia skargi do organu nadzorczego oraz profilowanie są identyczne, jak te w odniesieniu do osób fizycznych[11].

Dane osobowe przetwarzane podczas **rozpatrywania skarg, wniosków i petycji w Komendzie Głównej Straży Granicznej** przetwarza się w celu rozpatrzenia wniesionej skargi, wniosku lub petycji. Podanie danych osobowych jest konieczne do rozpatrzenia skargi, wniosku lub petycji. Wynika to z przepisów Kodeksu postępowania administracyjnego[12] i rozporządzenia Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków oraz ustawy o petycjach. W przypadku niepodania danych osobowych nie będzie możliwe rozpatrzenie wniesionych skarg, wniosków lub petycji. Będą one przetwarzane na podstawie Kodeksu postępowania administracyjnego i rozporządzenia Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków oraz na podstawie ustawy o petycjach. Ta kategoria danych osobowych może być przekazywana jedynie podmiotom uprawnionym na podstawie przepisów prawa. Ponadto nie są one przekazywane do państw trzecich. Są przetwarzane przez czas niezbędny do rozpatrzenia skargi, wniosku lub petycji, a następnie są archiwizowane i przechowywane zgodnie z obowiązującym prawem. Prawa osób fizycznych, których dane osobowe są przetwarzane, różnią się tylko treścią ostatniego punktu, mianowicie: w każdej chwili można wycofać zgodę na przetwarzanie danych we wskazanym celu, wówczas Straż Graniczna zaprzestanie przetwarzania danych pozyskanych na podstawie zgody. Należy w tym miejscu podkreślić, iż w razie wycofania zgody, czynności związane z rozpatrzeniem skargi, wniosku lub petycji mogą zostać niezrealizowane. Natomiast prawo wniesienia skargi do organu nadzorczego, profilowanie, jak

[11] Szerzej na ten temat: Straż Graniczna, Komenda Główna Straży Granicznej, https://www.strazgraniczna.pl/pl/odo/dane-osobowe-przetwarza-1/6652,Dane-osobowe-przetwarzane-w-ramach-kontaktow-z-rzecznikiem-prasowym.html [dostęp 31.10.2019].

[12] Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 1960 r. Nr 30, poz. 168).

również sposób pozyskiwania danych osobowych jest identyczny, jak tych w odniesieniu do osób fizycznych[13].

Dane osobowe **przetwarzane w celu nałożenia na przewoźnika lotniczego administracyjnej kary pieniężnej** są przetwarzane na podstawie Kodeksu postępowania administracyjnego[14] oraz Ustawy z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz.U. z 2018 r., poz. 894)[15] w Komendzie Głównej Straży Granicznej. Dane osobowe przetwarza się w celu prowadzenia postępowania administracyjnego na podstawie Kodeksu postępowania administracyjnego oraz Ustawy z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera, związanego z nałożeniem na przewoźnika lotniczego administracyjnej kary pieniężnej. Potencjalne dane osobowe przekazane Straży Granicznej będą przetwarzane na podstawie Kodeksu postępowania administracyjnego. Dane osobowe, przetwarzane w celu nałożenia na przewoźnika lotniczego administracyjnej kary pieniężnej, mogą być przekazywane do wojewódzkiego sądu administracyjnego oraz Naczelnego Sądu Administracyjnego, a także innym podmiotom uprawnionym na podstawie przepisów prawa. Dane osobowe przetwarzane w celu nałożenia na przewoźnika lotniczego administracyjnej kary pieniężnej nie będą przekazywane do państw trzecich. Dane osobowe są przetwarzane przez czas niezbędny do przeprowadzenia postępowania administracyjnego, a następnie są archiwizowane i przechowywane zgodnie z obowiązującym prawem. Pozostałe kryteria są takie same jak w pozostałych kategoriach danych osobowych, różnią się one jedynie sposobem pozyskiwania tych danych od innych podmiotów. Mianowicie: w przypadku postępowania związanego z nałożeniem na przewoźnika lotniczego administracyjnej kary pieniężnej, Straż Graniczna może uzyskać dane osobowe od strony postępowania (przewoźnika

[13] Szerzej na ten temat: Straż Graniczna, Komenda Główna Straży Granicznej, https://www.straz-graniczna.pl/pl/odo/skargi/6821,Dane-osobowe-przetwarzane-podczas-rozpatrywania-skarg-wnioskow-i-petycji.html [dostęp 31.10.2019].

[14] Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 1960 r. Nr 30, poz. 168).

[15] Ustawa z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz.U. z 2018 r., poz. 894).

lotniczego). Mogą to być dane reprezentantów, pełnomocników lub innych osób związanych z przewoźnikiem lotniczym i prowadzonym postepowaniem[16].

W Komendzie Głównej SG przetwarza się dane osobowe także w celu realizacji **usługi „Newsletter"** na podstawie udzielonej przez osobę zgody. Dane te nie są przekazywane poza Straż Graniczną, jak również do państw trzecich. Są one przetwarzane przez czas realizacji usługi „Newsletter". Po zrezygnowaniu z usługi, dane osobowe są automatycznie kasowane. W związku z realizacją usługi „Newsletter" przysługują następujące prawa:

1) prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
2) prawo do żądania sprostowania (poprawiania) danych osobowych – w przypadku gdy dane są nieprawidłowe lub niekompletne;
3) prawo do wycofania zgody na przetwarzanie danych. W takim przypadku Straż Graniczna zaprzestaje zarówno przetwarzania danych pozyskanych na podstawie zgody, jak i realizacji usługi.

W celu realizacji usługi „Newsletter", Straż Graniczna pozyskuje dane osobowe jedynie od użytkowników usługi[17]. Natomiast pozostałe kryteria są takie same jak w wyżej opisanych sytuacjach.

Dane osobowe przetwarzane w celu **realizacji wniosku o udostępnienie informacji publicznej** są przetwarzane na podstawie art. 6 ust. 1 pkt a) RODO[18], tj. na podstawie udzielonej zgody. Straż Graniczna uznaje, że wnioskodawca, wysyłając wniosek o udostępnienie informacji publicznej, wyraża zgodę na przetwarzanie swoich danych osobowych. Dane te są przetwarzane w celu realizacji wniosku o udostępnienie informacji publicznej i nie są przekazywane poza Komendę Główną Straży Granicznej. Ponadto nie są przekazywane do państw trzecich lub organizacji międzynarodowych. Są przetwarzane przez czas niezbędny do

[16] Szerzej na ten temat: Straż Graniczna, Komenda Główna Straży Granicznej, https://www.strazgraniczna.pl/pl/odo/dane-osobowe-przetwarza-3/7035,Dane-osobowe-przetwarzane-w-celu-nalozenia-na-przewoznika-lotniczego-administrac.html [dostęp 31.10.2019].

[17] Szerzej na ten temat: Straż Graniczna, Komenda Główna Straży Granicznej, https://www.strazgraniczna.pl/pl/odo/dane-osobowe-przetwarza-4/7206,Dane-osobowe-przetwarzane-w-celu-realizacji-uslugi-Newsletter.html [dostęp 31.10.2019].

[18] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

realizacji wniosku, a następnie podlegają archiwizacji i są przechowywane przez 2 lata. Poniżej przedstawiono uprawnienia wynikające z przetwarzania tych danych przez Straż Graniczną:

1) prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
2) prawo do żądania sprostowania (poprawiania) danych osobowych;
3) prawo do żądania usunięcia danych osobowych;
4) prawo do żądania ograniczenia przetwarzania danych osobowych;
5) prawo do wycofania zgody na przetwarzanie danych osobowych.

Procedura związana z prawem wniesienia skargi oraz profilowaniem wygląda tak samo, jak w poprzednich kategoriach. Należy jednak pamiętać, iż Straż Graniczna nie pozyskuje tych danych od innych podmiotów[19].

Jeżeli chodzi o przetwarzanie danych osobowych w Straży Granicznej w trybie Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[20], to administratorem tych danych jest **Komendant Główny Straży Granicznej.** Natomiast nadzór nad prawidłowym przetwarzaniem tych danych w Straży Granicznej sprawuje inspektor ochrony danych, którym jest Dyrektor Biura Ochrony Informacji Komendy Głównej Straży Granicznej. Dane osobowe przetwarza się na podstawie art. 13 ust. 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, ustawy o Straży Granicznej oraz innych przepisów w celu realizacji ustawowych zadań. Poniżej przedstawiono prawa osób fizycznych w związku z przetwarzaniem tych danych:

1) prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
2) prawo do żądania sprostowania (poprawiania) danych osobowych – w przypadku gdy dane są niekompletne, nieaktualne lub nieprawdziwe;
3) prawo do żądania usunięcia danych osobowych, w przypadku gdy dane osobowe zostały zebrane lub są przetwarzane z naruszeniem przepisów

[19] Szerzej na ten temat: Straż Graniczna, Komenda Główna Straży Granicznej, https://www.strazgraniczna.pl/pl/odo/dane-osobowe-przetwarza-5/7262,Dane-osobowe-przetwarzane-w-celu-realizacji-wniosku-o-udostepnienie-informacji-p.html [dostęp 31.10.2019].

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

ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;

4) prawo do żądania ograniczenia przetwarzania danych osobowych – w przypadku, gdy:
   - kwestionowana jest prawidłowość danych osobowych;
   - dane osobowe muszą zostać zachowane do celów dowodowych, a zgodnie z prawem podlegają one usunięciu.

Należy jednak mieć na uwadze, że Straż Graniczna przetwarza dane osobowe głównie na podstawie prawa, zatem powyższe uprawnienia w całości lub części mogą osobom nie przysługiwać. Odmowa realizacji powyższych uprawnień zawsze będzie opierała się na przepisach prawa. Natomiast w przypadku powzięcia informacji o niezgodnym z prawem przetwarzaniu w Straży Granicznej danych osobowych, przysługuje prawo wniesienia skargi do organu nadzorczego właściwego w sprawach ochrony danych osobowych – jest nim Prezes Urzędu Ochrony Danych Osobowych[21].

Przetwarzanie **danych osobowych funkcjonariuszy i pracowników Straży Granicznej**, których właściwym przełożonym jest Komendant Główny Straży Granicznej w sprawach osobowych oraz pracowników Komendy Głównej Straży Granicznej dokonuje się na podstawie art. 6 ust. 1 pkt b) c) i e) RODO, ustawy o Straży Granicznej oraz na podstawie przepisów w zakresie prawa pracy, w celu zrealizowania obowiązków ciążących na pracodawcy oraz na przełożonym funkcjonariuszy Straży Granicznej. Odbiorcami danych osobowych mogą być organy władzy publicznej oraz podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów powszechnie obowiązującego prawa. Dane osobowe mogą być przekazywane do państw trzecich lub organizacji międzynarodowych jedynie na podstawie obowiązujących przepisów prawa lub za zgodą osób, których dane dotyczą. Dane osobowe w takim wypadku są przechowywane przez okres zatrudnienia lub pełnienia służby, a po zwolnieniu ze służby lub zakończeniu umowy o pracę są archiwizowane i przechowywane zgodnie z obowiązującymi przepisami w zakresie archiwizacji dokumentów. Podanie danych przez osoby pełniące służbę lub

[21] Szerzej na ten temat: Straż Graniczna, Komenda Główna Straży Granicznej, https://www.straz-graniczna.pl/pl/odo/przetwarzanie-danych-os/7639,Przetwarzanie-danych-osobowych-w-Strazy-Granicznej-w-trybie-Ustawy-z-dnia-14-gru.html [dostęp 31.10.2019].

zatrudnione w Straży Granicznej jest wymogiem prawnym wynikającym z ustawy o Straży Granicznej oraz z przepisów w zakresie prawa pracy. Niektóre dane zbierane przez Straż Graniczną nie są wymagane, podawane są dobrowolnie (np. dane dotyczące trwającej edukacji dorosłych dzieci), lecz ich niepodanie może skutkować odmową wykonania uprawnienia funkcjonariusza lub pracownika (np. dopłaty do wypoczynku lub świadczenia socjalnego). Poniżej przedstawiono uprawnienia wynikające z przetwarzanie przez Straż Graniczną tych danych:

1) prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
2) prawo do żądania sprostowania (poprawiania) danych osobowych;
3) prawo do żądania ograniczenia przetwarzania danych osobowych;
4) prawo do żądania usunięcia danych osobowych (tzw. prawo do bycia zapomnianym), w przypadku, gdy:
   - dane nie są już niezbędne do celów, dla których były zebrane lub w inny sposób przetwarzane,
   - dane osobowe przetwarzane są niezgodnie z prawem,
   - dane osobowe muszą być usunięte w celu wywiązania się z obowiązku wynikającego z przepisów prawa.

Prawo wniesienia skargi do organu nadzorczego jest takie samo jak w opisanych wcześniej przypadkach, a dane osobowe nie są przetwarzane w sposób zautomatyzowany i nie są one profilowane, a decyzje nie są podejmowane automatycznie[22].

Przetwarzanie danych osobowych **w związku z monitoringiem** obiektu Komendy Głównej Straży Granicznej oraz terenu będącego w zasięgu kamer monitorujących odbywa się w celu zapewnienia ochrony obiektu oraz bezpieczeństwa osób i mienia na podstawie art. 11 ust. 1 pkt 7a Ustawy z dnia 12 października 1990 r. o Straży Granicznej[23]. Powyższe dane mogą być przekazywane podmiotom uprawnionym na podstawie przepisów prawa. Natomiast nie są one przekazywane do państw trzecich lub organizacji międzynarodowych. Nagrania z kamer przechowywane są przez okres nieprzekraczający 3 miesięcy od dnia nagrania. Prawo

[22] Szerzej na ten temat: Straż Graniczna, Komenda Główna Straży Granicznej, https://www.strazgraniczna.pl/pl/odo/przetwarzanie-danych-os-1/7640,Przetwarzanie-danych-osobowych-funkcjonariuszy-i-pracownikow-Strazy-Granicznej.html [dostęp 31.10.2019].
[23] Ustawa z dnia 12 października 1990 o Straży Granicznej (Dz.U. z 2019 r., poz. 147 i 125).

wniesienia skargi do organu nadzorczego jest takie samo jak w wymienionych wcześniej sytuacjach. Dane osobowe nie są przetwarzane w sposób zautomatyzowany i nie są one profilowane, a decyzje nie są podejmowane automatycznie[24].

Podsumowanie

Straż Graniczna to formacja o charakterze policyjnym, realizująca szereg ustawowych zadań w sposób efektywny. Jest to wynik nieustannego podnoszenia kwalifikacji funkcjonariuszy SG, jak również specjalistycznego wyposażenia, jakim formacja dysponuje. Realizując ustawowe zadania, przetwarza bardzo dużo danych osobowych na podstawie różnych przepisów. W artykule przedstawiono kategorie danych, które są przetwarzane przez Komendę Główną Straży Granicznej. Są to dane osobowe osób fizycznych, dane osobowe przetwarzane podczas naboru do służby lub pracy, dane osobowe przetwarzane podczas odbywania praktyk studenckich, dane osobowe przetwarzane w ramach kontaktu z rzecznikiem prasowym, dane osobowe przetwarzane podczas rozpatrywania skarg, wniosków lub petycji, dane osobowe przetwarzane w celu nałożenia na przewoźnika lotniczego administracyjnej kary pieniężnej, dane osobowe przetwarzane w celu realizacji usługi „Newsletter", dane osobowe przetwarzane w celu realizacji wniosku o udostępnienie informacji publicznej, dane osobowe przetwarzane w trybie Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, dane osobowe funkcjonariuszy i pracowników oraz dane osobowe, które są przetwarzane w związku z monitoringiem. We wszystkich opisywanych kategoriach danych osobowych administratorem jest Komendant Główny Straży Granicznej, natomiast Inspektorem Ochrony Danych jest Dyrektor Biura Ochrony Informacji Komendy Głównej Straży Granicznej, organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych. Należy podkreślić, iż wszystkie dane przetwarzane przez Straż Graniczną są przetwarzane na podstawie i w granicach prawa.

[24] Szerzej na ten temat: Straż Graniczna, Komenda Główna Straży Granicznej, https://www.strazgraniczna.pl/pl/odo/przetwarzanie-danych-os-2/7641,Przetwarzanie-danych-osbowych-w-zw-z-monitoringiem.html [dostęp 31.10.2019].

Bibliografia

Akty normatywne i dokumenty

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 1960 r. Nr 30, poz. 168).

Ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz.U. Nr 78, poz. 462).

Ustawa z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz.U. z 2018 r., poz. 894).

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

Monografie

System ochrony granicy państwowej Rzeczypospolitej Polskiej. Stan obecny i prognozy na przyszłość, red. B. Wiśniewski, R. Jakubczak, Szczytno 2015.

Truchan J.R., *Wybrane obszary współdziałania Policji i Straży Granicznej w ochronie granicy Polski – zewnętrznej granicy Unii Europejskiej*, Szczytno 2016.

Źródła internetowe

https://www.strazgraniczna.pl/pl/odo/informacje-ogolne/6642,Klauzula-informacyjna-glowna.html [dostęp 28.10.2019].

https://www.strazgraniczna.pl/pl/odo/dane-osobowe-przetwarza-2/6651,Dane-osobowepodczas-odbywania-praktyk-studenckich.html [dostęp 31.10.2019].

https://www.strazgraniczna.pl/pl/odo/dane-osobowe-przetwarza-1/6652,Dane-osoboweprzetwarzane-w-ramach-kontaktow-z-rzecznikiem-prasowym.html [dostęp 31.10.2019].

https://www.strazgraniczna.pl/pl/odo/skargi/6821,Dane-osobowe-przetwarzane-podczas -rozpatrywania-skarg-wnioskow-i-petycji.html [dostęp 31.10.2019].

https://www.strazgraniczna.pl/pl/odo/dane-osobowe-przetwarza-3/7035,Dane-osobowe-przetwarzane-w-celu-nalozenia-na-przewoznika-lotniczego-administrac.html [dostęp dn. 31.10.2019].

https://www.strazgraniczna.pl/pl/odo/dane-osobowe-przetwarza-4/7206,Dane-osobowe- przetwarzane-w-celu-realizacji-uslugi-Newsletter.html [dostęp 31.10.2019].

https://www.strazgraniczna.pl/pl/odo/dane-osobowe-przetwarza-5/7262,Dane-osobowe-przetwarzane-w-celu-realizacji-wniosku-o-udostepnienie-informacji-p.html [dostęp 31.10.2019].

https://www.strazgraniczna.pl/pl/odo/przetwarzanie-danych-os/7639,Przetwarzanie-danych-osobowych-w-Strazy-Granicznej-w-trybie-Ustawy-z-dnia-14-gru.html [dostęp 31.10.2019].

https://www.strazgraniczna.pl/pl/odo/przetwarzanie-danych-os-1/7640,Przetwarzanie-danych-osobowych-funkcjonariuszy-i-pracownikow-Strazy-Granicznej.html [dostęp 31.10.2019].

https://www.strazgraniczna.pl/pl/odo/przetwarzanie-danych-os-2/7641,Przetwarzanie-danych-osbowych-w-zw-z-monitoringiem.html [dostęp 31.10.2019].

Processing of personal data in the Border Guards

Summary: The article presents the Border Guards, a law enforcement agency. The statutory tasks of this agency are presented. It is pointed out that while processing its statutory tasks the Border Guards process a lot of information, including personal data, based on various legal provisions. Personal data are presented and processed by the Border Guards Headquarters. Purposes, conditions or methods of obtaining personal data are described. It should be emphasized that the Border Guards process personal data on the basis and within the limits of the law.
Keywords: *Border Guards, personal data, personal data processing*

JOANNA TYBURSKA
ORCID: 0000-0002-4771-3070
Polska Akademia Nauk, Instytut Nauk Prawnych

Zasada jawności dostępu do informacji publicznej – postępowanie egzekucyjne a prywatność osoby fizycznej

Definicja danych osobowych

Podstawy prawne ochrony danych osobowych w Polsce tworzą Konstytucja RP[1], ogólne rozporządzenie o ochronie danych (RODO)[2] oraz ustawa o ochronie danych osobowych[3]. Przepis art. 51 Konstytucji RP gwarantuje każdemu obywatelowi prawo do ochrony informacji. Władze państwowe nie posiadają prawa do pozyskiwania, gromadzenia oraz udostępniania innych informacji na temat obywateli niż te, które są niezbędne w każdym demokratycznym państwie prawnym. Każdy obywatel ma możliwość zażądania sprostowania i usunięcia informacji niepełnych, nieprawdziwych albo zebranych niezgodnie z ustawą, każdy posiada prawo dostępu do dokumentów oraz zbiorów danych, które dotyczą go w sposób bezpośredni.

[1] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 z późn. zm.).
[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119/1 z 4.05.2016), dalej w skrócie RODO.
[3] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000).

RODO wprowadza definicję legalną danych osobowych i – zgodnie z art. 4 pkt. 1 rozporządzenia – dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Za osobę możliwą do zidentyfikowania należy rozumieć osobę, której tożsamość można pośrednio lub bezpośrednio zidentyfikować. Przyjmuje się, że pojęcie danych osobowych obejmuje takie dane, które zawierają informacje dotyczące życia prywatnego i rodzinnego danej osoby czy też dotyczące działań podejmowanych przez daną osobę, w tym informacje dotyczące relacji zawodowych, zachowań ekonomicznych albo społecznych osoby, niezależnie od jej pozycji lub stanowiska, o ile służą zidentyfikowaniu konkretnej osoby fizycznej poprzez użycie informacji o charakterze osobowym. Zasadny jest pogląd, że jako dane osobowe powinny być kwalifikowane wszelkie informacje, gdy tylko możliwe jest ich odniesienie do konkretnej osoby[4].

W RODO wymieniono przykładowe identyfikatory jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy. Inne informacje o charakterze osobowym to płeć, kolor oczu, waga, wzrost lub inne dane biometryczne wskazujące na właściwości biologiczne, czynniki o charakterze fizycznym, fizjologicznym, ale również informacje dotyczące poglądów, przekonań, wypowiedzi czy życzeń. Chodzi zatem o czynniki określające fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej, a także informacje o wszelkich aktywnościach, relacjach zawodowych, zachowaniach ekonomicznych czy społecznych, niezależnie od zajmowanego stanowiska czy prawdziwości, o ile prowadzą do identyfikowalności danej osoby fizycznej[5]. Za dane osobowe należy więc uznać dane ekonomiczne, umożliwiające zidentyfikowanie osoby fizycznej, takie jak: wysokość zadłużenia, charakter roszczenia, wypłacalność dłużnika.

Z kolei zdaniem judykatury „dane osobowe to zespół wiadomości (komunikatów) o konkretnym człowieku, na tyle zintegrowany, że pozwala na jego zindywidualizowanie. Ten zbiór wiadomości obejmuje co najmniej informacje niezbędne do identyfikacji (imię, nazwisko, miejsce zamieszkania), jednakże do tego się nie ogranicza, gdyż mieszczą się w nim również dalsze informacje, wzmacniające stopień identyfikacji”[6].

[4] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych*, Warszawa 2007, s. 383–384.
[5] D. Lubasz, [w:] *RODO. Ogólne rozporządzenie o ochronie danych*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 171.
[6] Wyrok NSA z dnia 18 listopada 2009 r., sygn. akt I OSK 667/09, CBOSA.

Nie będą danymi osobowymi takie informacje, co do których nie da się ustalić, kogo one dotyczą[7]. Ponadto danymi osobowymi nie będą informacje, gdy wykorzystanie ich do identyfikacji osoby fizycznej będzie niewykonalne w praktyce, np. wiążąc się z nadmiernym nakładem czasu, kosztów i pracy ludzkiej[8].

Dane osobowe dzieli się na: dane osobowe zwykłe, typu: imię i nazwisko, adres zamieszkania, identyfikatory internetowe, numer telefonu, płeć, kolor oczu, waga, wzrost oraz – dane osobowe szczególne (wrażliwe). Za dane wrażliwe należy uważać dane o poglądach politycznych, religijnych lub filozoficznych, dane ujawniające pochodzenie rasowe lub etniczne, przynależność do partii politycznej, dane o stanie zdrowia, w tym dane o życiu seksualnym oraz o nałogach, dane na temat przeszłości kryminalnej z rejestru skazanych, jak również dane o orientacji seksualnej, dane biometryczne i dane genetyczne[9]. Zgodnie z RODO dane osobowe dotyczące zdrowia to dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej (w tym o korzystaniu z usług opieki zdrowotnej), które ujawniają informacje o stanie jej zdrowia (art. 4 pkt 15 RODO).

Dane biometryczne to dane osobowe dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiające lub potwierdzające jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Dane genetyczne dotyczą odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.

Kolizja wartości konstytucyjnych: dostęp do informacji publicznej a prywatność osoby fizycznej

Prawo dostępu do informacji publicznej uregulowane zostało w art. 61 Konstytucji RP i obejmuje możliwość uzyskiwania informacji o działalności organów władzy publicznej, osób pełniących funkcje publiczne, organów samorządu gospodarczego i zawodowego oraz innych osób i jednostek organizacyjnych w zakresie, w jakim podmioty te wykonują zadania władzy publicznej lub też

[7] D. Lubasz, [w:] *RODO…*, dz. cyt., s. 172-173.
[8] Tamże, s. 180.
[9] Tamże, s. 171.

gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa, a więc – prawo to jest określone bardzo szeroko[10]. Ograniczenie prawa dostępu do informacji publicznej może nastąpić wyłącznie ze względu na określone w odrębnych ustawach przesłanki dotyczącej ochrony wolności i praw innych osób oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa.

Szczegółowe zasady i tryb udzielania informacji uregulowany został przede wszystkim w ustawie o dostępie do informacji publicznej[11]. Każdy posiada prawo dostępu do informacji publicznej, na które składa się uprawnienie do uzyskania informacji publicznej i informacji przetworzonej dla interesu publicznego, uprawnienie wglądu do dokumentów urzędowych, uprawnienie dostępu do posiedzeń kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów, a także uprawnienie do niezwłocznego uzyskania informacji publicznej zawierającej aktualną wiedzę o sprawach publicznych. Obowiązek udostępniania informacji publicznej spoczywa na władzach publicznych oraz innych podmiotach wykonujących zadania publiczne, w tym na organach władzy publicznej, organach samorządów gospodarczych i zawodowych, podmiotach reprezentujących Skarb Państwa, podmiotach reprezentujących podmioty, osoby i jednostki organizacyjne, które wykonują zadania publiczne lub dysponują majątkiem publicznym. Podstawowym trybem udostępnienia informacji jest Biuletyn Informacji Publicznej, a jego wykorzystanie wyłącza obowiązek ponownego udostępnienia informacji na wniosek zainteresowanego podmiotu[12]. Informacje publiczne o szczególnym znaczeniu dla rozwoju innowacyjności w państwie i rozwoju społeczeństwa informacyjnego są udostępniane w centralnym repozytorium, zaś informacja publiczna, która nie została udostępniona w Biuletynie Informacji Publicznej lub centralnym repozytorium, jest udostępniana na wniosek.

Przesłanką obowiązku udostępnienia informacji publicznej jest jej posiadanie przez podmiot zobowiązany do jej udostępnienia. Zdaniem doktryny definicja ta stanowi normę interpretacyjną w stosowaniu ustawy, podkreślając dominację

[10] W. Sokolewicz, *Komentarz do art. 61*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. IV, red. L. Garlicki, Warszawa 2005, s. 5.

[11] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2001 r. Nr 112, poz. 1198 z późn. zm.).

[12] I. Kamińska. M. Rozbicka-Ostrowska, *Dostęp do informacji publicznej. Orzecznictwo sądów administracyjnych*, Warszawa 2007, s. 107.

jawności informacji nad tajnością[13]. Ponadto przesłanką kwalifikującą konkretną informację do kategorii informacji publicznej jest spełnianie przez nią kryterium przedmiotowego, przy czym decydująca jest treść i charakter konkretnej informacji, a nie podmiot, który znajduje się w jej posiadaniu[14].

W judykaturze sprawą publiczną jest działalność organów władzy publicznej (samorządów, osób i jednostek organizacyjnych) w zakresie wykonywania zadań władzy publicznej oraz gospodarowania mieniem publicznym, w tym mieniem komunalnym lub Skarbu Państwa. Informację publiczną stanowi jednocześnie treść wszelkiego rodzaju dokumentów odnoszących się do organów władzy publicznej, związanych z organem bądź w jakikolwiek sposób dotyczących organu, bez względu na to, co jest ich przedmiotem. Charakteru informacji publicznej nie mają natomiast wnioski w sprawach indywidualnych, wnioski będące postulatem wszczęcia postępowania w innej sprawie, wnioski dotyczące przyszłych działań organu w sprawach indywidualnych, wnioski stanowiące ingerencję w działalność sądów, a także wnioski dotyczące dokumentów prywatnych. Informacja publiczna powinna poza tym mieć swój materialny odpowiednik, nie można zobowiązać do udzielenia informacji, która nie istnieje[15]. W judykaturze upowszechnił się pogląd, że ocena, czy określona informacja stanowi informację publiczną w rozumieniu ustawy, nie może zależeć od tego, jaki wnioskodawca ubiega się o jej udostępnienie[16]. Dlatego też identyfikacja określonego we wniosku dokumentu, jako informacji publicznej, determinuje konieczność jego udostępnienia, chyba że w ocenie organu istnieją ustawowe przeszkody do udostępnienia informacji w określony sposób lub w określonej formie, bądź istnieją ustawowe podstawy do odmowy udostępnienia informacji publicznej, wówczas organ zobligowany jest do załatwienia wniosku w formie procesowej. Brak udostępnienia informacji publicznej i brak rozstrzygnięć procesowych w tym zakresie powoduje, że organ pozostaje w bezczynności. Środkiem przysługującym w tej sytuacji osobie domagającej się udostępnienia informacji publicznej jest skarga do sądu administracyjnego[17].

[13] P. Sitniewski, *Ustawa o dostępie do informacji publicznej. Komentarz*, Wrocław 2011, s. 14.
[14] M. Bidziński, *Konstytucyjne prawo dostępu do informacji publicznej*, „Przegląd Prawa Konstytucyjnego" 2012, nr 4, s. 127.
[15] Wyrok WSA w Gdańsku, z dnia 29 maja 2013, II SA/Gd 183/13, LEX nr 1321102
[16] Wyrok WSA w Lublinie z dnia 23 kwietnia 2013, II SAB/Lu 85/13, Rzeczpospolita PCD 2013/114/3.
[17] Wyrok NSA z dnia 12 grudnia 2012, I OSK 2149/12, LEX nr 1285158.

Prawo do informacji publicznej podlega ograniczeniu przede wszystkim w zakresie określonym ustawą o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych[18]. Ponadto prawo do informacji publicznej ulega ograniczeniu ze względu na ochronę prywatności osoby fizycznej oraz ze względu na tajemnicę przedsiębiorcy, gdy ujawnienie mogłoby zagrażać lub naruszać interes indywidualnego przedsiębiorcy. Ograniczenie ze względu na ochronę prywatności nie dotyczy jednak informacji o osobach pełniących funkcje publiczne mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji (art. 5 u.d.i.p.) Chodzi tu o możliwości przetwarzania danych osobowych osób pełniących funkcje publiczne, czyli funkcjonariuszy publicznych, członków organów jednostek samorządu terytorialnego i innych organów samorządowych, realizujących zadania publiczne, a także osób zatrudnionych w jednostce organizacyjnej dysponującej środkami publicznymi, chyba że osoba ta wykonuje wyłącznie czynności usługowe.

Konieczność ochrony prywatności osób, jako ograniczenie prawa dostępu do informacji publicznej, gwarantuje przepis art. 47 Konstytucji stanowiący, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Prawo do prywatności służy ochronie jednostki przed nieuzasadnionymi ingerencjami, a także przed zbyt daleko posuniętym zainteresowaniem sferą życia prywatnego przez osoby trzecie. Konstytucyjne prawo do prywatności jest jednak ograniczone w przypadku osób pełniących funkcje publiczne czy prowadzących działalność publiczną, których sfera ochrony prywatności jest mniejsza w stosunku do osób nie pełniących funkcji publicznych.

Z kolei z orzecznictwa sądowego wynika, że imię i nazwisko osoby fizycznej podlega ochronie danych osobowych, co skutkuje tym, że organ nie może udostępnić danych, które umożliwiałyby zidentyfikowanie osoby fizycznej. Konieczność ochrony danych osobowych nie zwalnia organu z udostępniania informacji publicznej, ale organ powinien ograniczyć dostęp wyłącznie do informacji umożliwiających identyfikację osób fizycznych, co w praktyce oznacza udostępnienie dokumentów odpowiednio zanonimizowanych. „Konieczność dokonania anonimizacji nie może być natomiast utożsamiana z odmową udzielenia informacji

[18] Wyrok WSA w Warszawie z dnia 14 sierpnia 2007 r., sygn. akt II SA/Wa 280/07, LEX nr 368239.

publicznej z uwagi na ochronę informacji niejawnych lub innych tajemnic ustawowo chronionych”[19]. Z orzecznictwa wynika również, że zasłonięcie określonych danych składających się na treść dokumentu można uznać za uzasadnioną anonimizację, o ile czynność ta nie pozbawi dokumentu waloru informacyjnego, jaki wynika ze złożonego wniosku[20].

O konieczności utajnienia części danych osobowych przy udzielaniu informacji publicznej przesądza zasada minimalizacji przetwarzania danych osobowych uregulowana w art. 5 ust. 1 lit. c. RODO, która wymaga, by przetwarzane dane były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Zasada ta wprowadza ilościowe ograniczenie zbierania i dalszego przetwarzania danych osobowych, zatem zbierane dane nie mogą być nadmierne[21]. Jednocześnie administrator powinien wdrożyć odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania (art. 25 ust. 2 RODO).

Wobec powyższego organ publiczny rozpoznający wniosek o udzielenie informacji publicznej powinien udzielić informacji publicznej, ale nie ujawniając danych osobowych osób, których dane dotyczą, chyba, że to dotyczy osób pełniących funkcje publiczne. Konieczność przeprowadzenia anonimizacji danych osobowych nie może bowiem prowadzić do udostępnienia jedynie części wnioskowanych dokumentów ani nie może spowodować, że dokument stanie się nieczytelny czy niezrozumiały. Nierzadko rozpoznanie wniosków o udzielenie informacji publicznej nie wymaga w ogóle przetwarzania danych osobowych.

Możliwa jest odmowa udostępnienia informacji publicznej w razie stwierdzenia zaistnienia przesłanki, która ogranicza dostęp do żądanych informacji publicznych, np. ze względu na ochronę prywatności czy ochronę tajemnic prawnie chronionych. Odmowa udostępnienia informacji publicznej przez organ władzy publicznej wymaga wydania decyzji administracyjnej w jurysdykcyjnym postępowaniu administracyjnym regulowanym przez Kodeks postępowania administracyjnego. Od wydanej decyzji wnioskodawca, któremu odmówiono udostępnienia

[19] Wyrok WSA w Poznaniu, z dnia 7 marca 2013, II SA/Po 47/13, LEX nr 1293515.
[20] Wyrok WSA w Krakowie z dnia 27 lipca 2018 r., II SAB/Kr 99/18, CBOSA.
[21] P. Drobek, [w:] *RODO. Ogólne rozporządzenie o ochronie danych*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 338.

informacji publicznej, ma prawo do złożenia wniosku o ponowne rozpatrzenie sprawy lub złożenia odwołania do organu wyższego stopnia, w zależności od organu, który wydał decyzję. W przypadku otrzymania kolejnej decyzji o odmowie podmiotowi pozostaje wniesienie skargi na rozstrzygnięcia zobowiązanych organów poprzez skierowanie skargi do sądu na rozstrzygnięcie organu. Skarga przysługuje stronie postępowania, czyli podmiotowi, któremu odmówiono prawa dostępu do informacji publicznej ze względu na wyłączenie jej jawności z powołaniem się na ochronę danych osobowych, prawo do prywatności czy klauzule tajności informacji niejawnych.

Dopuszczalność ujawniania danych osobowych przy udzielaniu informacji publicznej przewiduje art. 86 RODO, zgodnie z którym „dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlegają dany organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy niniejszego rozporządzenia". Zatem RODO nie zakazuje udostępniania danych osobowych przy udzielaniu informacji publicznej, ale wymaga poszanowania prawa do prywatności. Konieczność ochrony danych osobowych nie może natomiast wykluczyć prawa jednostki do informacji publicznej. Wynika to także z motywu 4 RODO, gdzie podkreślono, że prawo do ochrony danych osobowych nie jest prawem bezwzględnym i stąd należy je postrzegać w kontekście jego funkcji społecznej oraz wyważyć względem innych praw podstawowych przy zastosowaniu zasady proporcjonalności.

Postępowanie windykacyjne a RODO

Konieczność ochrony danych osobowych zachodzi również przy prowadzeniu postępowań windykacyjnych i egzekucyjnych. Postępowanie egzekucyjne w znaczeniu szerokim stanowi prawnie zorganizowane działanie organów egzekucyjnych z udziałem zainteresowanych podmiotów, mające na celu skuteczne urzeczywistnienie konkretnej normy prawnej, ustalonej w tytule egzekucyjnym, poprzez doprowadzenie za pomocą środków przymusu do uzyskania przez wierzyciela świadczenia należnego mu od dłużnika. W ramach postępowania

egzekucyjnego dochodzi do egzekucji, czyli stosowania środków przymusu właściwych dla określonego sposobu egzekucji, jakie organ egzekucyjny może w określonej kolejności zastosować w ramach wybranego przez wierzyciela sposobu egzekucji, w celu zaspokojenia roszczeń wierzyciela zgodnie z treścią tytułu wykonawczego[22]. Egzekucja obowiązków cywilnoprawnych dłużnika odbywa się w drodze egzekucji sądowej uregulowanej w Kodeksie postępowania cywilnego[23], przy czym postępowanie egzekucyjne zmierza bezpośrednio do zaspokojenia roszczenia wierzyciela poprzez uzyskanie świadczenia, do którego spełnienia dłużnik jest zobowiązany[24]. Natomiast postępowanie egzekucyjne w administracji to postępowanie w sprawach stosowania przez organy administracji państwowej środków przymusu, które mają na celu doprowadzenie do wykonania przez zobowiązanych ich obowiązków o charakterze publicznoprawnym[25]. W odróżnieniu od postępowania egzekucyjnego, to postępowanie windykacyjne obejmuje już czynności poprzedzające postępowanie egzekucyjne, a mające na celu uzyskanie świadczenia od dłużnika, w tym wysłanie wezwania do zapłaty, zlecenie sprawy do firmy windykacyjnej czy złożenie pozwu do sądu.

Prowadzenie postępowania egzekucyjnego i windykacyjnego wymaga przetwarzania danych osobowych dłużnika. W postępowaniu egzekucyjnym dotyczy to przetwarzania danych dłużnika egzekwowanego, którym jest podmiot, w stosunku do którego istnieje, w przypadku egzekucji sądowej, wymagalne roszczenie stwierdzone tytułem wykonawczym, oraz w stosunku do którego wierzyciel wystąpił o przymusowe zrealizowanie obowiązku nałożonego w tym tytule. Do przetwarzania danych uprawnione są wtedy organy egzekucyjne, którymi są sądy rejonowe oraz komornicy, przy czym organy te są upoważnione do wykonywania tytułów wykonawczych za pomocą przymusu państwowego. Przetwarzania danych osobowych dokonuje również wierzyciel egzekucyjny, który jest inicjatorem oraz dysponentem postępowania egzekucyjnego, zaś jego uprawnienie wynika z tytułu wykonawczego. Natomiast w ramach postępowania windykacyjnego uprawnionym do przetwarzania danych osobowych dłużnika jest wierzyciel, a także firma windykacyjna działająca w imieniu wierzyciela i na jego zlecenie.

[22] R. Kowalkowski, *Encyklopedia egzekucji sądowej*, Sopot 2002, s. 61.
[23] Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2014 r., poz. 10 z późn. zm.).
[24] A. Marciniak, *Sądowe postępowanie egzekucyjne*, Warszawa 2013, s. 17.
[25] L. Klatt-Wertelecka, *Niedopuszczalność egzekucji administracyjnej*, Warszawa 2009, s. 105.

Istotą przetwarzania danych osobowych według definicji legalnej jest wykonywanie operacji lub zestawu operacji na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany (art. 4 pkt 2 RODO). Przetwarzaniem danych osobowych jest więc każde działanie na danych osobowych, niezależnie od tego, czy odbywa się techniką tradycyjną, czy przy wykorzystywaniu systemów informatycznych, a operacje przetwarzania danych osobowych to: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Operacje te są działaniami zmierzającymi do wykonania określonego celu[26].

Przetwarzanie danych zgodnie z RODO

Podstawę prawną do przetwarzania przez wierzyciela danych osobowych dłużnika stanowi art. 6. ust. 1 pkt b RODO, który dopuszcza przetwarzanie danych osobowych, gdy jest ono niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy. Przepis ten zezwala na przetwarzanie danych osoby, która jest stroną umowy i opiera się na woli osoby, jako podmiotu danych, która ukierunkowana jest w prawie na zawarcie umowy, ale skutkiem wyrażenia takiej woli jest zarazem dopuszczenie przetwarzania danych osobowych w celu wykonania umowy. Zatem warunkiem przetwarzania danych osobowych dłużnika na tej podstawie jest istnienie umowy, dłużnik jest stroną tej umowy, a poza tym przetwarzanie danych osobowych musi być niezbędne do wykonania umowy[27]. Niezbędność przetwarzania dla wykonania umowy oznacza, że przetwarzanie danych osobowych ma prowadzić do realizacji praw i obowiązków mających swoje źródło w umowie i przepisach uzupełniających jej treść, a więc wymagany jest bezpośredni związek pomiędzy realizacją praw lub obowiązków wynikających z umowy a potrzebą przetwarzania danych osobowych[28].

[26] W. Chomiczewski, [w:] *RODO. Ogólne rozporządzenie o ochronie danych*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 188.
[27] Tamże, s. 359.
[28] Tamże, s. 362.

Kolejną podstawę przetwarzania danych osobowych dłużnika reguluje art. 6 ust. 1 pkt f RODO, który dopuszcza przetwarzanie bez zgody podmiotu danych, o ile „przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem". Przyjmuje się w doktrynie, że ta przesłanka legalizacyjna przetwarzania danych wymaga kumulatywnego spełnienia dwóch przesłanek, tzn. musi zaistnieć prawnie uzasadniony interes, który jest realizowany przez administratora lub przez stronę trzecią, a ponadto przetwarzanie danych osobowych jest niezbędne dla realizacji celu wynikającego z powyższego interesu. Jednocześnie spełniona musi być przesłanka o charakterze negatywnym w postaci występowania interesów lub podstawowych praw i wolności podmiotu danych mających charakter nadrzędny wobec prawnie uzasadnionych interesów administratora lub strony trzeciej[29]. Przesłanka prawnie uzasadnionego interesu oznacza istnienie interesu wynikającego z przepisów prawa, a także interesu, który jest zgodny z prawem, przy czym takim interesem będzie interes gospodarczy. Ponadto musi występować bezpośredni związek między ochroną prawnie uzasadnionych interesów a potrzebą przetwarzania danych osobowych[30]. Jeżeli zatem nie ma umowy między dłużnikiem a wierzycielem, to wierzyciel może przetwarzać dane w postępowaniu windykacyjnym na tej podstawie.

W granicach określonych przepisami RODO wierzyciel ma prawa przetwarzać imię i nazwisko dłużnika, PESEL, adres zamieszkania, adres do korespondencji oraz dane dotyczące składników majątku. Takie dane może również przetwarzać firma windykacyjna, której powierzone zostały dane osobowe dłużników, przy czym może je wykorzystywać wyłącznie w celach określonych w umowie zawartej przez nią z wierzycielem.

Z kolei na podstawie art. 6 ust. 1 pkt c i e RODO w związku z art. 2-3 oraz art. 37a Ustawy z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji[31]

[29] Tamże, s. 390.
[30] Tamże, s. 393-394.
[31] Ustawa z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji (Dz.U. z 2015 r., poz. 790 z późn. zm.).

komornik ma prawo do przetwarzania danych osobowych dłużnika w celu wypełnienia obowiązku wykonania czynności egzekucji. Wskazane przepisy RODO dopuszczają, po pierwsze, przetwarzanie, gdy jest ono niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze[32], o ile obowiązek prawny administratora wynika z przepisu prawa obowiązującego, a takimi są wymienione przepisy ustawy o komornikach sądowych i egzekucji. Po drugie, podstawą przetwarzania jest niezbędność do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, a przecież komornik jest funkcjonariuszem publicznym. Komornik w przeciwieństwie do wierzyciela może przetwarzać dane osobowe w szerszym zakresie, gdyż może dodatkowo przetwarzać dane osobowe dotyczące siedziby pracodawcy dłużnika lub siedziby prowadzonej przez dłużnika działalności gospodarczej, NIP, REGON, dane dotyczące prowadzonych na rzecz dłużnika kont bankowych, dane dotyczące członków rodziny, o ile mają związek z podjętymi czynnościami dotyczącymi środków prawnie przeznaczonych do zajęcia komorniczego. Zakres tych danych i niezbędność ich przetwarzania wynika z obowiązków nałożonych na komornika jako organu egzekucyjnego oraz realizacji celu wyegzekwowania świadczenia od dłużnika.

Podsumowanie

Przetwarzanie danych osobowych dłużnika w postępowaniu windykacyjnym, a także udostępnianie danych osobowych dłużnika firmom windykacyjnym, jest uzasadnione, gdyż w przeciwnym razie byłoby to nienależytym przywilejem dłużnika, z którym nie można byłoby się nawet skontaktować, z uwagi na brak dostępu do danych osobowych[33]. Jednocześnie przesłanki legalizacyjne przetwarzania danych osobowych dłużnika bez jego zgody warunkują dochodzenie od dłużnika roszczeń, a bez nich dłużnik mógłby, odmawiając prawa do przetwarzania danych osobowych, uchylać się od wykonania zobowiązań wobec wierzyciela, który byłby de facto pozbawiony ochrony swoich interesów majątkowych. Dopuszczalność przetwarzania danych osobowych w celach windykacyjnych obejmuje m.in. przekazanie danych dłużnika firmie windykacyjnej, upublicznienie danych

[32] D. Lubasz, [w:] *RODO…*, dz. cyt., s. 368.
[33] Wyrok WSA w Warszawie z dnia 16 listopada 2005 r., sygn. akt II SA/Wa 139/05, CBOSA.

dotyczących wierzytelności celem dokonania cesji wierzytelności czy ujawnienia danych dłużnika w ogólnodostępnych bazach dłużników.

Samo przetwarzanie danych osobowych dłużnika w postępowaniu windykacyjnym i egzekucyjnym, choć dopuszczalne, to musi jednak pozostawać w zgodzie z zasadami, które reguluje RODO. Chodzi tu przede wszystkim o zasadę minimalizacji przetwarzania danych, ograniczającą przetwarzanie do danych osobowych niezbędnych do realizacji celów, w których są przetwarzane, a także zasadę prawidłowości przetwarzania danych, zasadę przejrzystości, zasadę ograniczenia, przechowywania czy zasadę bezpieczeństwa danych i zabezpieczenia ich przed udostępnieniem ich osobom.

Bibliografia

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2007.

Bidziński M., *Konstytucyjne prawo dostępu do informacji publicznej*, „Przegląd Prawa Konstytucyjnego" 2012, nr 4.

Kamińska I., Rozbicka-Ostrowska M., *Dostęp do informacji publicznej. Orzecznictwo sądów administracyjnych*, Warszawa 2007.

Klatt-Wertelecka L., *Niedopuszczalność egzekucji administracyjnej*, Warszawa 2009.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 z późn. zm.).

Kowalkowski R., *Encyklopedia egzekucji sądowej*, Sopot 2002.

Marciniak A., *Sądowe postępowanie egzekucyjne*, Warszawa 2013.

RODO. Ogólne rozporządzenie o ochronie danych, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119/1 z 04.05.2016).

Sitniewski P., *Ustawa o dostępie do informacji publicznej. Komentarz*, Wrocław 2011.

Sokolewicz W., *Komentarz do art. 61*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. IV, red. L. Garlicki, Warszawa 2005.

Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2014 r., poz. 10 z późn. zm.).

Ustawa z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji (Dz.U. z 2015 r., poz. 790 z późn. zm.).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. Nr 112, poz. 1198 z późn. zm.).

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

Wyrok NSA z dnia 18 listopada 2009 r., sygn. akt I OSK 667/09, CBOSA.

Wyrok NSA z dnia 12 grudnia 2012 r., I OSK 2149/12, LEX nr 1285158.

Wyrok WSA w Gdańsku z dnia 29 maja 2013 r., II SA/Gd 183/13, LEX nr 1321102.

Wyrok WSA w Krakowie z dnia 27 lipca 2018 r., II SAB/Kr 99/18, CBOSA.

Wyrok WSA w Lublinie z dnia 23 kwietnia 2013 r., II SAB/Lu 85/13, Rzeczpospolita PCD 2013/114/3.

Wyrok WSA w Poznaniu z dnia 7 marca 2013 r., II SA/Po 47/13, LEX nr 1293515.

Wyrok WSA w Warszawie z dnia 16 listopada 2005 r., sygn. akt II SA/Wa 139/05, CBOSA.

Wyrok WSA w Warszawie z dnia 14 sierpnia 2007 r., sygn. akt II SA/Wa 280/07, LEX nr 368239.

The transparency of access to public information – enforcement proceedings and the privacy of a natural person

Summary: The right to the protection of personal data lies within the individual's right to privacy, and the essence of this right is manifested in the decision by the natural person about the scope and extent of sharing information about their life, including their personal data. The right to the protection of personal data competes with the right of access to public information, which is not absolute and is subject to restrictions, including the protection of the right to privacy. Personal data protection applies to all forms of data processing by data controllers, including the context of debt recovery proceedings against the debtor. The basic legalization criterion for the processing of personal data is consent to the processing of personal data. However, the legislator also provided for other legalization requirements for the processing of personal data without the consent of the data subject, which constitutes the legal basis for the processing of the debtor's personal data in debt collection proceedings. These issues are the subject of this article, including the analysis of the provisions of the GDPR and their interpretation by doctrine and jurisprudence.
Keywords: *transparency, principle of openness, debt recovery, RODO, privacy, public information access*

ARTUR GAJOWNICZEK
ORCID: 0000-0002-8770-7089
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych

Wybrane aspekty funkcjonowania Krajowego Systemu Cyberbezpieczeństwa w jednostkach samorządu terytorialnego na przykładzie województwa mazowieckiego

Problematyka cyberbezpieczeństwa w jednostkach samorządu terytorialnego (JST) nabiera szczególnego znaczenia w kontekście rozwoju e-administracji. Pojawia się wiele platform o zasięgu regionalnym (Wrota Mazowsza, Wrota Podlasia) oraz ogólnopolskim (elektroniczna Platforma Usług Administracji Publicznej – e-PUAP), które służą mieszkańcom i przedsiębiorcom do załatwiania spraw administracyjnych drogą elektroniczną. Kontakt JST z organami administracji rządowej (wojewodami) i centralnymi (Zakładem Ubezpieczeń Społecznych, Urzędem Skarbowym) oraz wszelkie rozliczenia finansowe również odbywają się drogą elektroniczną[1]. Zakres świadczenia usług przez JST w cyberprzestrzeni oraz przekazywania i przetwarzania informacji w systemach teleinformatycznych na przestrzeni ostatnich 15 lat znacznie się zwiększył. Podwaliny budowy e-administracji w Polsce stanowiły akty prawne uchwalane w latach 2001–2005[2].

[1] Zob. P. Nadybski, *Elektroniczna administracja w Polsce – ograniczenia i bariery*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy" 2013, nr 9, s. 31-33.

[2] Akty prawne uchwalane w latach 2001-2005: Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych; Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym; Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej; Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną; Ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach

W literaturze przedmiotu wskazywane są dwa najważniejsze akty normatywne tworzące podstawy e-administracji Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, która nałożyła na władze publiczne obowiązek udostępniania informacji publicznych oraz Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[3].

Jednocześnie JST stały się potencjalnym podmiotem ataków i włamań do zasobów gromadzonych w przestrzeni cyfrowej. Spowodowało to konieczność identyfikowania zagrożeń występujących w cyberprzestrzeni i stosowania skutecznych narzędzi przeciwdziałania na wypadek prób przełamania zabezpieczeń. W literaturze przedmiotu podkreślane są dwa aspekty zagrożenia informatycznego, w którym celem jest technologia informatyczna lub jest ona narzędziem oraz formy zagrożenia związanego z Internetem: włamania, wirusy, ataki konwencjonalne[4]. Natomiast o skali zagrożeń, jakie wiążą się z rozwojem i wykorzystaniem Internetu, świadczą statystyki publikowane przez zespół CERT (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego). W 2016 r. CERT Polska działający w NASK – Państwowym Instytucie Badawczym – obsłużył 1926 incydentów, tj. o 32% więcej niż w 2015 r. Do najczęściej zgłaszanych należą następujące kategorie incydentów: oszustwa komputerowe (55,5%), obraźliwe i nielegalne treści (12,31%), złośliwe oprogramowanie (10,96%), próby włamań (5,66%), gromadzenie informacji (3,37%), włamania (2,8%), dostępność zasobów (2,34%), atak na bezpieczeństwo informacji (2,34%), inne (4,72%). Dla przykładu phishing (podszywanie się pod znane marki celem wyłudzenia wrażliwych danych) był zgłaszany do CERT Polska 722 584 razy, a otrzymanych zgłoszeń dotyczących unikalnych adresów IP, które są narażone na ataki oraz wyciek informacji, było 1,8 miliona[5].

płatniczych; Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

[3] R. Perdał, *Czynniki rozwoju elektronicznej administracji w samorządzie lokalnym w Polsce*, Poznań 2014, s. 46-48.

[4] Zob. S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki – organizacji – państwa*, Warszawa 2016, s. 207-209.

[5] *Krajobraz bezpieczeństwa polskiego Internetu 2016. Raport roczny z działalności CERT Polska*, NASK, https://www.cert.pl/PDF/Raport_CP_2016.pdf [dostęp marzec 2018].

W literaturze przedmiotu często podkreślana jest zależność między bezpieczeństwem informacji, w tym w systemach teleinformatycznych, a bezpieczeństwem w szerokim znaczeniu – dla administracji publicznej i JST[6]. Bardzo ważnym aspektem prowadzenia aktywności w cyberprzestrzeni jest postęp technologiczny zarówno w zakresie sprzętowym, jak i wykorzystywanego oprogramowania. Brak reakcji na zmiany technologiczne w sferze sprzętowej lub uaktualnienia oprogramowania może powodować znaczące skutki dla bezpieczeństwa systemów teleinformatycznych. Zmiany w podejściu do omawianego zagadnienia widać szczególnie wyraźnie w ewolucji samej definicji cyberbezpieczeństwa, która na przestrzeni ostatnich lat zmieniała się w aktach prawnych i teorii bezpieczeństwa. Podobnie zmianom ulegał zakres podmiotowy tego pojęcia, który dotyczył początkowo tylko sektora bankowego i biznesowego oraz administracji rządowej, a w kolejnych latach obejmował inne podmioty, w tym JST[7].

W 2013 r., powstał pierwszy w Polsce strategiczny dokument w zakresie cyberbezpieczeństwa: Polityka ochrony cyberprzestrzeni RP. Zostały w nim zdefiniowane między innymi pojęcia: „bezpieczeństwo cyberprzestrzeni – jako zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych, mający na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni" oraz „cyberprzestrzeń RP (CRP) – cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)"[8]. Cel strategiczny został określony w dokumencie jako osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa. Polityka została przyjęta uchwałą Rady Ministrów 25 czerwca 2013 r. i obowiązywała tylko administrację rządową. W 2017 r. została ona zastąpiona przez Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 (Krajowe Ramy)[9]. W dokumencie określono cztery cele, które wskazywały na potrzeby wynikające z rozbudowy Krajowego Systemu

[6] Zob. R. Cichocki, P. Jatkiewicz, *Bezpieczeństwo informacji w jednostkach samorządu terytorialnego*, „Roczniki Kolegium Analiz Ekonomicznych SGH" 2013, z. 99.

[7] Zob. D. Liszak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016.

[8] Definicje z Polityki ochrony cyberprzestrzeni, uchwała RM nr 111/2013 z dnia 25 czerwca 2013 r.

[9] Dokument został przyjęty 9 maja 2017 r. uchwałą Rady Ministrów nr 52/2017. Polityka ochrony cyberprzestrzeni RP, https://cyberpolicy.nask.pl/polityka-ochrony-cyberprzestrzeni-rp/ [dostęp 27.03.2020].

Cyberbezpieczeństwa. Pierwszy dotyczył osiągnięcia zdolności do skoordynowanego działania w skali kraju, które pozwoli zapobiegać, wykrywać, zwalczać oraz minimalizować skutki incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa. Kolejny cel zakładał wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom. Trzeci cel związany był ze zwiększaniem potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni. Ostatni z celów wymienionych w Krajowych Ramach zmierzał do zbudowania silnej pozycji międzynarodowej Polski w obszarze cyberbezpieczeństwa[10]. W Krajowych Ramach pojawiła się następująca definicja cyberbezpieczeństwa: „odporność systemów teleinformatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych przez te sieci i systemy informatyczne”[11]. Krajowe Ramy zostały również ustanowione tylko dla administracji rządowej: na pięć lat.

22 października 2019 r. Rada Ministrów przyjęła uchwałę w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (strategii cyberbezpieczeństwa)[12]. Dokument obowiązuje od 31 października 2019 r. i zastąpił Krajowe Ramy. Podstawa prawna przyjęcia strategii cyberbezpieczeństwa wynika z art. 68 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (ustawa o krajowym systemie)[13]. Głównym celem przyjęcia i wdrożenia strategii cyberbezpieczeństwa jest podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym, a także promowanie dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.

[10] Zob. M. Wrzosek, *Krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, https://cyberpolicy.nask.pl/rb-dokumenty-krajowe-2-krajowe-ramy-polityki-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/ [dostęp 12.12.2019].

[11] Uchwała nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.

[12] Uchwała Nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M.P. z 2019 r., 1037).

[13] Ustawa z dnia 5 lipca 2018 r.o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

W obecnie obowiązującym stanie prawnym w art. 2 ustawy o krajowym systemie została zawarta definicja cyberbezpieczeństwa oznaczająca „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”[14]. W literaturze przedmiotu znajdujemy wiele definicji tego pojęcia, w ocenie autora najbardziej trafna jest szersza definicja zawierająca nie tylko sprawy ochrony skuteczności zabezpieczeń technicznych infrastruktury informacyjnej, ale również aspekt np. organizacyjny: „cyberbezpieczeństwo – proces, na który składają się działania podejmowane przy pomocy środków technicznych i nietechnicznych dla ochrony cyberprzestrzeni, w tym urządzeń, oprogramowania oraz informacji lub danych”[15].

Ustawa o krajowym systemie jest wdrożeniem do polskiego porządku prawnego Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. Dyrektywa NIS)[16]. Zobowiązuje ona państwa członkowskie do zagwarantowania minimalnego poziomu cyberbezpieczeństwa poprzez ustanowienie organów właściwych oraz pojedynczych punktów kontaktowych do spraw cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcie krajowych strategii w zakresie cyberbezpieczeństwa[17].

Ustawa o krajowym systemie usankcjonowała trzy podmioty na poziomie krajowym, które zajmują się reagowaniem na incydenty komputerowe i zarządzanie nimi. Są to CSIRT GOV, CSIRT MON, CSIRT NASK[18]. Obsługą incydentów

[14] Ustawa z dnia 5 lipca 2018 r., o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560 ze zm.).

[15] *Vademecum bezpieczeństwa*, red. O. Wasiuta, R. Klepka, R. Kopeć, Kraków 2018, s. 223.

[16] Dz.Urz. UE L 194/1 z 2016 r.

[17] M. Sławińska, *Rok funkcjonowania ustawy o krajowym systemie cyberbezpieczeństwa – najważniejsze postanowienia i rozwiązania,* https://rcb.gov.pl/rok-funkcjonowania-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-najwazniejsze-postanowienia-i-rozwiazania/ [dostęp 27.04.2020].

[18] CSIRT GOV – prowadzony jest przez Agencję Bezpieczeństwa Wewnętrznego. Główne zadania CSIRT GOV to: rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych, z punktu widzenia ciągłości funkcjonowania państwa, systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej,

zgłaszanych przez JST jest CSIRT NASK prowadzony przez Naukową i Akademicką Sieć Komputerową. Zespoły CSIRT zapewniają spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym – są w europejskiej sieci CSIRT oraz przekazują do innych Państw i innych Punktów Kontaktowych informacje o incydentach. Zespołowi CERT Polska zostały powierzone obowiązki CSIRT NASK wynikające z ustawy o krajowym systemie. Podstawowe obowiązki wskazane w tej ustawie dla JST to wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa, szkolenie osób z cyberbezpieczeństwa w tym identyfikacji zagrożeń oraz zgłaszanie i obsługa incydentów będących zdarzeniami mającymi niekorzystny wpływ na cyberbezpieczeństwo[19]. Wagę tematu identyfikacji zagrożeń pokazuje przykład znaczącego incydentu, który miał miejsce w Holandii. Latem 2011 r. holenderski system zabezpieczeń informatycznych organu certyfikującego DigiNotar został poważnie naruszony, umożliwiając atakującym wygenerowanie fałszywych certyfikatów autentyczności. Przykład ilustruje naturę jednego z najpoważniejszych rodzajów utraty integralności urzędowego systemu certyfikacji[20].

a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej. CSIRT GOV zobowiązany jest do koordynacji incydentów zgłaszanych przez następujące podmioty: organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały; ZUS, KRUS, NFZ; Narodowy Bank Polski, Bank Gospodarstwa Krajowego. CSIRT MON – prowadzony przez Ministerstwo Obrony Narodowej. CSIRT MON zobowiązany jest do koordynacji incydentów zgłaszanych przez następujące podmioty: podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej; przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa jest Minister Obrony Narodowej. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT), https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt [dostęp 16.03.2020].

[19] CSIRT NASK, www.cert.gov.pl [dostęp 14.03.2020].

[20] Fałszywe certyfikaty, będące wynikiem naruszenia, zostały wykorzystane do podsłuchu komunikacji online setek tysięcy obywateli. Po naruszeniu wiele rządowych stron internetowych w Holandii było niedostępnych i uznanych za niebezpieczne. Rząd przejął zarządzanie operacyjne systemami DigiNotar, a sama firma wkrótce ogłosiła upadłość. Również utrata klucza prywatnego dowolnego rodzaju certyfikatu cyfrowego oznacza natychmiastowe unieważnienie danego certyfikatu. Szkodliwe ataki mogą wpływać na wszystkie rodzaje wyżej wymienionych usług zaufania

Zebrane dane ponad rok od wdrożenia ustawy o krajowym systemie (ustawa weszła w życie 28 sierpnia 2018 r.), dają możliwość podsumowania funkcjonowania systemu cyberbezpieczeństwa w Polsce przez podmioty do tego zobowiązane, w tym JST[21]. W literaturze przedmiotu zagadnienie funkcjonowania Krajowego Systemu Cyberbezpieczeństwa w JST jest nadal w niewielkim stopniu zbadane i opisane. Celem ogólnym badań prowadzonych przez autora od czerwca do sierpnia 2019 było bezpieczeństwo informacyjne, w tym ocena wdrożenia e-administracji i zapisów ustawy o krajowym systemie w jednostkach samorządowych na Mazowszu. Województwo mazowieckie zostało wybrane jako teren przeprowadzenia badań, ponieważ pod kątem poziomu innowacyjności jest jednym z najprężniej rozwijających się regionów w Polsce oraz umiarkowanym innowatorem wśród krajów Unii Europejskiej[22]. Jednocześnie system Elektronicznego Zarządzania Dokumentacją EZD wykorzystywało 59,6% ogółu urzędów w województwie mazowieckim, co spowodowało umieszczenie go na 7 pozycji w zestawieniu 16 województw[23]. Średnia stopa relatywnego ubóstwa w 2017 r.

i obejmować szereg usług, takich jak podpisy elektroniczne, znaczniki czasu i uwierzytelnianie witryn internetowych. Obecnie uwierzytelnianie strony internetowej, które pozwala użytkownikom zweryfikować autentyczność strony internetowej i powiązać osobę prawną ze stroną internetową, staje się dość powszechne. Źródło: *Implementation of article 15, of the draft regulation on electronic identification and trusted services for electronictransactions in the internal market*, s. 7-8 www.enisa.europa.eu, tłum. własne [dostęp 17.11.2019].

[21] Ustawa o krajowym systemie cyberbezpieczeństwa wprowadziła pojęcie systemu cyberbezpieczeństwa, który „ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych, służących do świadczenia tych usług oraz zapewnienie obsługi incydentów". Art. 2 pkt 4, Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

[22] Poziom innowacyjności – złożony wskaźnik opracowywany przez Komisję Europejską, na podstawie którego kraje UE sklasyfikowane są w czterech grupach w zależności od poziomu wskaźnika względem średniej unijnej: liderzy innowacji (powyżej 120% średniej unijnej), kraje doganiające (90-120%), umiarkowani innowatorzy (50-90%), słabi innowatorzy (poniżej 50%) Na podstawie *Atlasu statystycznego województwa mazowieckiego*, http://warszawa.stat.gov.pl/publikacje-i-foldery/inne-opracowania/atlas-statystyczny-wojewodztwa-mazowieckiego,28,1.html [dostęp 07.12.2018].

[23] *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2013–2017*, https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/1/11/1/spoleczenstwo_informacyjne_w_polsce._wyniki_badan_statystycznych_z_lat_2013-2017.pdf [dostęp 15.12.2018].

mieszkańców województwa mazowieckiego wynosiła 10%[24], z czego dla Warszawy wynosiła ona 6%, dla podregionu warszawskiego zachodniego ok 10%, dla podregionu warszawskiego wschodniego – 14% i dla podregionów peryferyjnych aż 21-26% w stosunku do średniej stopy relatywnego ubóstwa w całym kraju – na poziomie 17,7%; województwo mazowieckie stanowi więc próbę reprezentatywną[25]. Reasumując, podobnie jak w całej Polsce, w województwie mazowieckim jest pełno dysproporcji i kontrastów, zarówno pod względem rozwoju gospodarczego poszczególnych gmin, jak i zaludnienia oraz ubóstwa. Właśnie te cechy decydują o tym, że jest to optymalny teren badawczy dla zakresu tematycznego dotyczącego sfery bezpieczeństwa w cyberprzestrzeni.

Badanie zostało przeprowadzone w formie elektronicznej, żeby zapewnić respondentom anonimowość udzielania odpowiedzi[26]. Na podstawie ustawy o dostępie do informacji publicznej został skierowany wniosek do samorządów z województwa mazowieckiego o udzielenie informacji publicznej[27]. Jednostki administracji publicznej mają ustawowy obowiązek udzielić odpowiedzi w ciągu 14 dni od otrzymania wniosku w określonej we wniosku formie.

Sondażem diagnostycznym objęto próbę reprezentatywną dla Polski, zawierającą wszystkie JST na Mazowszu. Wysłano ankietę za pomocą systemu e-PUAP do 37 powiatów (zwanych dalej powiatem ziemskim) i 5 miast na prawach powiatu (zwanych dalej powiatem miejskim), 35 gmin miejskich, 53 gmin miejsko-wiejskich i 226 gmin wiejskich. Odpowiedzi udzieliło 71% procent respondentów, z czego otrzymano z powiatów ziemskich 54% (20 sztuk ankiet) i z miast na prawach powiatu 60% (tj. 3 ankiety). Najwięcej wypełnionych ankiet otrzymano z gmin miejskich (aż 91%, czyli 32 ankiety). Na wysokim poziomie

[24] Coraz mniej mieszkańców Mazowsza żyje w ubóstwie, https://warszawa.stat.gov.pl/dla-mediow/informacje-prasowe/coraz-mniej-mieszkancow-mazowsza-zyje-w-ubostwie,151,1.html [dostęp 01.06.2019].

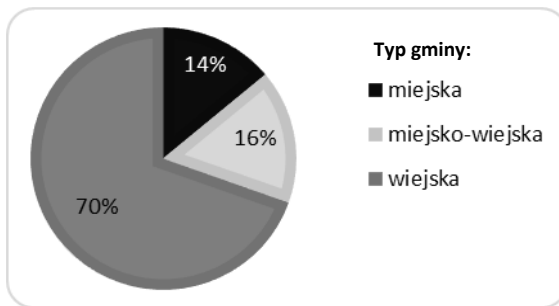
[25] Kancelaria Senatu, *Zróżnicowanie województwa mazowieckiego pod względem historycznym, demograficznym i warunków życia. Korekty do podziału terytorialnego kraju*, https://www.senat.gov.pl/gfx/senat/pl/senatekspertyzy/3842/plik/oe-256-internet.pdf [dostęp 02.01.2019].

[26] We wniosku o udzielenie informacji publicznej skierowanym do JST znajdował się link do adresu www portalu e-Badania, gdzie została przygotowana ankieta zawierająca pytania zamknięte i otwarte.

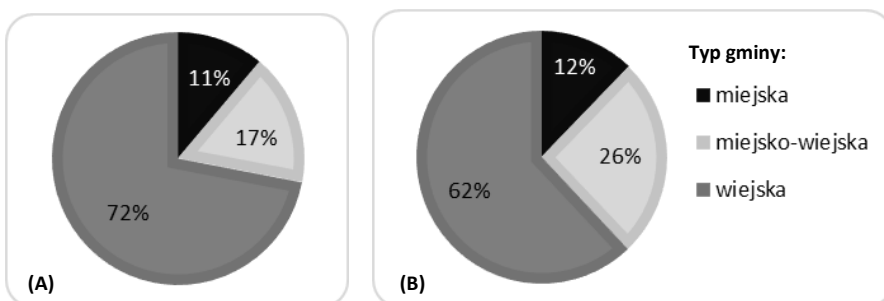
[27] Ustawa z dnia z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2018 r., poz. 1330).

prezentuje się odsetek respondentów z gmin miejsko-wiejskich (prawie 72%, tj. 38 ankiet) i gmin wiejskich (prawie 71%, czyli 160 ankiet). Część JST nie wypełniła ankiety, argumentując, że treść zadawanych pytań nie stanowi informacji publicznej.

Udział procentowy respondentów z poszczególnych gmin jest zbliżony do udziału procentowego gmin na Mazowszu, co oznacza, że zebrane dane są reprezentatywne dla całego województwa. Na rysunkach 1 i 2 zestawiono udział respondentów z poszczególnych typów gmin objętych badaniem z procentowym udziałem typów gmin na Mazowszu i w kraju.



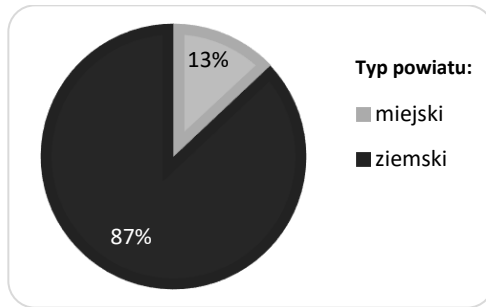
Rys. 1. Udział procentowy respondentów z poszczególnych typów gmin objętych badaniem
Źródło: opracowanie własne



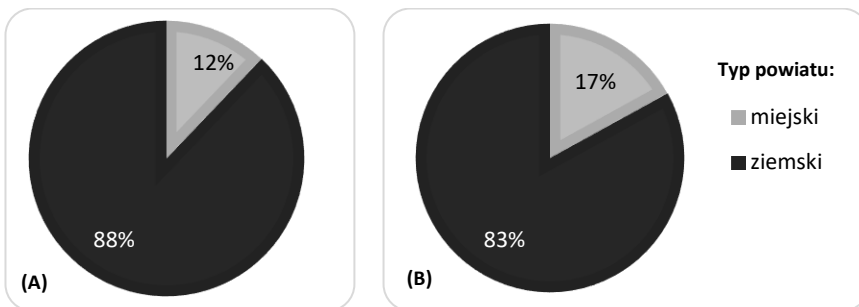
Rys. 2. Typy gmin na Mazowszu (A) i w Polsce (B) w ujęciu procentowym
Źródło: opracowanie własne

Podobne wnioski można wyciągnąć, obserwując dane na poziomie powiatu. Również w tym przypadku badana próba jest reprezentatywna dla całego województwa (różnica na poziomie 1%). Z kolei różnica 4 punktów procentowych dotyczy powiatów ziemskich i miejskich w skali Polski w porównaniu do próby

badawczej. Na rysunkach 3 i 4 przedstawiono porównanie rozkładu poszczególnych typów powiatów (ziemski i miejski) na Mazowszu i w Polsce z udziałem procentowym respondentów uczestniczących w badaniu sondażowym z poszczególnych powiatów.

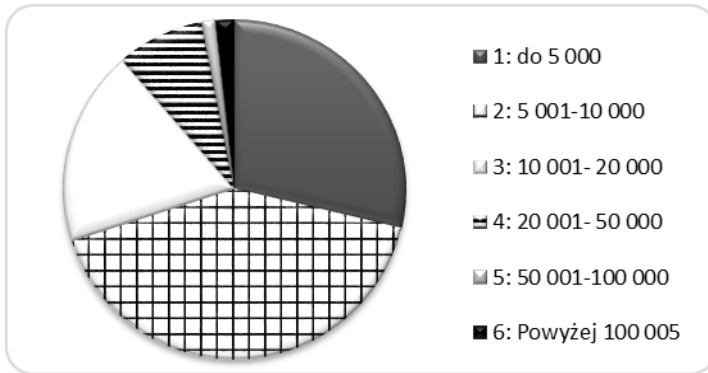


Rys. 3. Udział procentowy respondentów z poszczególnych typów powiatów objętych badaniem
Źródło: opracowanie własne



Rys. 4. Typy powiatów na Mazowszu (A) i w Polsce (B) w ujęciu procentowym
Źródło: opracowanie własne

Ankieta zasadniczo składała się z pytań zamkniętych, przy czym w niektórych przypadkach wybór określonej odpowiedzi wiązał się z możliwością jej uzupełnienia i rozwinięcia. Pierwsze trzy pytania dotyczyły identyfikacji rodzaju JST, jej cech i liczby mieszkańców (rysunek 5). Wśród badanych gmin dominują jednostki z relatywnie niedużą liczbą mieszkańców od 5 001 do 10 000 (41% ogółu) oraz do 5 000 (29% próby). W dziewiętnastu badanych jednostkach mieszka od 20 001 do 50 000 mieszkańców (8% całości). Najbardziej liczebne gminy, tj. takie, których liczba mieszkańców mieści się w zakresie od 50 001 do 100 000 (9% ogółu) i powyżej 100 000 (13% ogółu), stanowiły w badaniu najmniejszą grupę.



Rys.5. Liczba mieszkańców w gminach objętych badaniem [%]
Źródło: opracowanie własne

Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa jednym z podstawowych obowiązków JST jest zgłaszanie incydentów, czyli zdarzeń, które mają lub mogą mieć niekorzystny wpływ na odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[28]. Kolejnym obowiązkiem JST jest wyznaczenie w jednostce osoby do kontaktów z CSIRT-NASK oraz współpraca z CSIRT-NASK. Tego problemu dotyczyły w ankiecie następujące pytania:

- Czy w JST lub podległych jednostkach organizacyjnych w ostatnich 15 latach były próby przełamania zabezpieczeń sieci wewnętrznej w celu pozyskania danych (informacji) zlokalizowanych na serwerach JST?
- Czy w JST lub podległych jednostkach organizacyjnych w ostatnich 15 latach były przypadki włamań do sieci w celu kradzieży lub zablokowania danych (informacji) zlokalizowanych na serwerach JST?
- Czy JST poniosła straty finansowe związane z tymi włamaniami?
- Czy w JST i podległych jednostkach organizacyjnych wyznaczona jest osoba lub wyznaczone są osoby do kontaktu z CSIRT-NASK (Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzonym przez Naukową i Akademicką Sieć Komputerową)?
- Czy JST korzysta ze wsparcia CSIRT-NASK w zakresie bezpieczeństwa informacyjnego?

[28] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560 ze zm.).

Celem szczegółowym badań prowadzonych przez autora było ustalenie zakresu monitorowania przez JST prób przełamania zabezpieczeń lub włamań do sieci wewnętrznej (wyniki w tabelach od 1 do 6) oraz sprawdzenie realizacji współpracy z CSIRT-NASK (wyniki w tabelach od 7 do 11).

Tabela 1. Podsumowanie liczby odpowiedzi na pytanie ankiety własnej dotyczące wystąpienia prób przełamania zabezpieczeń sieci wewnętrznej w celu pozyskania danych (informacji) zlokalizowanych na serwerach JST w ciągu ostatnich 15 lat

Jednostka samorządu terytorialnego	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
gmina miejska	32	0	0	3	9,37	29	90,63
gmina wiejska	160	0	0	8	5,00	152	95,00
gmina miejsko-wiejska	38	0	0	2	5,26	36	94,74
powiat ziemski	20	0	0	1	5,00	19	95,00
powiat miejski	3	0	0	0	0	3	100,00
Liczba mieszkańców jednostki	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
do 5000	66	0	0	3	4,55	63	95,45
5001–10 000	95	0	0	3	3,16	92	96,84
10 001–20 000	43	0	0	4	9,30	39	90,70
20 001–50 000	25	0	0	4	16,00	21	84,00
50 001–100 000	13	0	0	0	0	13	100
powyżej 100 000	11	0	0	0	0	11	100

n – liczba obserwacji; *N* – liczba odpowiedzi Źródło: opracowanie własne

Tabela 2. Podsumowanie odpowiedzi na pytanie ankiety własnej dotyczące prób przełamania zabezpieczeń sieci wewnętrznej w celu pozyskania danych (informacji) zlokalizowanych na serwerach JST w ciągu ostatnich 15 lat

Jednostka samorządu terytorialnego	**Rodzaj zagrożeń, jakie wystąpiły**
gmina miejska	skanowanie portów, koń trojański
gmina wiejska	e-mail z niebezpiecznym załącznikiem (3), przelew środków na koncie gminy, włamanie na router główny, phishing, próba logowania z zewnątrz;
gmina miejsko-wiejska	e-mail z niebezpiecznym załącznikiem
powiat ziemski	--
powiat miejski	--

Źródło: opracowanie własne

Tabela 3. Podsumowanie liczby odpowiedzi na pytanie ankiety własnej dotyczące wystąpienia przełamania zabezpieczeń sieci wewnętrznej (włamań do sieci) w celu kradzieży lub zablokowania danych w ciągu ostatnich 15 lat

Jednostka samorządu terytorialnego	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
gmina miejska	32	0	0	3	9,37	29	90,63
gmina wiejska	160	1	0,62	6	3,75	153	95,63
gmina miejsko-wiejska	38	0	0	1	2,63	37	97,37
powiat ziemski	20	1	5,00	1	5,00	18	90,00
powiat miejski	3	0	0	0	0	3	100,00
Liczba mieszkańców jednostki	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
do 5000	66	0	0	2	3,03	64	96,97
5001–10 000	95	0	0	3	3,16	92	96,84
10 001–20 000	43	1	2,33	1	2,33	41	95,34
20 001–50 000	25	1	4	5	20,00	19	76,00
50 001–100 000	13	0	0	0	0	13	100,00
powyżej 100 000	11	0	0	0	0	11	100,00

n – liczba obserwacji; *N* – liczba odpowiedzi Źródło: opracowanie własne

Tabela 4. Podsumowanie odpowiedzi na pytanie ankiety własnej dotyczące wystąpienia przełamania zabezpieczeń sieci wewnętrznej (włamań do sieci) w celu kradzieży lub zablokowania danych w ciągu ostatnich 15 lat

Jednostka samorządu terytorialnego	**Rodzaj zagrożeń jakie wystąpiły** (liczba podobnych)
gmina miejska	wirus, wiadomość e-mail z BitLockerem
gmina wiejska	zaszyfrowanie plików, danych (4), logowanie na router główny, atak DDOS, wiadomość e-mail z niebezpiecznymi plikami
gmina miejsko-wiejska	wirus szyfrujący
powiat ziemski	zaszyfrowanie danych przez ransomware
powiat miejski	--

Źródło: opracowanie własne

Tabela 5. Podsumowanie liczby odpowiedzi na pytanie ankiety własnej dotyczące poniesionych strat finansowych związanych z włamaniami do sieci wewnętrznej w ciągu ostatnich 15 lat

Jednostka samorządu terytorialnego	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
gmina miejska	32	0	0	0	0	1	3,13
gmina wiejska	160	1	0,72	0	0	2	1,15
gmina miejsko-wiejska	38	1	2,63	0	0	0	0
powiat ziemski	20	1	5,00	0	0	0	0
powiat miejski	3	0	0	0	0	0	0
Liczba mieszkańców jednostki	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
do 5000	66	0	0	0	0	1	1,52
5001–10 000	95	1	1,06	0	0	1	1,05
10 001–20 000	43	1	2,33	0	0	0	0
20 001–50 000	25	1	4,00	0	0	0	0
50 001–100 000	13	0	0	0	0	0	0
powyżej 100 000	11	0	0	0	0	1	9,09

n – liczba obserwacji; *N* – liczba odpowiedzi Źródło: opracowanie własne

Tabela 6. Podsumowanie odpowiedzi badanych podmiotów na pytania dotyczące prób lub przełamania zabezpieczeń oraz poniesionych strat z powodu włamań w ciągu ostatnich 15 lat

Jednostka samorządu terytorialnego	**N**	**Brak odpowiedzi**	**Próby włamań**	**Dokonane włamania**	**Poniesione straty**
gmina miejska	32	0	3	3	0
gmina wiejska	160	0	8	6	0
gmina miejsko-wiejska	38	0	2	1	0
powiat ziemski	20	0	1	1	0
powiat miejski	3	0	0	0	0
Liczba mieszkańców jednostki	**N**	**Brak odpowiedzi**	**Próby włamań**	**Dokonane włamania**	**Poniesione straty**
do 5000	66	0	3	2	0
5001–10 000	95	0	3	3	0
10 001–20 000	43	0	4	1	0
20 001–50 000	25	0	4	5	0
50 001–100 000	13	0	0	0	0
powyżej 100 000	11	0	0	0	0

N – liczba odpowiedzi Źródło: opracowanie własne

Podsumowując wyniki badań związanych z monitorowaniem przez JST prób przełamania zabezpieczeń sieci wewnętrznej lub włamań do sieci wewnętrznej (wyniki w tabelach od 1 do 6) stwierdza się, że aż 9,37% badanych gmin miejskich, 5% gmin wiejskich i powiatów ziemskich oraz 5,26% gmin miejsko-wiejskich odnotowało próby przełamania zabezpieczeń sieci wewnętrznych swoich urzędów. Powiaty miejskie nie odnotowały takiego przypadku. Najwięcej zdarzeń miało miejsce w JST, gdzie liczba mieszkańców mieści się w przedziale między 20 001 a 50 000 mieszkańców – 16%. W JST w przedziałach między 50 001 a 100 000 mieszkańców i więcej nie odnotowano żadnej próby przełamania zabezpieczeń. Z kolei incydenty przełamania zabezpieczeń sieci wewnętrznych odnotowano w 9,37% gmin miejskich, 3,75% gmin wiejskich, 5% powiatów ziemskich oraz 2,63% gmin miejsko-wiejskich. Powiaty miejskie nie odnotowały takiego przypadku. Najwięcej zdarzeń (20%) miało miejsce w JST, gdzie liczba mieszkańców jest w przedziale między 20 001 a 50 000 mieszkańców. W JST w przedziałach między 50 001 a 100 000 mieszkańców i więcej nie odnotowano żadnej próby przełamania zabezpieczeń. Żaden z respondentów nie potwierdził poniesienia strat finansowych (było kilka odpowiedzi „brak rejestru"). Wyniki badań jakościowych prowadzonych przez autora (tabela 2 i 4) dotyczących rodzajów zdiagnozowanych zagrożeń (incydentów) mieści się w katalogu incydentów zaprezentowanych w Raporcie rocznym z działalności CERT Polska 2018 pod typami incydentów: obraźliwe i nielegalne treści, spam, dyskredytacja, obrażanie, niesklasyfikowane, złośliwe oprogramowanie, robak sieciowy, koń trojański, oszustwa komputerowe, dialer, próby włamań, próby nieuprawnionego logowania, podatne usługi, phishing, włamania, nieuprawniony dostęp, inne[29].

Porównując statystyki incydentów w Internecie odnotowywanych przez CERT z wynikami ankiety, można wysunąć hipotezę, że jest bardzo mało prawdopodobne, że JST, działając przez 15 lat w cyberprzestrzeni, nie zanotowały żadnych prób przełamania lub włamania do systemu zabezpieczeń sieci informatycznej. Wyniki badań wskazują, że systemy informatyczne JST w sposób niedostateczny są monitorowane i zabezpieczane. Jednocześnie włamanie do systemu JST zawsze będzie generowało straty finansowe (np. wymiana serwera, strony BIP lub

[29] Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2018 r., https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf [dostęp 07.01.2020].

audyt sprawdzający), a brak wykazania w ankiecie strat, oznaczać może, że zostały pokryte w inny, niepowiązany ze zdarzeniem, sposób. Przyczyną takiego działania samorządów może być fakt, że przyznając się do poniesionych strat finansowych, związanych z przełamaniem zabezpieczeń systemów informatycznych, mogłyby narazić się na zarzut niegospodarności majątkiem publicznym i narażeniem na straty majątkowe, które stanowią naruszenie dyscypliny finansów publicznych. Natomiast pracownicy komórek IT w JST mogliby narazić się na zarzut niedopełnienia obowiązków służbowych. Dlatego istnieje duże prawdopodobieństwo, że straty finansowe w JST z powodu przełamania systemów są dużo większe, ale ze względu na konsekwencje prawne są ukrywane.

Tabela 7. Podsumowanie liczby odpowiedzi na pytanie ankiety własnej dotyczące wyznaczenia osoby do kontaktu z CSIRT-NASK w obrębie jednostki

Jednostka samorządu terytorialnego	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
gmina miejska	32	0	0	8	25,00	24	75,00
gmina wiejska	160	1	0,62	34	21,25	125	78,13
gmina miejsko-wiejska	38	0	0	17	44,74	21	55,26
powiat ziemski	20	2	10,00	11	55,00	7	35,00
powiat miejski	3	0	0	0	0	3	100,00
Liczba mieszkańców jednostki	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
do 5000	66	1	1,51	8	12,12	57	86,36
5001–10 000	95	0	0	26	27,37	69	72,63
10 001–20 000	43	0	0	11	25,58	32	74,42
20 001–50 000	25	0	0	15	60,00	10	40,00
50 001–100 000	13	1	7,70	6	46,15	6	46,15
powyżej 100 000	11	1	9,09	4	36,36	6	54,55

n – liczba obserwacji; *N* – liczba odpowiedzi Źródło: opracowanie własne

Tabela 8. Podsumowanie odpowiedzi na pytanie ankiety własnej dotyczące wyznaczenia osoby do kontaktu z CSIRT-NASK w obrębie jednostki

Jednostka samorządu terytorialnego	**Podstawa do wyznaczenia osoby do kontaktu** (liczba podobnych)
gmina miejska	- zarządzenie 11/19 - zarządzenie 173.2019 - wyznaczenie - pracownik urzędu - pismo kierownika jednostki
gmina wiejska	- wyznaczony, wybór osób decyzyjnych, powołanie, zgłoszenie pracownika (6) - zarządzenie Wójta Gminy (5) - wyznaczony przez Wójta Gminy (3) - stanowisko do ochrony danych osobowych - firma zewnętrzna - Inspektor Bezpieczeństwa Informacji - elektroniczna - zatrudniony informatyk
gmina miejsko-wiejska	- zarządzenie burmistrza (5) - wyznaczenie pracownika (2) - zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa - w trakcie opracowywania
powiat ziemski	- zarządzenie starosty (4) - osoba wskazana - AS.212.25.2019
powiat miejski	--

Źródło: opracowanie własne

Tabela 9. Podsumowanie odpowiedzi na pytanie ankiety własnej dotyczące korzystania ze wsparcia CSIRT-NASK w zakresie bezpieczeństwa informacyjnego

Jednostka samorządu terytorialnego	**Rodzaj wykorzystania wsparcia**
gmina miejska	wykorzystanie wiedzy, wykorzystanie procedur, wykorzystanie instrukcji NASK
gmina wiejska	wykorzystanie wiedzy
gmina miejsko-wiejska	--
powiat ziemski	--
powiat miejski	--

Źródło: opracowanie własne

Tabela 10. Podsumowanie liczby odpowiedzi na pytanie ankiety własnej dotyczące korzystania ze wsparcia CSIRT-NASK w zakresie bezpieczeństwa informacyjnego

Jednostka samorządu terytorialnego	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
gmina miejska	32	0	0	4	12,5	28	87,5
gmina wiejska	160	0	0	3	1,88	157	98,12
gmina miejsko-wiejska	38	0	0	0	0	38	100,00
powiat ziemski	20	2	10	0	0	18	90,00
powiat miejski	3	0	0	0	0	3	100,00
Liczba mieszkańców jednostki	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
do 5000	66	0	0	1	1,52	65	98,48
5001–10 000	95	0	0	2	2,11	93	97,89
10 001–20 000	43	0	0	2	4,65	41	95,35
20 001–50 000	25	0	0	1	4,00	24	96,00
50 001–100 000	13	1	7,69	0	0	12	92,31
powyżej 100 000	11	1	9,09	1	9,09	9	81,82

n – liczba obserwacji; *N* – liczba odpowiedzi Źródło: opracowanie własne

Uzyskane odpowiedzi przedstawicieli JST na temat ich współpracy z CSIRT-NASK poddano ocenie wartościującej (tabela 11). Pozytywnie oceniono odpowiedzi świadczące o prawidłowej współpracy. Negatywnie oceniono braki odpowiedzi i odpowiedzi świadczące o braku współpracy. Za nieprecyzyjne uznano odpowiedzi niepełne, świadczące o mankamentach tej współpracy. Najwięcej negatywnych odpowiedzi dotyczących nieprawidłowości w tym zakresie odnotowano w gminach wiejskich (aż 88,4%) i gminach miejskich (81,25%), a także w gminach z małą liczbą mieszkańców (93,2%). Pozytywną ocenę uzyskało najwięcej powiatów ziemskich (18,4%) oraz gmin ze średnią (16%) i dużą liczbą mieszkańców (24%).

Tabela 11. Podsumowanie liczbowe i procentowe odpowiedzi badanych podmiotów na grupę pytań dotyczących współpracy JST z CSIRT-NASK

Jednostka samorządu terytorialnego	***N***	**Negatywna**		**Pozytywna**		**Nieprecyzyjna**	
		n	%	*n*	%	*n*	%
gmina miejska	64	52	81,25	9	14,10	3	4,65
gmina wiejska	320	283	88,40	22	6,90	15	4,70
gmina miejsko-wiejska	76	59	77,63	9	11,84	8	10,53
powiat ziemski	38	27	71,10	7	18,40	4	10,5
powiat miejski	6	6	100	0	0	0	0
Liczba mieszkańców jednostki	***N***	**Negatywna**		**Pozytywna**		**Nieprecyzyjna**	
		n	%	*n*	%	*n*	%
do 5000	132	123	93,2	7	5,3	2	1,5
5001–10 000	190	162	85,3	16	8,4	12	6,3
10 001–20 000	86	73	84,9	8	9,3	5	5,8
20 001–50 000	50	34	68	8	16	8	16
50 001–100 000	25	19	76	6	24	0	0
powyżej 100 000	22	17	77,3	2	9,1	3	13,6

n – liczba obserwacji; *N* – liczba odpowiedzi Źródło: opracowanie własne

Podsumowując wyniki badań własnych, związanych ze współpracą z CSIRT-NASK, warto podkreślić, że 55% powiatów ziemskich, 44,74% gmin miejsko-wiejskich, 25% gmin miejskich oraz 21,25% gmin wyznaczyło osoby do kontaktu z CSIRT-NASK. Żaden powiat miejski nie wyznaczył osoby do kontaktu. Najczęściej osoby do kontaktu wyznaczały gminy, w których liczba mieszkańców mieści się w przedziale 5001–10000 mieszkańców, najrzadziej zaś te, w których mieszka do 5000 obywateli. Współpracę z CSIRT-NASK deklaruje jedynie 12,5% gmin miejskich i 1,88% gmin wiejskich. Gminy miejsko-wiejskie, powiaty miejskie i ziemskie nie korzystały ze wsparcia lub nie udzieliły odpowiedzi. Niepokojący jest fakt braku realizacji obowiązku wyznaczenia osoby do kontaktów oraz zakres współpracy JST z CSIRT-NASK. Szczególnie negatywnie wypadają powiaty miejskie (100% odpowiedzi negatywnych) oraz gminy wiejskie (88,4% odpowiedzi negatywnych).

Podsumowanie

W maju 2019 r. Najwyższa Izba Kontroli (NIK) opublikowała informację o wynikach kontroli: „Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego”[30]. W podsumowaniu NIK negatywnie ocenił wykonywanie przez blisko 70% skontrolowanych urzędów jednostek samorządu terytorialnego zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji w okresie objętym kontrolą. W 61% skontrolowanych urzędów brak było systemowego podejścia do zapewnienia bezpieczeństwa informacji. W 74% badanych urzędów brak było pełnej i aktualnej informacji o posiadanych zasobach informatycznych służących do przetwarzania danych, co w przypadku wystąpienia poważnej awarii lub innego zdarzenia losowego (zalanie, pożar, kradzież), może znacząco utrudnić szybkie odtworzenie infrastruktury i zapewnienie ciągłości świadczenia usług dla obywateli. W wielu skontrolowanych urzędach JST nie dostrzegano występujących zagrożeń. W 48% jednostek nie dokonywano analiz ryzyka, a w 70% nie przeprowadzono obowiązkowego corocznego audytu z zakresu bezpieczeństwa informacji. Brak cyklicznych analiz ryzyka i nieprowadzenie audytów bezpieczeństwa nie pozwalały na identyfikację istotnych ryzyk w zakresie bezpieczeństwa informacji. Kontrola wykazała, że w części urzędów JST zasady mające na celu zwiększenie bezpieczeństwa przetwarzania danych nie były przestrzegane. W ponad 80% skontrolowanych urzędów wystąpiły nieprawidłowości w zarządzaniu uprawnieniami użytkowników w systemach informatycznych. W zakresie uzyskiwania dostępu do systemów informatycznych, w ponad połowie kontrolowanych urzędów (57%) ustanowione zasady nie były przestrzegane (np. użytkownicy używali haseł do systemów informatycznych krótszych niż wymagane). W 56% jednostek wykorzystywano komputery z zainstalowanym systemem operacyjnym bez wsparcia producenta, a w 48% urzędów stwierdzono nieprawidłowości w zakresie tworzenia, przechowywania oraz weryfikacji kopii zapasowych danych. Kontrole NIK również w 2014 r. i 2016 r. ujawniły istotne nieprawidłowości w zakresie bezpieczeństwa systemów informatycznych i zgromadzonych w nich danych o obywatelach. Brak było systemowego podejścia

[30] Informacja o wynikach kontroli „Zarządzanie bezpieczeństwem informacji w Jednostkach Samorządu Terytorialnego”. Nr ewid. 187/2018/P/18/006/KAP, https://www.nik.gov.pl/plik/id,20027, vp,22647.pdf [dostęp 15.02.2020].

kierowników urzędów do zarządzania bezpieczeństwem informacji oraz właściwego zabezpieczenia danych będących w posiadaniu urzędów[31].

Wyniki przeprowadzonych kontroli NIK znajdują potwierdzenie w przeprowadzonych przez autora badaniach w JST na Mazowszu. Mniej niż 10% JST zidentyfikowało i wykazało próby przełamania systemów zabezpieczeń lub włamań do systemów teleinformatycznych urzędu. W 55% badanych powiatów ziemskich zostały wyznaczone osoby do kontaktów z CSIRT-NASK. Wśród gmin wiejskich odsetek ten wyniósł 21,25%. Efektem tego jest brak raportowania do CSIRT-NASK incydentów, co powoduje brak informacji wejściowych i niemożność zidentyfikowania skali zagrożeń przez zespół CERT Polska.

W ostatnich latach można zaobserwować stale rosnącą tendencję do załatwiania przez obywateli spraw w urzędach JST w formie elektronicznej. Zatem zapewnienie bezpieczeństwa przetwarzania informacji w systemach teleinformatycznych urzędów staje się jednym z najistotniejszych wyzwań stojących przed samorządami. Braki w systemach zabezpieczeń sieci wewnętrznej lub nieprzestrzeganie procedur bezpieczeństwa może doprowadzić do kradzieży informacji lub środków finansowych, utraty lub sfałszowania informacji będących w zasobach danej JST. W skrajnych przypadkach może to doprowadzić do paraliżu pracy urzędu i braku możliwości realizacji niektórych obowiązków ustawowych. Warto podkreślić, że każda kategoria JST – gmina, powiat, samorząd województwa – może mieć inną organizację wewnętrzną urzędu, ale realizuje taki sam zakres zadań ustawowych. Dlatego opracowanie jednolitych wytycznych w zakresie organizacji systemu cyberbezpieczeństwa na poziomie każdej z kategorii JST znacznie poprawiłoby spójność bezpieczeństwa systemów i zmobilizowałoby do ich wprowadzenia. Dodatkową wartość stanowiłyby praktyczne ćwiczenia w ramach gminnych i powiatowych zespołów zarządzania kryzysowego z zakresu identyfikacji ryzyk związanych z incydentami w sieciach teleinformatycznych urzędów JST oraz przeciwdziałania skutkom ich wystąpienia. Dużym ułatwieniem dla samorządów byłyby również szkolenia i propagowanie dobrych praktyk, czyli wzorców procedur cyberbezpieczeństwa. Najbardziej kompetentnym podmiotem w tym zakresie jest CSIRT-NASK (CERT Polska) wskazany w ustawie o krajowym systemie do współpracy z JST.

[31] Tamże, s. 7-10.

Bibliografia

Cichocki R., Jatkiewicz P., *Bezpieczeństwo informacji w jednostkach samorządu terytorialnego*, „Roczniki Kolegium Analiz Ekonomicznych SGH" 2013, z. 99.

Liszak-Felicka D., Szmit M., *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016.

Nadybski P., *Elektroniczna administracja w Polsce – ograniczenia i bariery*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy" 2013, nr 9.

Perdał R., *Czynniki rozwoju elektronicznej administracji w samorządzie lokalnym w Polsce*, Poznań 2014.

Sławińska M., *Rok funkcjonowania ustawy o krajowym systemie cyberbezpieczeństwa – najważniejsze postanowienia i rozwiązania*, https://rcb.gov.pl/rok-funkcjonowania-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-najwazniejsze-postanowienia-i-rozwiazania/.

Vademecum bezpieczeństwa, red. O. Wasiuta, R. Klepka, R. Kopeć, Kraków 2018.

Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki – organizacji – państwa*, Warszawa 2016.

Wrzosek M., *Krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, https://cyberpolicy.nask.pl/rb-dokumenty-krajowe-2-krajowe-ramy-polityki-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/.

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. Dyrektywa NIS) (Dz.Urz. UE L 194/1 z 2016 r.).

Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. z 2020 r., poz. 288).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2018 r., poz. 1330).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2020 r., poz. 695).

Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. z 2015 r., poz. 1893).

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r., poz. 344).

Ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz.U. z 2012 r., poz. 1232).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2020 r., poz. 346).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560 ze zm.).

Uchwała Rady Ministrów nr 111/2013 z dnia 25 czerwca 2013 r. w sprawie Polityki Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej.

Uchwała Rady Ministrów nr 52/2017 z dnia 9 maja 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.

Uchwała Rady Ministrów Nr 125/2019 z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 (M.P. z 2019 r., 1037).

Źródła internetowe

www.cert.pl

www.lex.pl

www.cyberpolicy.nask.pl

www.enisa.europa.eu

www.warszawa.stat.gov.pl

www.stat.gov.pl

www.senat.gov.pl

www.nik.gov.pl

Selected aspects of the functioning of National Cybersecurity System in Local Government Units: A case of the Masovian Voivodeship

Summary: The scope of providing services in the field of e-administration by local governments in cyberspace and the transmission and processing of information in ICT systems has increased significantly over the last 15 years. At the same time, local governments have become a potential subject of attacks and hacks into resources collected in digital space. This resulted in the need to identify threats in cyberspace and to use effective countermeasures in the event of security breach attempts. Mazovian voivodeship has been selected as the area of the present research to study cybersecurity in the local government. In recent years, there has been a constantly growing tendency for citizens to handle matters in local government offices in electronic form. Therefore, ensuring the

security of information processing in the ICT systems of offices is becoming one of the most important challenges facing local governments.
Keywords: *cybersecurity, e-administration, National Cybersecurity System, local government, website threats, incident, computerization*

URSZULA ADAMCZYK
ORCID: 0000-0002-4257-4745
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych

Prawo do prywatności i ochrony danych osobowych w Rzeczypospolitej Polskiej

Wprowadzenie

Każdy sposób posługiwania się informacją dotyczącą jednostki może być uznany za wkroczenie w sferę jej prywatności. Prawo do prywatności jest nierozerwalnie związane z godnością człowieka, będącą źródłem wszystkich praw i wolności[1], z czego wywodzi się ich charakter: uniwersalny (przysługują każdemu, niezależnie od miejsca zamieszkania, przynależności etnicznej, płci, religii itp.), przyrodzony (przysługują każdemu od chwili narodzin, nie wiążą się ze statusem społecznym), niezbywalny (jednostka nie może ich zbyć ani ograniczyć), nienaruszalny (brak prawnych możliwości pozbawienia praw jednostki).

Pojęcie prawa do prywatności ujawnia coraz to nowe aspekty w miarę rozwoju stosunków społecznych, politycznych oraz w wyniku rozwoju techniki. Z jednej strony istnieje naturalna chęć ograniczania prawa do prywatności przez władze publiczne, z różnych względów, zwykle motywowanych szeroko rozumianym dobrem obywateli, z drugiej – tendencja do jej chronienia po stronie osób fizycznych. Powszechna panika wywołana zamachami z 11 września 2001 r., i potęgowana ostatnio masowym napływem ludności zamieszkującej Syrię i niektóre obszary Północnej Afryki lub globalną pandemią związaną z COVID-19, stała się

[1] A. Gajda, *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace" / OW SGH 2014, s. 59.

niejako usprawiedliwieniem władz publicznych dla ochrony bezpieczeństwa przed zagrożeniami i do coraz szerszej kontroli sfery prywatnej życia zwykłego obywatela. Takie stanowisko obywatele wielu państw gotowi są zaakceptować.

Prywatność w aspekcie psychologicznym i socjologicznym

Prywatność dopiero w drugiej połowie dwudziestego wieku stała się odrębnym przedmiotem badań nauk psychologicznych i socjologicznych. Wcześniej wiązano ją z innymi pojęciami takimi, jak afiliacja, terytorializm, samotność czy izolacja[2]. Można stwierdzić, że prywatność oznacza uniwersalną potrzebę każdego człowieka, niezależną od wpływu środowiska i kręgu kulturowego. Stanowi cechę osobowości objawiającą się potrzebą izolacji, wyraża potrzebę określonej jednostki, jednak granice prywatności nie są jednakowe dla wszystkich ludzi. Rozumienie prywatności jest zależne od kręgu kulturowego, wieku, osobistych preferencji w zakresie nawiązywania relacji społecznych, pozycji zawodowej czy społecznej. Ta sama osoba może w tym samym czasie, będąc w tym samym wieku, oceniać tę samą sytuację jako naruszającą jej poczucie prywatności lub nie – w zależności od kontekstu sytuacyjnego.

Jak podkreśla R. Dopierała, „rozwój i utrzymanie tożsamości jest zatem najwyżej umieszczoną w hierarchii, centralną funkcją prywatności, a jej dopełnieniem jest zarządzanie interakcjami społecznymi”[3]. Można stwierdzić, że prywatność jednostki to sposób kontrolowania przez nią budowanych relacji społecznych warunkujących prawidłową interakcję z otoczeniem. Istniejące normy społeczne i wynikające z nich wzorce zachowania nie pozostają bez wpływu na zakres oraz rozumienie prywatności. Socjolog M. Ossowska określiła prywatność w trzech perspektywach: jako uprawnienie do okresowej samotności, środek zabezpieczający przed kontrolą lub ingerencją ze strony osób trzecich oraz element godności człowieka[4]. Wskazane podejścia mogą się łączyć i przenikać, powodując, że faktyczne zrozumienie prywatności jest zmienne w czasie i zależne od

[2] K. Jędruszczak, *Prywatność jako potrzeba w ramach koncepcji siebie*, „Roczniki Psychologiczne” 2005, nr 2, s. 112.
[3] R. Dopierała, *Internetowe manifestacje prywatności*, „Media – Kultura – Społeczeństwo” 2008, nr 3, s. 108.
[4] M. Ossowska, *Normy moralne. Próba systematyzacji*, PWN, Warszawa 1985, s. 101-106.

uwarunkowań kulturowych[5]. Zasadnym jest więc oczekiwanie, że prywatność, tak jak wolność, godność i bezpieczeństwo, będzie chroniona nie tylko normami moralnymi, ale także prawnymi.

A. Kopff określił prywatność jako „prawo jednostki do życia swym własnym życiem, układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej"[6]. Prawo do prywatności podzielił na dwie sfery: prawa do intymności życia osobistego oraz prawa do prywatności życia osobistego. Uważa on, że strefa życia intymnego zasługuje zawsze na ochronę prawną i nie ma żadnych okoliczności usprawiedliwiających jakiekolwiek wkroczenie w tę strefę"[7], w tym także związanych z prawem do informacji. Jednak granice strefy prywatności życia osobistego, powiązane ze światem zewnętrznym poprzez interakcje jednostki z otoczeniem i będące efektem tej relacji, mogą budzić „usprawiedliwione zainteresowanie". Teoria sfer Kopffa, w niemal niezmienionej formie, znalazła także miejsce w orzecznictwie Trybunału Konstytucyjnego: „o ile sfera życia intymnego (w znaczeniu szerszym niż potocznie przyjęte) objęta jest pełną prawną ochroną, o tyle ochrona sfery życia prywatnego podlega pewnym ograniczeniom, uzasadnionym usprawiedliwionym zainteresowaniem"[8].

Kopff określił naruszenie prawa do prywatności jako ingerencję w życie prywatne, rodzinne lub domowe, naruszenie integralności psychofizycznej jednostki, naruszenie wolności, przekonań lub obyczajów człowieka, naruszenie czci, honoru lub uzyskanej opinii, ukazanie innej osoby w niekorzystnym dla niej świetle, ujawnienie krępujących lub intymnych faktów odnoszących się do życia prywatnego, przywłaszczenie sobie cudzego nazwiska, pseudonimu lub osiągnięć, niepokojenie drugiej osoby przez jej śledzenie, narzucanie swojego towarzystwa lub w inny sposób, dopuszczenie się naruszenia korespondencji oraz rozpowszechniania cudzego wizerunku bez zezwolenia tej osoby, nadużywanie informacji uzyskanych prywatnie oraz ujawnienie informacji udzielonych w warunkach poufności[9].

[5] J. Kopka, *Prywatność w społecznej komunikacji. Odniesienia teoretyczne i dynamika przemian w społeczeństwie sieci*, [w:] *E-społeczeństwo w Europie Środkowej i Wschodniej. Teraźniejszość i perspektywy rozwoju*, red. S. Partycki, Wyd. KUL, Lublin 2015, s. 26.

[6] A. Kopff, *Koncepcja praw do intymności i do prywatności życia osobistego*, „Studia Cywilistyczne", t. XX, PWN, Warszawa 1972, s. 30.

[7] Tamże, s. 33.

[8] Wyrok TK z 21.10.1998, sygn. K 24/98, OTK 1998, nr 6, poz. 97.

[9] A. Kopff, *Koncepcja praw do intymności…*, dz. cyt., s. 30-33.

Rozwój społeczeństwa informacyjnego

Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych, jako komponentu sfery prywatności, który współcześnie podlega ochronie w większości systemów prawnych. Znacząco wzrosła skala zbierania i wymiany danych, a rozwój technologii umożliwił, na niespotykaną dotąd skalę, wykorzystywanie danych osobowych w działalności. Osoby fizyczne coraz częściej udostępniają informacje o sobie publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zapewniając wysoki stopień ich ochrony[10].

Współczesne korzystanie z sieci otrzymało nową jakość dzięki Internetowi, który służy jako środek komunikacji pozwalający na porozumiewanie się z wieloma osobami w jednym czasie, w skali globalnej. Coraz bardziej rosnąca dostępność, możliwość zastosowania i wykorzystywanie technik informatycznych i telekomunikacyjnych prowadzą do wzrostu złożoności systemów społecznych, gospodarczych i politycznych[11]. Według niektórych badaczy Internet nie jest zwykłą technologią, a rewolucją w sposobie porozumiewania się społeczeństwa i funkcjonowania całego świata. Dynamiczny rozwój Internetu jest najważniejszym czynnikiem i przyczyną pojawienia się społeczeństwa informacyjnego[12]. „Nie jest to już prognoza, lecz stwierdzenie tendencji rozwojowej. Nie spekuluje się, czy to społeczeństwo nadejdzie, lecz rozważa się, w jakim kierunku ewoluuje. To bowiem, że istnieje i określa ramy naszego życia indywidualnego i zbiorowego, stało się faktem. Jest to społeczeństwo najbardziej w historii nasycone techniką i od niej zależne”[13].

[10] Ogólne rozporządzenie o ochronie danych, preambuła, motyw 6. Dziennik Urzędowy Unii Europejskiej.
[11] M. Goliński, *Społeczeństwo informacyjne – geneza koncepcji i problematyka pomiaru*, OW SGH, Warszawa 2011, s. 26.
[12] M. Golka, *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, PWN, Warszawa 2008, s. 83.
[13] K. Krzysztofek, M.S. Szczepański, *Zrozumieć rozwój. Od społeczeństw tradycyjnych do informacyjnych*, Wyd. UŚ, Katowice 2005, s. 169.

Społeczeństwo informacyjne charakteryzuje się ogólną otwartością, szybkością wymiany informacji, podniesieniem kwalifikacji i wiedzy. Informacja zaczęła odgrywać dominującą rolę oraz stanowić podstawowy zasób nowoczesnego społeczeństwa.

Możliwość gromadzenia i przetwarzania dużych zbiorów danych, pozyskanych z wielu rozproszonych baz danych i ich swobodne, globalne przetwarzanie, doprowadziły do powstania rynku brokerów danych (przedsiębiorców, posiadających bazy danych setek milionów osób, zawierających informacje na temat ich stanu zdrowia, indywidualnych preferencji, sytuacji finansowej czy przynależności do określonych mniejszości). Profilowanie, a więc budowanie w oparciu o informacje pozyskiwane z wielu elektronicznych baz danych opisujących jednostkę, stało się skuteczną techniką marketingu , ale także badania i przewidywania zachowań ludzi lub całych społeczności, stając się tym samym skutecznym narzędziem inwigilacji. Europejski Inspektor Ochrony Danych zauważył, że „nigdy wcześniej podstawowe prawa do prywatności i ochrony danych osobowych nie były tak istotne dla ochrony godności człowieka. (…) Dają one człowiekowi możliwość rozwijania własnej osobowości, prowadzenia niezależnego życia, wykazywania się innowacyjnością oraz korzystania z innych praw i wolności. (…) Technologia nie powinna narzucać wartości i praw, jednak relacji tej nie należy również sprowadzać do błędnej dychotomii. Z rewolucją cyfrową wiążą się obietnice korzyści w takich obszarach jak zdrowie, środowisko, międzynarodowy rozwój i efektywność ekonomiczna”[14].

Podkreśla się, że przepisy dotyczące ochrony danych osobowych mają być nie tylko instrumentem niezbędnym dla poszanowania podstawowych, uznanych powszechnie praw i wolności, zwłaszcza prawa do prywatności, ale też pełnić funkcję ochronną interesów użytkowników najnowszej technologii informatycznej i Internetu, w tym różnych instytucji publicznych, oraz zapewnić niezbędne do ich działania zaufanie i bezpieczeństwo[15].

[14] Europejski Inspektor Ochrony Danych, „*W kierunku nowej etyki cyfrowej: dane, godność i technologia*”, https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_summary_pl.pdf [dostęp 9.04.2020].

[15] J. Barta, P. Fajgielski, R. Markiewicz, *Część pierwsza – Wstęp*, [w:] *Ochrona danych osobowych. Komentarz*, Wolters Kluwer, Warszawa 2015.

M. Safjan wskazuje, że charakter prawny przepisów o ochronie danych osobowych jest ukierunkowany na zapobieganie naruszeniom, podczas gdy mechanizmy ochrony prywatności – na działanie „po fakcie" w postaci sankcji cywilnoprawnych i karnych[16]. O ile ochrona danych osobowych związana jest z kontrolowaniem zakresu wykorzystania informacji oraz nadzorowaniem administratorów danych poprzez nadanie specyficznych praw podmiotom danych (np. prawo do informacji, prawo do poprawienia i uzupełniania danych), to prawo do prywatności zorientowane jest na zachowanie poufności informacji. K. Motyka wskazuje, że „ekspansywność pojęcia prawa do prywatności przynajmniej w części jest rezultatem braku jego wyraźniej definicji, która miałaby jakieś szersze uznanie"[17], natomiast prawna definicja ochrony danych osobowych ma charakter bardziej szczegółowy.

Z uwagi na globalny charakter cyberprzestrzeni wiążą się z nią liczne zagrożenia i ryzyka dla ochrony praw podstawowych. Ważnym przykładem jest ochrona prywatności, rozumiana jako prawo do decydowania jednostek o zakresie przekazywanych innym informacji na swój temat, która jest szczególnie podatna na zagrożenia płynące z pozornie anonimowej cyberprzestrzeni. Oczekiwaniem jednostek, grup i instytucji jest decydowanie kiedy, gdzie i jakie informacje ich dotyczące zostaną udostępnione innym. Najpopularniejszymi zagrożeniami w cyberprzestrzeni są ataki z użyciem szkodliwego oprogramowania, kradzieże tożsamości, wyłudzenia mające na celu modyfikacje bądź niszczenie danych, blokowanie dostępu do usług, ataki socjotechniczne, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję[18].

Rozwój nowych sposobów przetwarzania danych związanych z nowoczesnymi technikami również niesie za sobą ryzyko kradzieży danych, ich bezprawnego niszczenia i publikowania, profilowania realizowanego bez poszanowania praw podmiotu danych, niezgodnie z jego interesem, często bez wiedzy danej osoby, cyberinwigilacji, utraty kontroli nad informacją w efekcie przetwarzania

[16] M. Safjan, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, „Państwo i Prawo" 2002, nr 6, s. 7.
[17] K. Motyka, *Prawo do prywatności*, „Zeszyty Naukowe Akademii Podlaskiej w Siedlcach. Seria Administracja i Zarządzanie" 2010, nr 85, s. 25.
[18] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 2, s. 131.

niezgodnego z pierwotnie ustalonym celem lub zakresem, ale również ujawnienia informacji wskutek błędu człowieka, awarii systemu, ale też normalnego działania e-usług[19].

Konstytucjonalizacja prawa do prywatności

Mechanizmy prowadzące do ochrony sfery prywatnej zostały określone już w Konstytucji marcowej z okresu II RP, gwarantującej ochronę nietykalności osobistej, ochronę miru domowego oraz zachowanie tajemnicy korespondencji[20]. Konstytucja kwietniowa z kolei gwarantowała (zgodnie z art. 5 ust. 2), że państwo zapewni obywatelom możność rozwoju ich wartości osobistych oraz wolności sumienia, słowa i zrzeszeń oraz – z art. 68 ust. 2 – „wolność osobistą, mieszkania i tajemnicę korespondencji", jednak granicą tych wolności było dobro powszechne. Norma art. 10 ust. 1, zgodnie z którą żadne działanie nie mogło stanąć w sprzeczności z celami państwa, wyrażonymi w jego prawach, w znaczny sposób ograniczała prawa i wolności osobiste w relacji z władzą publiczną[21]. W Konstytucji PRL utrzymano gwarancje związane z nietykalnością osobistą, jednak kwestię zakresu nienaruszalności mieszkania i tajemnicy korespondencji delegowano do regulacji zwykłej ustawy[22]. Z uwagi na brak poszanowania zasady rządów prawa w okresie PRL, faktyczne znaczenie tych regulacji było niewielkie.

Źródłem norm prawnych ochrony życia prywatnego były akty prawa międzynarodowego, ratyfikowane przez Polskę i przyjęte do bezpośredniego stosowania. Jednym z pierwszych, a zarazem podstawowych, aktów prawnych respektujących te wartości jest Konwencja o ochronie praw człowieka i podstawowych wolności (europejska konwencja praw człowieka) sporządzona w Rzymie dnia 4 listopada 1950 r.[23] Konwencja gwarantowała prawo do poszanowania życia prywatnego i rodzinnego, w tym mieszkania i korespondencji, oraz brak ingerencji

[19] P. Leja, *Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych*, „Prawo Mediów Elektronicznych" 2017, nr 3, s. 10-17.

[20] Ustawa z dn. 17 marca 1921 r. – Konstytucja Rzeczypospolitej Polskiej (Dz.U. z 1921 r. Nr 44, poz. 267, art. 97, 100, 106).

[21] Ustawa Konstytucyjna z dn. 23 kwietnia 1935 r. (Dz.U. z 1935 r. Nr 30, poz. 227).

[22] Konstytucja Polskiej Rzeczypospolitej Ludowej uchwalona przez Sejm Ustawodawczy w dn. 22 lipca 1952 (Dz.U. z 1952 r. Nr 33, poz. 232 ze zm., art. 74).

[23] Konwencja o ochronie praw człowieka i podstawowych wolności (europejska konwencja praw człowieka) (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.).

władzy publicznej w korzystanie z tych praw, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom oraz ochronę zdrowia i moralności lub ochronę praw i wolności innych osób. Gwarancje związane z ochroną prywatności zostały wyrażone również w art. 17 ust. 1 Międzynarodowego Paktu Praw Obywatelskich i Politycznych[24], wprowadzając zakaz samowolnej lub bezprawnej ingerencji w życie prywatne, rodzinne, dom oraz korespondencję, w tym – prowadzące do naruszenia czci i dobrego imienia. Zgodnie z art. 17 ust. 2 Paktu każdy ma prawo do ochrony prawnej przed tego typu ingerencjami i zamachami.

Przemiany polityczne po 1989 r. wzmocniły znaczenie ochrony praw człowieka. W nadal obowiązującej Konstytucji PRL znowelizowano art. 1, w którym wybrzmiało, że „Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej”[25]. Sąd Najwyższy wyrokiem z dnia 8 kwietnia 1994 dokonał potwierdzenia istnienia oraz zakresu prawnej ochrony prywatności przed ingerencją władzy publicznej: „Wolności obywatelskie są (…) elementem wspólnego, demokratycznego i legalistycznego porządku, przeto mogą być również, z uwagi na wspólne dobro i interesy, w rozsądny i odpowiadający prawu sposób, ograniczone, przy uwzględnieniu służącego każdemu obywatelowi prawa do prywatności chroniącego indywidualną sferę jego osobistego życia”[26].

Po uchwaleniu Konstytucji Rzeczypospolitej Polskiej z 1997 r.[27], na mocy art. 47 („Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.”) oraz art. 49 („Zapewnia się wolność i ochronę tajemnicy komunikowania się.”) ochrona prywatności zyskała rangę gwarancji konstytucyjnej. Konstytucja nie wprowadziła zamkniętej definicji terminu prywatność ani zamkniętej listy dóbr chronionych,

[24]Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167).
[25] Ustawa z dnia 29 grudnia 1989 o zmianie Konstytucji Polskiej Rzeczypospolitej Ludowej (Dz.U. z 1989 r. Nr 75, poz. 444).
[26] Wyrok SN z dnia 8 kwietnia1994 r., sygn. III ARN 18/94, OSNP 1994, nr 4, poz. 550.
[27] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 2009 r. Nr 114, poz. 946).

a jedynie wyliczała przykładowe wartości podlegające ochronie i tradycyjnie kojarzone z życiem prywatnym.

Przepis art. 47 został uzupełniony normą art. 51 ust. 1 odnoszącą się do kwestii ochrony danych osobowych: „Nikt nie może być obowiązany, inaczej niż na podstawie ustawy, do ujawniania informacji dotyczących jego osoby". Art. 51 określa również ograniczenia władz publicznych dotyczące pozyskiwania, gromadzenia i udostępniania informacji o obywatelach oraz nadaje prawo dostępu każdemu obywatelowi do dotyczących go urzędowych dokumentów i zbiorów danych oraz żądania sprostowania lub usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. Konstytucyjne gwarancje związane z ochroną prywatności zawarto również w art. 41, zapewniającym nietykalność i wolność osobistą, art. 50, gwarantującym nienaruszalność mieszkania, oraz art. 53, zapewniającym wolność sumienia i wyznania. Ponadto z art. 76 Konstytucji wynika ochrona konsumentów, użytkowników i najemców przed działaniami zagrażającymi ich prywatności.

Konstytucja RP art. 233 ust. 1 w czasie stanu wojennego i wyjątkowego przewiduje zakres ograniczeń wolności i praw człowieka i obywatela z wyłączeniem ograniczenia prawa do poszanowania prywatności (art. 47). Jak zauważa M. Safjan, konsekwencją zaliczenia prywatności do praw, które nie mogą podlegać ograniczeniom nawet w przypadku stanu wojennego lub wyjątkowego, jest uznanie, że ochrona prywatności należy do grona praw i gwarancji o najsilniejszej ochronie konstytucyjnej[28].

Ochrona danych osobowych

Prawo do poszanowania życia prywatnego i ochrona danych osobowych ściśle są ze sobą powiązane, ponieważ chronią to samo dobro – prywatność człowieka.

Zgodnie z konstytucyjną dyspozycją art. 51 ust. 5: „Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa". Pierwszym polskim aktem normatywnym dotyczącym danych osobowych była Ustawa z dnia 29 sierpnia

[28] M. Safjan, *Ochrona prywatności na tle Konstytucji z 1997 roku – ramy normatywne*, [w:] *Wyzwania dla państwa prawa*, Oficyna, Warszawa 2007, s. 86-92.

1997 r. o ochronie danych osobowych[29], nowelizowana przez wzgląd na dostosowanie jej do przepisów unijnych, w tym wdrożenia Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady (UE) z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, wprowadzającej zniesienie przeszkód w przepływie danych osobowych poprzez jednakowy we wszystkich państwach członkowskich stopień ochrony praw i wolności jednostek w zakresie przetwarzania tych danych.

Różnice w stopniu ochrony praw i wolności osób fizycznych poszczególnych państw członkowskich w związku z przetwarzaniem danych osobowych powstałe w wyniku różnic we wdrażaniu i stosowaniu dyrektywy 95/46/WE skutkowały dalszymi pracami nad ujednoliceniem przepisów w tym zakresie na terenie całej Unii, czego efektem było Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[30]. Wszystkie kraje Unii z dniem 25 maja 2018 r. przyjęły rozporządzenie ogólne do bezpośredniego stosowania. Miało ono na celu wzmocnienie podstawowych praw obywateli w epoce cyfrowej oraz ułatwienie przedsiębiorcom i organizacjom działania na wspólnym rynku poprzez spójne i jednolite przepisy na terenie całej Unii. Równocześnie w Polsce weszła w życie nowa ustawa o ochronie danych osobowych[31]. Ustawa stanowi uzupełnienie rozporządzenia w zakresie, w jakim ustawodawca unijny dopuścił doprecyzowanie pewnych zagadnień w porządku prawnym na poziomie państw członkowskich UE.

Definicja danych osobowych w rozporządzeniu ogólnym

Funkcjonowanie w wirtualnym świecie ma wymiar transgraniczny i dotyczy całej międzynarodowej społeczności. Internet daje dostęp do nieograniczonej liczby informacji i wiąże się nie tylko z licznymi korzyściami, ale także z jeszcze

[29] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r., poz. 922).
[30] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, tj. ogólne rozporządzenie o ochronie danych (Dz.Urz. UE L 119 z 04.05.2016).
[31] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000).

większą liczbą zagrożeń. Niemal każdy, bez większej weryfikacji, może umieszczać tam w zasadzie dowolną informację, nie zawsze prawdziwą, co może powodować negatywne skutki dla osoby, których dane dotyczą. Rosnąca liczba przypadków, w których osoby zostały niesłusznie ocenione lub szykanowane, zaowocowała decyzją o zabezpieczeniu praw osób w szerszym zakresie[32].

Dane osobowe to „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”[33].

„Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (…), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby ustalić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas, potrzebne do zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny”[34].

Katalog szczególnych kategorii danych, tzw. „wrażliwych”, zawiera dane biometryczne, wynikające ze specjalnego przetwarzania, dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej, umożliwiające jednoznaczną identyfikację osoby: wizerunek twarzy czy dane daktyloskopijne oraz „dane dotyczące zdrowia” fizycznego i psychicznego osoby, w tym o korzystaniu z usług opieki zdrowotnej ujawniające informacje o stanie jej zdrowia. Art. 9 pkt 1 rozporządzenia ogólnego określa jako szczególne kategorie danych te,

[32] A. Stępień, *Ochrona danych osobowych w świetle rozporządzenia ogólnego – omówienie wybranych zagadnień*, [w:] *Współczesne wyzwania i zagrożenia wobec ochrony informacji niejawnych i danych osobowych*, red. M. Kubiak, S. Topolewski, Wyd. Nauk. UPH, Siedlce 2018, s. 132-133.

[33] Ogólne rozporządzenie o ochronie danych, art. 4 pkt 1.

[34] Ogólne rozporządzenie o ochronie danych, preambuła, motyw 26.

ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne i biometryczne jednoznacznie identyfikujące osobę fizyczną lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

Automatyczne przetwarzanie danych w celu podjęcia decyzji, w tym profilowanie, jest dziś bardzo powszechnym zjawiskiem. Branża reklamowa, marketing, bankowość, ubezpieczenia, ochrona zdrowia – to tylko niektóre sektory korzystające z narzędzi profilowania. Profilowanie, w myśl motywu 71 preambuły, polega na dowolnym zautomatyzowanym przetwarzaniu danych pozwalającym ocenić czynniki osobowe osoby fizycznej, analizować i prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowań, lokalizacji lub przemieszczania się osoby, której dane dotyczą.

Każda osoba, której dane dotyczą, ma prawo, by nie podlegać decyzjom, które opierają się na przetwarzaniu zautomatyzowanym, w tym profilowaniu, wywołującym dla tej osoby określone skutki prawne lub w istotny sposób na nią wpływające. Administrator danych obowiązany jest wdrożyć środki techniczne i organizacyjne, które zapewnią właściwe i bezpieczne przetwarzanie danych z wykorzystaniem profilowania[35]. Zwłaszcza jeśli do profilowania używa się szczególnych kategorii danych osobowych, tzw. danych wrażliwych lub danych osobowych dzieci[36].

Zgodnie z przewidzianym w rozporządzeniu ogólnym podejściem opartym na analizie ryzyka, zwłaszcza kiedy działania na danych odbywają się przy użyciu nowych technologii, obecnie to administrator przed rozpoczęciem przetwarzania zobowiązany jest dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, biorąc pod uwagę charakter, zakres i cele oraz prawdopodobieństwo spowodowania wysokiego ryzyka naruszenia praw i wolności osób fizycznych. Należy szacować je na podstawie obiektywnej oceny, w ramach której stwierdza się, czy operacje przetwarzania danych wiążą się z ryzykiem lub wysokim ryzykiem[37].

[35] Ogólne rozporządzenie o ochronie danych, art. 22.
[36] Gotowi na RODO. Opracowanie GIODO, https://uodo.gov.pl [dostęp 19.11.2018].
[37] Ogólne rozporządzenie o ochronie danych, preambuła, motyw 76.

W przypadku gdy dane zbierane są bezpośrednio od osoby, której dotyczą, administrator, podczas ich pozyskiwania, zobowiązany jest do udzielenia wszelkich przewidzianych prawem informacji oraz do podania w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, zwłaszcza gdy informacja jest kierowana do dziecka[38]:

- danych organizacji, w tym danych kontaktowych i informacji o przedstawicielu, jeśli jest;
- danych kontaktowych inspektora ochrony danych, gdy ma to zastosowanie;
- celu przetwarzania danych i podstawy prawnej;
- odbiorców danych lub kategorii odbiorców, jeśli występują;
- informacji o zamiarze przekazania danych osobowych do państwa trzeciego, gdy ma to zastosowanie;
- informacji o okresie przechowywania danych, a gdy jest to możliwe, kryteriach ustalania tego okresu;
- informacji o prawie osoby do żądania dostępu do danych jej dotyczących, ich sprostowania, usunięcia, ograniczenia przetwarzania, prawie wniesienia sprzeciwu wobec przetwarzania, a także prawie do przenoszenia danych;
- informacji o prawie do cofnięcia zgody w dowolnym momencie i sposobie, w jaki można to zrobić;
- informacji o prawie do wniesienia skargi do organu nadzorczego;
- informacji, czy podanie danych osobowych jest wymogiem ustawowym, umownym czy warunkiem zawarcia umowy, oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą[39].

W przypadku pozyskania danych z innych źródeł (nie od osoby, której dane dotyczą), dodatkowo należy poinformować o źródle pozyskania danych. Informacje te administrator podaje w rozsądnym terminie, najpóźniej w ciągu miesiąca. Jeśli dane mają być stosowane do komunikacji z osobą, której dotyczą,

[38] Ogólne rozporządzenie o ochronie danych, art. 12, pkt. 1.
[39] Ogólne rozporządzenie o ochronie danych, art. 13.

takiej informacji udziela się najpóźniej przy pierwszej takiej komunikacji. Natomiast jeżeli planuje się ujawnić dane innemu odbiorcy – najpóźniej przy pierwszym ujawnieniu.

Bez względu na to, czy dane pozyskuje się od osoby, której one dotyczą, czy z innych źródeł, jeżeli administrator planuje przetwarzać dane osobowe w innym celu niż ten, w którym dane osobowe zostały zebrane, powinien o tym poinformować osobę, której dane dotyczą, oraz udzielić jej pozostałych stosownych informacji.

Przed wyrażeniem zgody osoba ujawniająca swoje dane osobowe powinna otrzymać informację, że ma prawo wycofania zgody w dowolnym momencie, a wycofanie zgody musi być równie łatwe jak jej wyrażenie. Oceniając, czy zgodę wyrażono dobrowolnie, uwzględnić należy między innymi, czy od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, świadczenie usługi, jeśli przetwarzanie danych nie jest niezbędne do wykonania tej umowy. Administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Jeżeli osoba, której dane dotyczą, wyrazi zgodę pisemnym oświadczeniem, które dotyczy więcej niż jednej kwestii, zapytanie o zgodę powinno wyraźnie odróżniać te kwestie w zrozumiałej, łatwo dostępnej formie, jasnym i prostym językiem[40].

W przypadku oferowania usług społeczeństwa informacyjnego bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych dziecka, które ukończyło 16 lat. W innym przypadku zgodę na takie przetwarzanie musi wyrazić (lub zaakceptować ją) osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem. Przetwarzanie jest zgodne z prawem wyłącznie w zakresie wyrażonej zgody[41].

Rozporządzenie ogólne wyposażyło obywateli w możliwość kontroli treści ich dotyczących poprzez prawo do żądania usunięcia danych: tzw. „prawo do bycia zapomnianym", które nakłada na administratora obowiązek niezwłocznego usunięcia tych danych, jeżeli zachodzi jedna z poniższych okoliczności:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

[40] Ogólne rozporządzenie o ochronie danych, art. 7.
[41] Ogólne rozporządzenie o ochronie danych, art. 8.

- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
- dane osoby były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa, któremu podlega administrator[42].

Prawo do bycia zapomnianym nie ma charakteru absolutnego[43]. Ustawodawca wskazuje okoliczności ograniczające korzystanie z niego. Nie ma ono zastosowania, jeżeli prawdopodobnym jest, że uniemożliwi lub poważnie utrudni dochodzenie i obronę roszczeń, a także gdy narusza prawo do wolności wypowiedzi i informacji, utrudnia wykonanie zadań realizowanych w interesie publicznym w ramach sprawowania władzy publicznej powierzonej administratorowi, ze względu na interes publiczny w zakresie zdrowia publicznego, w przypadku badań naukowych oraz realizacji celów archiwalnych, historycznych i statystycznych[44].

Osoba, której dane dotyczą, ma również prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania jej danych, w tym profilowania. Administratorowi nie wolno przetwarzać tych danych, chyba że wykaże prawnie uzasadnione podstawy do przetwarzania nadrzędnych wobec interesów, praw i wolności tej osoby lub podstaw do ustalenia, dochodzenia lub obrony roszczeń[45].

Naruszenie ochrony danych osobowych

Obecnie w polskim prawie stosuje się procedurę powiadamiania o naruszeniu ochrony danych osobowych zarówno organu nadzorczego, jak i osoby,

[42] Ogólne rozporządzenie o ochronie danych, art. 17, pkt 1.
[43] J.J. Feliński, *Bezpieczeństwo danych osobowych w kontekście zmiany przepisów prawa polskiego i Unii Europejskiej dotyczącego gromadzenia, przechowywania, komercyjnego wykorzystywania – nowy zakres administratorów*, [w:] *Aspekty bezpieczeństwa informacyjnego w obszarze cyberprzestrzeni: wymiar teoretyczny i praktyczny*, red. S. Topolewski, K. Karwacka, Wyd. Akademickie AMW, Gdynia 2015, s. 31.
[44] Ogólne rozporządzenie o ochronie danych, art. 17, pkt 3.
[45] Ogólne rozporządzenie o ochronie danych, art. 21, pkt 1.

której dane dotyczą. Naruszenie ochrony danych osobowych to naruszenie bezpieczeństwa prowadzące do przypadkowego, niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia oraz nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych[46]. Brak wiedzy o skali tego zjawiska uniemożliwiał dotąd wypracowanie skutecznych mechanizmów przeciwdziałających powstawaniu takich incydentów, a i osoba, której dane dotyczą, często nie wiedziała, że jej dane stały się przedmiotem naruszenia[47]. Upowszechnienie obowiązku zgłaszania przez administratorów danych naruszeń ma na celu, w głównej mierze, zminimalizowanie możliwych do wystąpienia szkód o charakterze majątkowym, jak i niemajątkowym, osób, których dane dotyczą[48].

Zgłoszenie naruszenia danych osobowych do organu nadzorczego musi nastąpić najpóźniej w ciągu 72 godzin od momentu stwierdzenia tego naruszenia, chyba że administrator jest w stanie, zgodnie z zasadą rozliczalności, uprawdopodobnić, że to naruszenie nie będzie powodować ryzyka naruszenia praw i wolności osób fizycznych. Jeżeli nie jest możliwe dokonanie zgłoszenia w obowiązującym terminie, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn tego opóźnienia, a informacje mogą być przekazywane sukcesywnie, bez zbędnej zwłoki[49].

Zgłoszenie naruszenia ochrony danych do organu nadzorczego musi zawierać co najmniej:

- opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opis możliwych konsekwencji naruszenia ochrony danych osobowych;

[46] Ogólne rozporządzenie o ochronie danych, art. 4, pkt 12.
[47] A. Stępień, P. Biały, *Bezpieczeństwo danych osobowych zgodnie z RODO*, Wiedza i Praktyka, Warszawa 2017, s. 43.
[48] A. Stępień, *Ochrona danych osobowych…*, dz. cyt., s. 129.
[49] Ogólne rozporządzenie o ochronie danych, preambuła, motyw 85.

- opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków[50].

Na administratora został też nałożony obowiązek zawiadomienia o naruszeniu ochrony danych osoby, której dane dotyczą, w przypadku gdy może powodować ono wysokie ryzyko naruszenia jej praw i wolności. Informację, sformułowaną jasnym, prostym językiem, zawierającą opis charakteru naruszenia ochrony danych oraz zalecenia co do minimalizacji potencjalnych niekorzystnych skutków, należy przekazać najszybciej, jak to możliwe[51]. Ustawodawca na mocy art. 34 pkt 3 przewiduje zwolnienie administratora z obowiązku zawiadamiania osoby, której dane dotyczą, w przypadkach gdy:

- wdrożył odpowiednie środki techniczne i organizacyjne i zostały one zastosowane do danych osobowych, których dotyczy naruszenie;
- zastosował środki mające na celu wyeliminowanie prawdopodobieństwa wysokiego ryzyka naruszenia praw i wolności osoby, której dane dotyczą;
- zawiadomienie osoby, której dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku; w takiej sytuacji zostaje wydany publiczny komunikat informujący osoby, których dane dotyczą, o powstałym naruszeniu.

Przetwarzanie danych osobowych

Przetwarzanie dostosowane do wymogów nowoczesnej technologii oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany. Jest to każde zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie[52].

Przetwarzanie danych podlega kilku zasadom. Są to:

[50] Ogólne rozporządzenie o ochronie danych, art. 33 pkt 3.
[51] Ogólne rozporządzenie o ochronie danych, preambuła, motyw 86.
[52] Ogólne rozporządzenie o ochronie danych, art. 4 pkt 2.

- zgodność z prawem, rzetelność i przejrzystość – przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- ograniczenie celu – zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
- minimalizacja danych – dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
- prawidłowość – prawidłowe i w razie potrzeby uaktualniane dane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
- ograniczenie przechowywania – przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane;
- integralność i poufność – przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych[53].

Zasada rozliczalności nakłada na administratora obowiązek ewentualnego udowodnienia, że sposób przetwarzania i wprowadzone zabezpieczenia są wystarczające w stosunku do przetwarzanych przez niego kategorii danych, charakteru i celu przetwarzania bez ryzyka naruszenia praw lub wolności osób fizycznych. Przepisy prawa nie konkretyzują przykładów najlepszych rozwiązań i nie określają minimalnych standardów technicznych zabezpieczenia danych, wprowadzają jednak pojęcie pseudonimizacji, czyli przetwarzania danych w taki sposób, by nie można ich było przypisać konkretnej osobie bez użycia dodatkowych informacji, pod warunkiem że te dodatkowe informacje są przechowywane osobno i odpowiednio zabezpieczone. W praktyce oznacza to wdrożenie niezbędnych zabezpieczeń, adekwatnych dla każdego administratora, zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, w celu skutecznej realizacji zasad ochrony danych[54].

[53] Ogólne rozporządzenie o ochronie danych, art. 5 pkt. 1 lit. a)-f).
[54] *Gotowi na RODO. Opracowanie GIODO*, https://uodo.gov.pl [dostęp 19.11.2018].

Przetwarzanie danych osobowych zgodnie z prawem odbywa się, jeżeli zostanie spełniony jeden z poniższych warunków:

- osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym określonym celu lub w większej liczbie (również określonych) celów;
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub przed zawarciem umowy – do podjęcia działań na żądanie osoby, której dane dotyczą;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem[55].

Wiele organizacji, instytucji, zarówno sektora publicznego, jak i prywatnego, wykorzystuje w swoich codziennych działaniach dane osobowe. Różnego rodzaju informacje, w tym także dane wrażliwe, są gromadzone i przetwarzane w celu sprawnego świadczenia usług. Współczesna rzeczywistość, w której informacja o osobie zyskała wymierną wartość materialną, znacznie utrudnia skuteczną ochronę prywatności i bezpieczeństwo danych osobowych, które mogą być w wielu przypadkach narażone na niewłaściwe wykorzystanie. Dynamika obszaru usług elektronicznych skutkuje coraz szerszym przetwarzaniem informacji, co może wiązać się ze wzrostem zagrożeń związanych z ich wykorzystaniem przez podmioty do tego nieuprawnione. Obecnie nie można lekceważyć nawet

[55] Ogólne rozporządzenie o ochronie danych, art. 6 pkt 1.

minimalnych cyberzagrożeń dla bezpieczeństwa danych osobowych, a co za tym idzie, szeroko rozumianego bezpieczeństwa prywatności jednostki.

Bibliografia

Akty prawne

Konstytucja Polskiej Rzeczypospolitej Ludowej uchwalona przez Sejm Ustawodawczy w dniu 22 lipca 1952 (Dz.U. z 1952 r. Nr 33, poz. 232 ze zm.).

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 (Dz.U. z 2009 r. Nr 114, poz. 946).

Konwencja o ochronie praw człowieka i podstawowych wolności (europejska konwencja praw człowieka) (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.).

Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016).

Ustawa z dnia 17 marca 1921 r. – Konstytucja Rzeczypospolitej Polskiej (Dz.U. z 1921 r. Nr 44, poz. 267).

Ustawa Konstytucyjna z dnia 23 kwietnia 1935 r. (Dz.U. z 1935 r. Nr 30, poz. 227).

Ustawa z dnia 19 grudnia 1989 o zmianie Konstytucji Polskiej Rzeczypospolitej Ludowej (Dz.U. z 1989 r. Nr 75, poz. 444).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r., poz. 922).

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

Wyrok SN z dnia 8 kwietnia 1994 r., sygn. III ARN 18/94, OSNP 1994, nr 4, poz. 550.

Wyrok TK z dnia 21 października 1998 r., sygn. K 24/98, OTK 1998, nr 6, poz. 97.

Opracowania

Barta J., Fajgielski P., Markiewicz R., *Część pierwsza – Wstęp*, [w:] *Ochrona danych osobowych. Komentarz*, Wolters Kluwer, Warszawa 2015.

Dopierała R., *Internetowe manifestacje prywatności*, „Media – Kultura – Społeczeństwo" 2008, nr 3.

Feliński J.J., *Bezpieczeństwo danych osobowych w kontekście zmiany przepisów prawa polskiego i Unii Europejskiej dotyczącego gromadzenia, przechowywania, komercyjnego wykorzystywania – nowy zakres administratorów*, [w:] *Aspekty bezpieczeństwa informacyjnego w obszarze cyberprzestrzeni wymiar teoretyczny i praktyczny*, red. S. Topolewski, K. Karwacka, Wyd. Akademickie AMW, Gdynia, 2015.

Gajda A., *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace" / OW SGH, 2014.

Goliński M., *Społeczeństwo informacyjne – geneza koncepcji i problematyka pomiaru*, OW SGH, Warszawa 2011.

Golka M., *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, PWN, Warszawa 2008.

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 2.

Jędruszczak K., *Prywatność jako potrzeba w ramach koncepcji siebie*, „Roczniki Psychologiczne" 2005, nr 2.

Kopff A., *Koncepcja praw do intymności i do prywatności życia osobistego*, „Studia Cywilistyczne" t. XX, PWN 1972.

Kopka J., *Prywatność w społecznej komunikacji. Odniesienia teoretyczne i dynamika przemian w społeczeństwie sieci*, [w:] *E-społeczeństwo w Europie Środkowej i Wschodniej. Teraźniejszość i perspektywy rozwoju*, red. S. Partycki, Wyd. KUL, Lublin 2015.

Krzysztofek K., Szczepański M.S., *Zrozumieć rozwój. Od społeczeństw tradycyjnych do informacyjnych*, Wyd. UŚ, Katowice 2005.

Leja P., *Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych*, „Prawo Mediów Elektronicznych" 2017, nr 3.

Motyka K., *Prawo do prywatności*, „Zeszyty Naukowe Akademii Podlaskiej w Siedlcach. Seria Administracja i Zarządzanie" 2010, nr 85.

Ossowska M., *Normy moralne. Próba systematyzacji*, PWN, Warszawa 1985.

Safjan M., *Ochrona prywatności na tle Konstytucji z 1997 roku – ramy normatywne*, [w:] *Wyzwania dla państwa prawa*, Oficyna, Warszawa 2007.

Safjan M., *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, „Państwo i Prawo" 2002, nr 6.

Stępień A., Biały P., *Bezpieczeństwo danych osobowych zgodnie z RODO*, Wiedza i Praktyka, Warszawa 2017.

Stępień A., *Ochrona danych osobowych w świetle rozporządzenia ogólnego – omówienie wybranych zagadnień*, [w:] *Współczesne wyzwania i zagrożenia wobec ochrony informacji niejawnych i danych osobowych*, red. M. Kubiak, S. Topolewski, Wyd. Nauk. UPH, Siedlce 2018.

Źródła internetowe

Europejski Inspektor Ochrony Danych, „W kierunku nowej etyki cyfrowej: dane, godność i technologia", https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_summary_pl.pdf [dostęp 9.04.2020].

Gotowi na RODO. Opracowanie GIODO, https://uodo.gov.pl [dostęp 19.11.2018].

The right to privacy and personal data protection in the Republic of Poland

Summary: Allowing people to be innovative and to use other rights and freedoms, the right to privacy protects human dignity and opens up opportunities for independent life and personality development. Fast technical development and globalization have brought new challenges for the protection of personal data as part of privacy protection. Technology has transformed both economy and social life, and should further facilitate the free flow of personal data within the European Union and to third countries and international organizations, while ensuring a high level of personal data protection.
Keywords: *right to privacy, personal data protection*