Włodzimierz Fehler

PODSTAWY BEZPIECZEŃSTWA INFORMACYJNEGO

Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach ▪ 2021

Autor monografii:

dr hab. Włodzimierz Fehler, prof. uczelni
ORCID: 0000-0002-0927-4337

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

Recenzja naukowa:

prof. dr hab. Bernard Wiśniewski – Akademia WSB, Dąbrowa Górnicza

prof. dr hab. Piotr Sienkiewicz – Wojskowa Akademia Techniczna, Warszawa

ISBN 978-83-66541-71-9

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. 14.5. Ark. druk. 16.1.

Projekt okładki, druk i oprawa: Volumina.pl

Spis treści

Wstęp

W wyniku dokonanych przeobrażeń cywilizacyjnych przy ciągle wzrastającym tempie postępu technicznego i technologicznego żyjemy obecnie w epoce uwarunkowań i zmian, którą określa się mianem czwartej rewolucji przemysłowej. Ta pierwsza rozpoczęła się w Anglii w latach 60. XVIII w. wraz z wprowadzeniem maszyny przędzalniczej, która zrewolucjonizowała przemysł tkacki. Później pojawiały się kolejne tego typu wynalazki, w tym zastępująca siłę mięśni ludzi i zwierząt, ale niezbyt efektywna maszyna parowa. Przełomem było jednak wynalezienie przez Jamesa Watta silnika parowego, opatentowanego w 1769 r. To dzięki niemu w praktyce gospodarczej na stałe zagościł proces produkcyjny. Fundamentalną zmianą, do której doszło w wyniku tej rewolucji, było również przeistoczenie społeczeństwa agrarnego w społeczeństwo industrialne. Druga rewolucja przemysłowa, której główną siłą sprawczą stało się wynalezienie i zastosowanie na szeroką skalę elektryczności oraz silnika spalinowego, dokonała się na przełomie XIX i XX w. Jej swoistym znakiem firmowym było rozpoczęcie masowej produkcji przemysłowej opartej na wykorzystaniu linii produkcyjnych, które jako pierwszy do montowania samochodów zastosował Henry Ford. Początków trzeciej rewolucji przemysłowej należy szukać w końcówce lat 60. XX w. To w tym czasie w Japonii narodziła się koncepcja społeczeństwa informacyjnego i zaczęto wprowadzać do użytku komputery. Stworzenie w latach 70. XX w. mikroprocesora oraz skonstruowanie na początku lat 80. tego samego stulecia komputera osobistego doprowadziło do szybkiego rozwoju informatyzacji. Systematyczne zwiększanie możliwości komputerów w połączeniu z wynalezieniem i upowszechnieniem Internetu oraz postępująca automatyzacja i robotyzacja po raz kolejny zmieniły oblicze świata.

Nadspodziewanie szybki proces implementacji rozwiązań opartych na technologiach informatycznych przyczynił się do dalszego rozwoju produkcji, tak na poziomie wytwórczym, jak i projektowo, planistyczno-kontrolnie. Biorąc za symboliczny punkt odniesienia początek XXI wieku, można

stwierdzić, że w nowym tysiącleciu postęp technologiczny oparty w dużej mierze na informatyzacji i cyfryzacji zaczął przyspieszać tak gwałtownie, że, jak już wspomniano, faktem stała się czwarta rewolucja, związana z upowszechnianiem technologii sieciowych, wzajemnie komunikujących się obiektów (tzw. Internet rzeczy) oraz rozwojem sztucznej inteligencji. Oprócz tych cech należy dostrzec również niespotykaną wcześniej skalę zmian, ich zasięg oraz tempo, a także siłę oddziaływania nie tylko na gospodarkę, ale również na sferę polityczną, społeczną czy militarną. W rezultacie mamy do czynienia z sytuacją, w której rzeczywistość zaczynają kształtować dwa wzajemnie przenikające się komponenty: cyfrowy i fizyczny.

Jedną z najbardziej znaczących konsekwencji czwartej rewolucji przemysłowej jest ciągły wzrost znaczenia wykorzystywanej w różnych postaciach informacji. Rodzi to (co nie wszyscy w pełni dostrzegają) ciągłe podnoszenie w hierarchii ważności ludzkich działań pozycji informacyjnego wymiaru bezpieczeństwa. Można w związku z tym postawić tezę, że kwestia bezpieczeństwa informacyjnego to obecnie problem o znaczeniu fundamentalnym, a przy tym także nacechowany złożonością oraz wielowątkowością. Przyjmując pogląd, że bezpieczeństwo informacyjne to proces i ciąg stanów, w ramach których zapewniana jest swoboda wytwarzania, dostępu, gromadzenia i przepływu wysokiej jakości informacji połączona z racjonalnym prawnym i zwyczajowym wyodrębnieniem pewnych ich kategorii, podlegających ochronie bądź reglamentacji ze względu na bezpieczeństwo podmiotów, których one dotyczą, trzeba pamiętać, że procesom tym i stanom towarzyszą różnorodne wydarzenia i zjawiska tworzące cały szereg szans, wyzwań i zagrożeń. Ich identyfikacja, charakterystyka, a tym bardziej definiowanie nie jest zadaniem łatwym. Wynika to m.in. z istoty informacji, która, jak wskazują zajmujący się jej badaniem naukowcy, jest fenomenem niedającym zamknąć się w sztywne ramy definicyjne. Scharakteryzowane powyżej uwarunkowania w pełni uzasadniają prowadzenie pogłębionej badawczej penetracji sfery bezpieczeństwa informacyjnego. Konieczność realizacji tego rodzaju badań wynika przede wszystkim z potrzeby zaspokajania na odpowiednim poziomie jakościowym i ilościowym potrzeb informacyjnych różnych podmiotów. To z kolei wiąże się ze znajomością uwarunkowań bezpieczeństwa informacyjnego oraz adekwatnym postrzeganiem istoty tego bezpieczeństwa. Zważywszy na ciągle zmieniający się charakter wspomnianych uwarunkowań (w dużej mierze następujący pod wpływem postępu technicznego w zakresie wytwarzania, przekazywania, analizowania i gromadzenia

informacji), nie jest to zadanie łatwe. Kwestia powiązania informacji z informatycznymi narzędziami i komputerowymi systemami ich wytwarzania i przetwarzania oraz ich wpływem na budowanie wiedzy, funkcjonowanie gospodarki i społeczeństwa jest przedmiotem ożywionego dyskursu. Bardzo mocno w jego ramach eksponowane są poglądy mówiące o tym, że dzięki technologiom informatycznym przekazywanie informacji w postaci sygnałów, wiadomości, tekstów czy obrazów multimedialnych, jej cyfryzacja, przetwarzanie, gromadzenie, szybkie udostępnianie tworzy coraz lepsze warunki do rozwoju wiedzy, zwiększa poznawcze możliwości społeczeństw, a w efekcie systematycznie przyspiesza tempo rozwoju cywilizacyjnego. Można w tym kontekście zauważyć, że na bazie skokowego postępu technologiczno-informatycznego wytwarza się specyficzny obraz wszechpotęgi informacji, który zaczyna opanowywać zbiorową wyobraźnię. Do takiego wysoce entuzjastycznego spojrzenia można mieć jednak sporo zastrzeżeń. Podkreślić należy bowiem, że część związanych z postępem technologicznym nowych możliwości bywa z chwilą ich pojawienia się natychmiast wykorzystywana do działań bezprawnych czy nieetycznych. To powoduje intensywne poszukiwanie i wdrażanie środków mających takim sytuacjom zapobiegać, jednak środki te w wielu przypadkach generują nowe zagrożenia, np. w postaci nadmiernej ingerencji w prawa i wolności informacyjne jednostek. Pamiętać także trzeba o istnieniu barier informacyjnych, które w różnym zakresie utrudniają, zniekształcają czy nawet uniemożliwiają rozpoznawanie istoty i znaczenia danej informacji, a tym samym ograniczają możliwości radzenia sobie z negatywnymi skutkami takich sytuacji dla efektywnego poznania i budowania rzetelnej wiedzy. Także zagrożenia informacyjne, np. w postaci nadmiaru informacji, operowania informacją niskiej jakości, stosowania dezinformacji czy prowadzenia walki informacyjnej, w różnych konfiguracjach przeszkadzają w dokonywaniu poprawnych wyborów, podejmowaniu racjonalnych decyzji, właściwym rozwiązywaniu problemów, osłabiają także przekaz i odbiór wiarygodnych i niezbędnych do bezpiecznej egzystencji informacji.

Tego rodzaju sytuacje, oprócz konieczności prowadzenia działań praktycznych w sferze politycznej, organizacyjnej, prawnej czy technicznej, obligują również do podejmowania systematycznego wysiłku badawczego. Powinien być on ukierunkowany na rozpoznawanie, objaśnianie i prognozowanie sytuacji w sferze bezpieczeństwa informacyjnego w taki sposób, aby – uwzględniając interesy jednostek i społeczeństw – skuteczniej wykorzy-

stywać szanse, maksymalnie ograniczać występowanie zagrożeń i łagodzić ich skutki oraz sprawnie i efektywnie podejmować wyzwania. Należy przyznać, że takie wysiłki są podejmowane w sposób zauważalny i obejmują rozległy wachlarz zagadnień. Bowiem oprócz wspomnianych czynów przestępczych związanych z informacją wśród obszarów, które obecnie leżą w centrum zainteresowania zarówno badaczy, jak i praktyków, znajdują się także kwestie funkcjonowania społeczeństwa informacyjnego, rozwoju sztucznej inteligencji, kształtu zagrożeń oraz barier informacyjnych. Niemniej jednak negatywne zjawiska towarzyszące rozwojowi infosfery są cały czas znaczącym wyzwaniem, z którym muszą się mierzyć zarówno badacze, jak i teoretycy oraz wszyscy wytwórcy, posiadacze i użytkownicy informacji.

Zważywszy na przedstawione przesłanki naukowe oraz utylitarne, za uzasadnione uznano przyjęcie jako przedmiotu badań teoretycznych podstaw kształtowania informacyjnego wymiaru bezpieczeństwa. Za cel badań przyjęto weryfikację dotychczasowych ustaleń w zakresie fundamentalnych pojęć odnoszących się do istoty bezpieczeństwa informacyjnego oraz zaproponowanie adekwatnego, przystającego do współczesnych realiów ich zbioru. Wielość pojęć związanych z bezpieczeństwem informacyjnym i duża liczba ich nieprecyzyjnych czy błędnych definicji zamazuje wyrazistość i zniekształca sens używanych terminów, co powoduje nie tylko chaos myślowy, ale może prowadzić do kreowania nieprecyzyjnych (a nawet błędnych) rozwiązań. Jeżeli bowiem do opisywania i wyjaśniania rzeczywistości korzysta się z niejasnych i nieadekwatnych pojęć, to opisy te i wyjaśnienia również będą niejasne i nieprecyzyjne. Dlatego też podstawy porządku definicyjno-terminologicznego są niezbędne.

Biorąc pod uwagę powyżej przedstawione założenia, sformułowano główny problem badawczy, który sprowadza się do poszukiwania odpowiedzi na pytanie, jak współcześnie powinniśmy rozumieć istotę bezpieczeństwa informacyjnego i jakie zasadnicze składniki wpływają na jego kształtowanie. Istnieje szereg powodów takiego ujęcia problemu badawczego. Po pierwsze, kluczowe znaczenie ma to, że bezpieczeństwo informacyjne współcześnie wykracza dalece poza ochronę informacji. Zmieniły się i ciągle ewoluują również zagrożenia w sferze informacyjnej. Zatem nie można postrzegać bezpieczeństwa informacyjnego w wąskich kontekstach, np. ochrony informacji czy cyberbezpieczeństwa.

Po drugie, sposób pojmowania informacji, jej klasyfikowanie oraz przyjmowane w różnych dziedzinach ludzkiej działalności poglądy na

traktowanie informacji jako zasobu nadają kierunki dalszym aktywnościom w dziedzinie bezpieczeństwa informacyjnego. Także postrzeganie i definiowanie istoty społeczeństwa informacyjnego, określanie zasadniczego katalogu zagrożeń informacyjnych wraz z ich rozumieniem, trendy w zakresie definiowania istoty polityki bezpieczeństwa informacyjnego oraz bezpieczeństwa informacji wywierają wpływ na kształtowanie poziomu bezpieczeństwa informacyjnego. Tym samym czynią aktualizację i systematyzację podstawowych pojęć zagadnieniem o znaczeniu fundamentalnym.

Dążąc do rozwiązania głównego problemu badawczego, sformułowano również problemy szczegółowe dotyczące tego:

- jak współcześnie jest pojmowana, klasyfikowana i traktowana informacja oraz jakie pełni ona funkcje?
- jaki jest współczesny obraz społeczeństwa informacyjnego i jakie skutki rodzi jego funkcjonowanie?
- jak należy postrzegać i adekwatnie do posiadanych cech definiować główne rodzaje zagrożeń i barier informacyjnych?
- jak powinno być postrzegane i rozumiane bezpieczeństwo informacyjne, bezpieczeństwo informacji oraz polityki ich dotyczące?

Za podstawę służącą do rozwiązania wymienionych problemów badawczych przyjęto weryfikację zasadniczej hipotezy badawczej mówiącej, że bezpieczeństwo informacyjne stanowi integralną część bezpieczeństwa państw, grup społecznych oraz jednostek i musi być ono adekwatnie definiowane w celu odpowiedniego programowania i podejmowania skutecznych działań na rzecz jego zapewnienia. Kierując się regułami metodologicznymi oraz dążąc do weryfikacji hipotezy głównej, sformułowano również hipotezy szczegółowe mówiące o tym, że:

- sposób pojmowania i kategoryzacja informacji oraz postrzegania jej roli i funkcji w dużej mierze jest uzależniony od dziedziny aktywności ludzkiej, w której się je wykorzystuje;
- powstanie i rozwój społeczeństwa informacyjnego wywarły istotny wpływ na ewolucję postrzegania bezpieczeństwa informacyjnego oraz jego uwarunkowania;
- istniejący szeroki zakres zagrożeń, barier informacyjnych oraz ich zmienna natura rodzi potrzebę nowych systematyzacji, doprecyzowania już istniejących oraz wprowadzania nowych pojęć związanych z tym obszarem;

– aktualnie stosowany aparat pojęciowy odnoszący się do sfery pojmowania bezpieczeństwa informacyjnego i bezpieczeństwa informacji ze względu na ograniczoną adekwatność nie pozwala w pełni skutecznie działać na rzecz zapewnienia tego bezpieczeństwa i wymaga redefinicji.

Zważywszy na fakt, że bezpieczeństwo, niezależnie od analizowanego wymiaru i sposobu jego postrzegania, posiada cechy i właściwości systemu, jako przydatny paradygmat, w oparciu o który postanowiono dokonać analiz i charakterystyk w zakresie badanej tematyki, wybrano paradygmat systemowy. Takie rozstrzygnięcie podyktowała nie tylko złożoność i dynamika bezpieczeństwa informacyjnego, ale także przekonanie, że uchwycenie zjawisk i procesów związanych z tym wymiarem bezpieczeństwa oraz ich zmian wymaga ujęcia dynamicznego, które zapewni spojrzenie systemowe i takąż analizę.

Myślenie i ujęcie systemowe uznano także za właściwy instrument służący do wyjaśniania oraz interpretacji problemów dotyczących zagrożeń i barier informacyjnych. Wspomniany paradygmat zastosowano jako przydatny poznawczo także w odniesieniu do kwestii definiowania bezpieczeństwa informacyjnego i bezpieczeństwa informacji. Tę samą użyteczność dostrzeżono w odniesieniu do polityki bezpieczeństwa informacji oraz polityki bezpieczeństwa informacyjnego jako punktów wyjścia do przedsięwzięć mających na celu zapewnienie pożądanego poziomu bezpieczeństwa informacyjnego.

Zakres i kształt problemów badawczych, postawionych hipotez, teoretyczny charakter monografii oraz przyjęty paradygmat naukowy zadecydowały o wyborze i zastosowaniu metod badawczych, takich jak analiza, synteza, analogia i wnioskowanie.

Metodę analizy jako metodę jakościową zastosowano głównie w zakresie badania istniejącego dorobku naukowego dotyczącego poszczególnych pojęć, klasyfikacji oraz charakterystyk. Ważnym elementem badań była również analiza aktów prawnych i dokumentów zawierających odniesienia do badanych problemów. Metoda ta została wykorzystana przy opracowaniu pierwszego rozdziału, jak również w pozostałych trzech rozdziałach. Jak zaznaczono, użyte zostały również metody syntezy i wnioskowania. Pozwoliły one ująć uzyskane w trakcie badań wyniki w całość i dokonać ich interpretacji, dającej podstawy do sformułowania odpowiedzi na postawione problemy badawcze oraz weryfikacji hipotez. Metody te umożliwiły również określenie prawidłowości oraz odnalezienie najbardziej prawdopodobnych rozwiązań

problemów, a także dokonanie uogólnień. Wspomniane powyżej metody najszersze zastosowanie znalazły w przygotowaniu konkluzji zamykających poszczególne części monografii oraz w jej zakończeniu.

Struktura monografii składa się z wstępu, czterech rozdziałów merytorycznych oraz zakończenia. W rozdziale pierwszym podjęte zostały rozważania poświęcone sposobom pojmowania informacji i jej znaczeniu. W otwierającym ten rozdział podrozdziale, na tle charakterystyki przedmiotu zainteresowań nauki o informacji, dokonano przeglądu sposobów definiowania informacji oraz przedstawiono poglądy dotyczące rozumienia i charakterystyki pojęć pokrewnych, takich jak dane, wiadomość, komunikat, wiedza. W końcowym fragmencie tej części scharakteryzowano również główne teorie informacji. Następnie podjęto zagadnienie klasyfikacji informacji oraz poddano analizie poglądy badaczy na kwestię jej cech oraz funkcji. Rozdział pierwszy kończą rozważania na temat postrzegania i traktowania informacji jako zasobu ważnego, a nawet strategicznego z punktu widzenia funkcjonowania różnych podmiotów.

Drugi rozdział monografii zawiera analizy poświęcone społeczeństwu informacyjnemu. Po przedstawieniu genezy i etapów rozwoju tego społeczeństwa dokonano charakterystyki różnych sposobów definiowania jego istoty. W kolejnych częściach rozdziału badawczemu oglądowi poddane zostały zagadnienia cech i funkcji społeczeństwa informacyjnego oraz dokonano analiz dotyczących zagrożeń i wyzwań towarzyszących funkcjonowaniu tego społeczeństwa. Ostatni fragment tej części rozważań poświęcony został przedstawieniu nowego etapu rozwoju infosfery związanego z postępującym wzrostem znaczenia sztucznej inteligencji.

Trzeci rozdział dotyczy zagrożeń i barier informacyjnych. W obrębie tego fragmentu monografii, po przeprowadzeniu ogólnej charakterystyki i klasyfikacji zagrożeń dla bezpieczeństwa informacyjnego, przedstawiono argumenty na rzecz koniecznego wyodrębnienia przestępstw informacyjnych jako specyficznych rodzajów zagrożenia informacyjnego. W dalszej kolejności dokonano charakterystyki jednego z najgroźniejszych dla bezpieczeństwa informacyjnego zagrożeń, jakim jest dezinformacja. W końcowej części rozdziału przedstawiono adekwatne dla obecnego stanu rozwoju zagrożeń informacyjnych ujęcia walki i wojny informacyjnej oraz analizy, ukazujące różne oblicza, a także klasyfikacje barier informacyjnych.

W ramach czwartego rozdziału zostały zawarte rozważania dotyczące pojmowania istoty bezpieczeństwa informacyjnego oraz bezpieczeństwa

informacji. W początkowym fragmencie tej części monografii dokonano krytycznej analizy funkcjonujących w literaturze przedmiotu ujęć bezpieczeństwa informacyjnego, a następnie na ich bazie zaproponowano definicję oddającą współczesny obraz tego bezpieczeństwa. W kolejnej części podkreślono wyraźną potrzebę wyodrębniania pojęcia bezpieczeństwa informacji jako kategorii znaczącej dla właściwego traktowania i postrzegania bezpieczeństwa informacyjnego. W uzupełnieniu autorskiej definicji bezpieczeństwa informacji scharakteryzowano również podstawowe właściwości decydujące o tym, kiedy informacja może być uznana za bezpieczną. W końcowej części rozdziału czwartego, po przeprowadzeniu przeglądu istniejących poglądów na pojmowanie polityki bezpieczeństwa informacyjnego oraz polityki bezpieczeństwa informacji, przedstawiono propozycje w zakresie definiowania tych pojęć. W ramach tej części rozważań sformułowano również zestaw reguł służących do konceptualizacji i realizacji wspomnianych polityk.

Należy podnieść fakt, że poszczególne rozdziały pracy nie wyczerpują tak złożonego zagadnienia, jakim jest kwestia podstaw teoretycznego opisu i objaśniania współczesnego obrazu oraz perspektywicznego kształtu bezpieczeństwa informacyjnego. Przedstawiony w monografii sposób ujęcia problematyki ma z założenia charakter autorski i ograniczony został do zagadnień uznanych za najważniejsze. Jednocześnie zawartość merytoryczna monografii oraz towarzyszące jej przesłania naukowe pozostają otwarte na refleksje, uzupełnienia, poprawki oraz dyskusje nad przedstawionymi w ich ramach ustaleniami i propozycjami.

W zakresie źródeł naukowych wykorzystanych w trakcie przygotowywania monografii przede wszystkim należy stwierdzić, że w odniesieniu do szeregu podejmowanych zagadnień, w szczególności zaś tych dotyczących teorii informacji, istnieje dość obszerne piśmiennictwo. Jako szczególnie ważne dla powstania prezentowanej książki w części dotyczącej istoty i klasyfikacji oraz cech i funkcji informacji należy wymienić przede wszystkim monografie i artykuły naukowe autorstwa Bogdana Stefanowicza, Marka Hetmańskiego, Luciana Floridiego, Claude'a A. Shanonna, Wiesława Babika, Mirosława Górnego oraz Hanny Batorowskiej. Stosunkowo dobrze scharakteryzowana jest kwestia społeczeństwa informacyjnego. W tym obszarze za wielce przydatne dla powstania monografii należy uznać prace Manuella Castellsa, Marii Nowiny-Konopki, Lecha W. Zachera, Tomasza Gobana-Klasa czy Kazimierza Krzysztofka. Wiele istotnych ustaleń i inspiracji w odniesieniu do kwestii zagrożeń i barier informacyjnych dostarczyły publikacje

Tomasza R. Aleksandrowicza, Krzysztofa Liedla, Andrzeja Żebrowskiego, Marka Wrzoska oraz Marzeny Świgoń i Thomasa T. Wilsona. W przypadku zagadnień walki i wojny informacyjnej należy podkreślić znaczenie prac autorstwa Olgi Wasiuty, Sergiusza Wasiuty, Jacka Reginy-Zacharskiego, Piotra Sienkiewicza, Marka Madeja, Leopolda Ciborowskiego, Michała Wojnowskiego oraz Dorothy E. Denning. Zauważalny jest także wkład w badanie tych szczególnych zagrożeń informacyjnych wspomnianych już wcześniej Andrzeja
Żebrowskiego oraz Marka Wrzoska. Istnieje natomiast deficyt opracowań dotyczących teoretycznego ujmowania istoty bezpieczeństwa informacyjnego. Tylko częściowo poziom tego deficytu obniżają prace takich badaczy, jak Krzysztof Liderman, Józef Janczak, Andrzej Nowak, Eugeniusz Nowak, Maciej Nowak, którzy podejmują próby opisu i charakterystyki tego, czym jest bezpieczeństwo informacyjne. Nie ma natomiast w literaturze przedmiotu, poza powielanymi wielokrotnie odwołaniami do norm ISO i rozwiązań instrukcyjnych, liczących się publikacji dotyczących polityki bezpieczeństwa informacyjnego oraz polityki bezpieczeństwa informacji. Oprócz wykorzystania prac monograficznych wymienionych powyżej badaczy sięgano również w wymiarze przyczynkowym po szereg innych artykułów naukowych zawierających uwagi i odniesienia dotyczące podejmowanych problemów. Z bogatej ich listy jako szczególnie przydatne do prowadzonych analiz wymienić należy prace Ewy Wędrowskiej dotyczące ilościowych i jakościowych koncepcji informacji, Mariusza Grabowskiego i Agnieszki Zając charakteryzujące relacje pomiędzy danymi, informacjami a wiedzą, Marcina Orzechowskiego o koncepcjach walki informacyjnej, Adama Lelonka poświęcone wojnie informacyjnej oraz Doroty Fleszer analizujące ogólne uwarunkowania bezpieczeństwa informacji.

Należy także dodać, że oprócz książek i artykułów naukowych korzystano również z dokumentów źródłowych w postaci strategii, programów rozwojowych oraz aktów prawnych, przyjmowanych w odniesieniu do infosfery. Oprócz krajowej wykorzystywano również w niezbędnym zakresie zagraniczną literaturę przedmiotu.

Ze względu na charakter monografii, która stanowi zbiór rozważań o charakterze teoretycznym, należy na koniec poczynić trzy uwagi. Po pierwsze, autor, od kilkunastu lat zajmujący się teoretycznymi zagadnieniami bezpieczeństwa informacyjnego, w części fragmentów monografii wykorzystywał i odwoływał się również do własnego dorobku, w tym zwłaszcza do

definicji, klasyfikacji oraz innych ustaleń, które wytrzymały próbę czasu i zostały pozytywnie zweryfikowane przez innych badaczy posługujących się nimi w swoich pracach. Po drugie, autor odniósł się do kluczowych pojęć z zakresu bezpieczeństwa informacyjnego poprzez zaproponowanie własnych definicji, nie roszcząc sobie jednak pretensji do ostateczności zawartych w nich rozstrzygnięć, mając świadomość, że szybko zmieniająca się rzeczywistość ciągle przynosi nowe ustalenia. Po trzecie, mająca wieloaspektowy charakter (systematycznie zresztą wzbogacany o nowe wątki) problematyka bezpieczeństwa informacyjnego to niewątpliwie fascynujący obszar badań i analiz dla naukowców, lecz także obszar wysoce zajmujący dla praktyków. Stąd też dążeniem autora monografii było przekazanie zawartych w niej treści w taki sposób, żeby obie kategorie odbiorców mogły uaktualnić oraz poszerzyć swoją wiedzę w odniesieniu do tej sfery bezpieczeństwa.

Włodzimierz Fehler

1. Informacja i jej znaczenie

1.1. Pojęcie informacji

Wśród najważniejszych elementów charakteryzujących oblicze i trendy współczesnego świata mieści się nieustany wzrost (od dawna zresztą i tak już wysokiego) znaczenia informacji, której zastosowanie w różnych aspektach ludzkiej aktywności stanowi obecnie jeden z dominujących czynników rozwojowych. Termin „informacja", którego rodowód sięga przełomu XIX[1] i XX wieku, kiedy to zaczęto go stosować na użytek termodynamiki, należy współcześnie do grupy fundamentalnych pojęć używanych w różnych dziedzinach i dyscyplinach naukowych oraz w języku potocznym. Ponadto szeroko wykorzystywany jest on w różnorodnych kontekstach związanych z funkcjonowaniem systemów społecznych, ekonomicznych czy technicznych i sterowaniem nimi. W ramach każdego z tych rodzajów aktywności podejmowane są uwzględniające sektorowe potrzeby próby uchwycenia istoty informacji. Efektem jest coraz większa liczba definicji oraz opisów, których twórcy starają się określić, czym jest informacja. Istotny wpływ na taki stan rzeczy wywiera także rozwój technologii informacyjnych, w wyniku którego pojęcie informacji jest systematycznie wzbogacane o nowe aspekty. Tego rodzaju sytuacja z jednej strony oddala nas od przyjęcia w miarę jednolitego poglądu na sposób postrzegania informacji, z drugiej strony jednak ukazuje jej bogactwo treściowe i zmienną naturę. Jednym z efektów tak szerokiego spojrzenia na informację i rosnącego jej znaczenia stało się powstanie nauki o informacji. Jak zauważyła Wanda K. Roman, jej złożoność jest rezultatem procesów doświadczanych

[1] Jak podaje Mieczysław Lubański w przypadku języka polskiego, wyraz ten odnaleźć można u S.B. Lindego *Słownik języka polskiego*, t. II, Lwów 1855, gdzie jest on zapisywany jako „informacya" i oznacza: uwiadomienie, nauczanie, naukę. Zob. M. Lubański, *Filozoficzne zagadnienia teorii informacji*, Warszawa 1974, s. 7.

przez ludzkość, która stopniowo wkraczała w epokę informacji aż do momentu kulminacji, która miała miejsce w drugiej połowie XX w.[2] Mirosław Górny, pisząc o przyczynach powstania nauki o informacji, wskazuje, że spowodował to m.in. ogromny przyrost zasobów informacji, do obsługi których konieczne stało się kształcenie specjalistów[3]. Ewa Wędrowska zauważa w tym kontekście, że najpierw miała ona służyć potrzebom łączności i cybernetyki, ale wyszła poza te ramy[4]. Hanna Batorowska podkreśla, że początkowo była to nauka praktyczna, która następnie poszerzyła pole swoich zainteresowań o badania podstawowe zmierzające do podbudowy teoretycznej dla działalności naukowo-informacyjnej. W efekcie na przestrzeni ostatniego półwiecza nauka o informacji konkretyzowała swoją nazwę, poczynając od dokumentacji naukowej poprzez informację naukową, informację naukowo-techniczną i ekonomiczną, na informatologii kończąc. Obecnie postrzega się ją jako naukę interdyscyplinarną, wprawdzie mocno powiązaną z technologią informacyjną, ale mającą także wymiar społeczny i ludzki wykraczający poza tę technologię[5]. W słownikowym ujęciu nauka o informacji zajmuje się „systematycznym badaniem i analizą źródeł, opracowywaniem, gromadzeniem, organizacją rozpowszechniania, oceną wykorzystywania i zarządzania informacją we wszystkich jej formach, kanałów jej przepływu (formalnych i nieformalnych) oraz technologii wykorzystywanych w komunikacji”[6]. W syntetycznej formule opisuje naukę o informacji przywoływany już M. Górny, który ujmuje ją jako zajmującą się „badaniem wszystkich procesów, z którymi ludzie mają do czynienia, korzystając z informacji w działalności naukowej, gospodarczej i publicznej”[7]. Jednocześnie wspomniany autor zauważa bardzo celnie, że gromadzi ona wiedzę praktyków i badaczy uprawiających naukę o informacji, ale sięga również po dorobek innych dyscyplin, takich jak językoznawstwo, psychologia, socjologia, prawo, informatyka, organizacja i zarządzanie, matematyka[8].

[2] Zob. W.K. Roman, *Między archiwistyką a architekturą informacji*, „Archiwa – Kancelarie – Zbiory” 2018, nr 9, s. 227.
[3] Zob. M. Górny, *Nauka o informacji jako dyscyplina naukowa*, [w:] *Nauka o informacji*, W. Babik (red.), Warszawa 2016, s. 23.
[4] Zob. E. Wędrowska, *Ilościowe i jakościowe koncepcje informacji*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług” 2010, nr 57, s. 49.
[5] Zob. H. Batorowska, *Nauka o informacji (informatologia) z perspektywy nowych wyzwań edukacyjnych,* „Edukacja – Technika – Informatyka” 2015, nr 3, s.73.
[6] *Dictionary for Library and Information Science,* https://products.abc-clio.com/ODLIS/ odlis_w.aspx [dostęp: 12.04.2021 r.].
[7] M. Górny, dz. cyt., s. 33.
[8] Zob. tamże, s. 39.

W konsekwencji cytowany badacz jako główne obszary badawcze nauki o informacji wymienia:

„– odkrywanie cech i właściwości obiektów i procesów informacyjnych;
– badanie funkcji obiektów i procesów informacyjnych;
– wyjaśnianie mechanizmów procesów informacyjnych i wszelkich procesów mających miejsce w informacyjnej infrastrukturze;
– projektowanie i modernizowanie systemów informacyjnych”[9].

Podejmując problem określenia istoty i sposobu pojmowania terminu „informacja” przystającego do potrzeb współczesnych, należy zauważyć, iż jej wytwarzanie i przekazywanie stanowi czynność, która w sposób naturalny towarzyszy człowiekowi[10] od początków jego istnienia. Ludzie bowiem zawsze przy pomocy środków dostępnych im na danym etapie rozwoju starali się komunikować ze swoim otoczeniem. Odbierali także i przekazywali odczucia, doświadczenia, emocje oraz wrażenia. Można zatem powiedzieć, że każdy człowiek już z chwilą pojawienia się na ziemi funkcjonował w określonym środowisku informacyjnym. Środowisko to, rzecz jasna, wraz z procesami rozwojowymi zmieniało swój kształt. W optyce Małgorzaty Kisilowskiej środowisko informacyjne to zbiór osób, organizacji i systemów, które gromadzą, przetwarzają i rozpowszechniają informację oraz otoczenie, w jakim te procesy są realizowane[11]. O wiele szersze ujęcie środowiska informacyjnego (infosfery) proponuje Wiesław Babik, pisząc, że w „infosferze mamy do czynienia z tworzeniem nowych źródeł informacji i ciągłym przepływem informacji. Nieustannie powstają nowe informacje, które podlegają różnorodnym procesom przetwarzania, trwa też ich multiplikacja. Dzięki temu infosfera ciągle się rozszerza, chociaż w sposób niekontrolowany. Zjawisko to, oprócz pozytywnych skutków polegających na zwiększeniu dostępu do informacji, generuje również skutki negatywne, czyli zagrożenia. Infosferę tworzą ludzie, informacje (zbiory, źródła), kanały informacyjne, a także narzędzia do jej przekazu od nadawców do

[9] M. Górny, dz. cyt., s. 36.

[10] Nie oznacza to, że jest to właściwość tylko rodzaju ludzkiego. Informacje generują i przekazują we właściwy dla siebie sposób także inne składniki świata ożywionego, np. rośliny czy zwierzęta. Chociaż należy podkreślić, że w dyskusji nad obecnością informacji w przyrodzie nieożywionej zarysowują się trzy zasadnicze tendencje, zgodnie z którymi albo stanowi ona właściwość wszystkich obiektów materialnych, albo występuje tylko w systemach samoregulujących się, albo jest wynikiem stosunków międzyludzkich, to pierwsze z nich wydaje się najbardziej adekwatne.

[11] Zob. M. Kisilowska, *Przestrzeń informacyjna jako termin informatologiczny*, „Zagadnienia Informacji Naukowej” 2011, nr 2, s. 44.

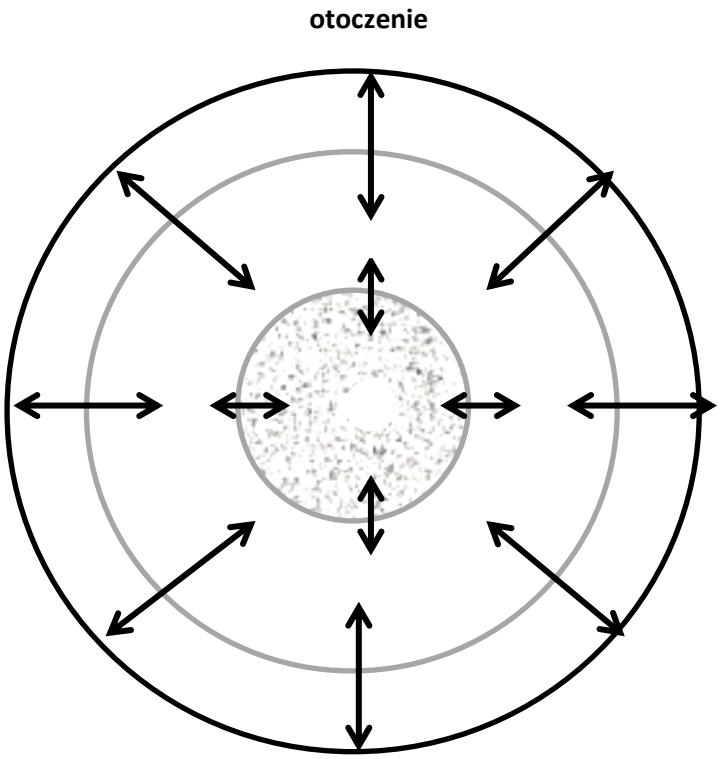
odbiorców w procesie informowania”[12]. Ponieważ wiek XXI przyniósł z sobą olbrzymi, wręcz niekontrolowany przyrost zasobów informacyjnych, skutkuje to narastaniem znaczących zakłóceń tego środowiska polegających m.in. na pojawieniu się nadmiaru informacji rodzącego coraz więcej trudności (barier) w docieraniu do tych informacji, które mają charakter wartościowy i są rzeczywiście potrzebne danemu użytkownikowi. Taka sytuacja sprzyja także wszystkim tym podmiotom, które sięgają po różne narzędzia służące do walki informacyjnej czy działań przestępczych, pozwala bowiem zręcznie ukrywać ich destrukcyjną działalność w coraz bardziej zagmatwanej i trudnej do w pełni racjonalnej oceny i percepcji przez przeciętnego człowieka infosferze. Dążąc do podkreślenia związków człowieka z infosferą, przywoływany wcześniej W. Babik używa pojęcia antropoinfosfera, która jest traktowana przez niego jako „ogół informacji dostępnych człowiekowi poprzez jego świadomość, które potencjalnie może on zużytkować przy realizacji swych życiowych celów”[13]. Jak wskazuje cytowany autor (z czym należy się zgodzić), termin ten wyraźnie podkreśla, jak istotnym elementem środowiska informacyjnego jest człowiek, który nie znajduje się na zewnątrz, ale pozostając w ścisłych relacjach z informacją, stanowi jego integralną część. Relacje te zachodzą zarówno w infosferze wewnętrznej, jak i w infosferze zewnętrznej[14]. Charakteryzując te dwie warstwy infosfery, można za Juliuszem. L Kulikowskim[15] wskazać. że:

- infosfera wewnętrzna to informacje utrwalone w pamięci człowieka, obejmujące życiowe doświadczenie, wiedzę, wspomnienia oraz informacje w pamięci krótkotrwałej, odbierane zmysłami;
- infosfera zewnętrzna to informacje dostępne człowiekowi potencjalnie, pod warunkiem podjęcia czynności zgodnych z jego możliwościami fizycznymi, psychicznymi, społecznymi, materialnymi oraz kompetencjami informacyjnymi[16].

Jednym z przejawów reakcji na działania niszczące środowisko informacyjne jest wyodrębnianie nowych dziedzin nauki, które za przedmiot swoich zainteresowań obierają budowanie świadomości znaczenia informacji, usuwanie barier informacyjnych, a także ochronę dóbr intelektualnych[17]. Do najbardziej

[12] W. Babik, *Ekologia informacji*, Kraków 2014, s. 20.
[13] Tamże, s. 23.
[14] Zob. tamże.
[15] Zob. rys 1.
[16] Zob. J.L. Kulikowski, *Człowiek i infosfera*, „Problemy” 1978, nr 3, s. 4.
[17] Zob. W. Babik, *Ekologia informacji…*, s. 7.

dojrzałych (oprócz scharakteryzowanej już wcześniej nauki o informacji) tego typu dziedzin należy ekologia informacji, czasami też określana jako infoekologia. Pojęcia tego badacze zaczęli używać z końcem lat 70. minionego stulecia. Obecnie ekologia informacji jest traktowana jako dziedzina wiedzy badająca prawa i odkrywająca prawidłowości rządzące informacją w tzw. ekosystemach informacyjnych, w szczególności zaś te związane z przepływem informacji między ludźmi[18].



Rysunek 1. Infosfera
Źródło: J.L. Kulikowski, *Człowiek i infosfera*, „Problemy" 1978, nr 3, s. 3.

W ogólnym ujęciu zainteresowania badawcze infoekologii koncentrują się wokół:

– infosfery i nisz informacyjnych;
– nadmiaru oraz deficytu informacji;
– szumu i smogu informacyjnego;

[18] Tamże, s. 8.

– barier informacyjnych oraz stresu informacyjnego;
– kompetencji informacyjnych.

W poszerzonym zakresie, według W. Babika, badania te dotyczą:

– ludzkiego środowiska informacyjnego;
– ekologicznego zarządzania informacją;
– potrzeb i barier informacyjnych;
– zachowań informacyjnych;
– kultury i etyki informacyjnej;
– konsumpcji informacji;
– profilaktyki i higieny informacyjnej;
– bezpieczeństwa informacji;
– polityki informacyjnej[19].

Do grupy dyscyplin naukowych podejmujących kwestię zagadnień związanych z funkcjonowaniem środowiska informacyjnego należą również stosunkowo niedawno powstałe nauki o bezpieczeństwie. W polskim piśmiennictwie utrwalonym sposobem działania ze strony przedstawicieli tych nauk jest rozpatrywanie różnych kwestii z zakresu bezpieczeństwa informacyjnego. Według ustaleń poczynionych przez H. Batorowską konteksty, jakich dotyczą publikacje wspomnianej powyżej grupy badaczy, obejmują następujące kategorie: „komponent bezpieczeństwa narodowego, komponent kultury bezpieczeństwa, komponent kultury informacyjnej, komponent ekologii informacji, bezpieczeństwo w dobie globalizacji i społeczeństwa informacyjnego, element międzynarodowej i lokalnej polityki informacyjnej, cel polityki bezpieczeństwa informacyjnego, przedmiot technologii informatyczno-komunikacyjnych (infrastruktura teleinformatyczna – obsługa i eksploatacja), równoznacznik bezpieczeństwa informacji i ochrony danych, proces zarządzania bezpieczeństwem informacji (organizacja audytu informacji), obszar wpływu manipulacji medialnej przez środki masowego przekazu, wyznacznik organizacji i jej kultury organizacyjnej, przedmiot walki konkurencyjnej i biznesowej (gospodarka elektroniczna), element walki informacyjnej (przedmiot wojny informacyjnej, cyberwojny), część edukacji dla bezpieczeństwa”[20]. Przywołana autorka dokonała także analizy ilościowego przyrostu publikacji w polskim piśmiennictwie naukowym w latach 2002–2017,

[19] Zob. tamże, s. 109–110.
[20] Zob. H. Batorowska, *Bezpieczeństwo informacyjne w dyskursie naukowym – kierunki badań*, [w:] *Bezpieczeństwo informacyjne w dyskursie naukowym*, H. Batorowska, E. Musiał (red.), Kraków 2017, s. 11.

odnoszących się do kwestii bezpieczeństwa informacyjnego w oparciu o dane z Biblioteki Narodowej. Jak wynika z tych ustaleń, w latach 2002–-2009 zarejestrowano w katalogach Biblioteki Narodowej 51 rekordów dotyczących tego obszaru, natomiast w latach 2010–2017 tych rekordów było 428, w tym aż 214 w latach 2016–2017[21].

Dążąc do znalezienia najbardziej przydatnego dla celów prowadzonych analiz ujęcia terminu informacja[22], należy podkreślić, że wywodzi się on od łacińskiego rzeczownika „informatio" oznaczającego wizerunek, zarys, pojęcie[23]. W świetle tej starożytnej etymologii termin ten wskazuje na istnienie procesu odwzorowywania stanów i rzeczy, tworzenia ich przedstawienia, a następnie przekazywania tego w postaci komunikatów. Znajduje to zresztą odzwierciedlenie w potocznym (intuicyjnym) rozumieniu informacji, gdzie jest ona pojmowana jako treść komunikatu, a także jako sam komunikat.

Zgodnie ze słownikowymi definicjami informacja to: „wiadomość o czymś lub zakomunikowanie czegoś"[24], „informacja o jakiejś sprawie, osobie, rzeczy lub wydarzeniu to coś, co napisano lub powiedziano o nich i po czym czasem można je rozpoznać"[25], „wiadomość dotycząca fragmentu rzeczywistości lub go zastępująca, czynnik fizyczny powodujący taką wiadomość, możliwy do utrwalenia i podatny na przetwarzanie"[26].

W ujęciu jednej z najnowszych tematycznych encyklopedii poświęconej bezpieczeństwu informacja jest postrzegana „jako odbicie (odwzorowanie) różnorodności cechującej otaczającą rzeczywistość (obiekt, zdarzenie, proces, zjawisko)"[27].

W literaturze przedmiotu nie ma konsensusu co do rozumienia pojęcia „informacja". Co więcej, dość często podkreśla się, że ma ono charakter pierwotny i w sensie normatywnym nie poddaje się definiowaniu[28]. Zajmujący się filozofią informacji Luciano Floridi[29] stwierdza wręcz, że „informacja jest

[21] Zob. tamże, s. 9.
[22] Zob. rozważania na ten temat: W. Fehler, *Informacja jako przedmiot polityki bezpieczeństwa informacyjnego*, „Studia Humanistyczno-Społeczne" 2018, t. 22, s. 161–164.
[23] Zob. K. Kumaniecki *Słownik łacińsko-polski*, Warszawa 1957, s. 260.
[24] J. Bralczyk, *Słownik 100 tysięcy potrzebnych słów*, Warszawa 2005, s. 247.
[25] *Inny słownik języka polskiego*, M. Bańko (red.), Warszawa 2000, t.1, s. 537.
[26] Z. Ploski, *Słownik encyklopedyczny – informatyka*, Wrocław 1999, s. 135.
[27] *Encyklopedia bezpieczeństwa*, O. Wasiuta, S. Wasiuta (red.), Kraków 2021, t. 2, s. 570.
[28] Zob. *Vademecum bezpieczeństwa informacyjnego*, O. Wasiuta, R. Klepka (red.), Kraków 2019, t. 1, s. 428.
[29] Luciano Floridi – profesor filozofii i etyki informacji na Uniwersytecie w Oksfordzie. Dyrektor Cyfrowego Laboratorium Etyki w Oxford Internet Institute. Zajmuje się badaniami

ciągle złudnym pojęciem. Jest to skandaliczne nie samo przez się, ale dlatego, że tak wiele fundamentalnej pracy teoretycznej opiera się na wyraźnej analizie i wyjaśnieniu informacji oraz jej pojęć pokrewnych"[30]. W uzupełnieniu stanowiska L. Floridiego można jako swego rodzaju komentarz przedstawić opinię M. Hetmańskiego, który podkreśla, że termin informacja „nie jest zwykłą nazwą leksykalną, której cechy w prosty i bezproblemowy sposób formułowane byłyby w dowolnym słowniku czy jakimkolwiek innym kompendium wiedzy. Jest to nazwa zbyt ogólna, aby mogła być zwykłą nazwą leksykalną, chociaż większość słowników i encyklopedii (….) trafnie wylicza jej podstawowe cechy konstytutywne – informacyjność (cecha rzeczy), bycie informacją (cecha stanu rzeczy), informowanie (cecha relacji)"[31]. Zbigniew Tworak, podkreślając wieloznaczność terminu „informacja" i jego szczególną zdolność do zmiany znaczenia pod wpływem otoczenia i kontekstu, uważa brak rozpoznania specyficznej natury informacji za stan niefortunny, zważywszy na wypracowany duży zbiór ilościowych i ścisłych metod opisu i pomiaru informacji[32]. Jak zauważa uznana i przywoływana już wcześniej badaczka problematyki – H. Batorowska – mimo iż informacja jest pojęciem niedefiniowalnym w sensie normatywnym, to stanowi, podobnie jak materia czy energia, konstytutywny składnik otaczającej człowieka rzeczywistości[33]. Podobny pogląd prezentują Jerzy Kisielnicki oraz Tomasz Gwiazda, podkreślający, że „informacja jest jednym z najtrudniej definiowanych pojęć naukowych. Mimo że każdy intuicyjnie zdaje sobie sprawę z tego, co to jest informacja, to jednak jej zdefiniowanie napotyka wiele problemów"[34]. Według Norberta Wienera, który jest nazywany ojcem cybernetyki i który uznał pojęcie informacji za jedno z trzech fundamentalnych (obok masy i energii) pojęć niezbędnych do opisu świata, jest ona „nazwą treści zaczerpniętej ze świata zewnętrznego w miarę jak dostosowujemy doń swe zmysły"[35]. Zdaniem Jamesa A.F. Stonera,

dotyczącymi informacji i etyki komputerowej (etyki cyfrowej), filozofii informacji i filozofii technologii.

[30] L. Floridi, *Open problems in the philosophy of information,* „Metaphilosophy" 2004, no. 35 (4), p. 560, cyt. za: M.J. Schroeder, *Spór o pojęcie informacji*, „Studia Metodologiczne" 2015, nr 34, s. 19.

[31] M. Hetmański, *Świat informacji,* Warszawa 2015, s. 25.

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

[33] Zob. O. Wasiuta, R. Klepka, dz. cyt., t. 1, s. 428.

[34] J. Kisielnicki, T. Gwiazda, *Wstęp do informatyki w zarządzaniu*, Warszawa 2004, s. 9.

[35] N. Wiener, *Cybernetyka i społeczeństwo*, Warszawa 1960, s. 16.

specjalisty od zarządzania, „informacja jest wynikiem uporządkowania danych lub ich przeanalizowania w jakiś znaczący sposób”[36]. W zbliżony sposób informację definiuje kolejny autorytet z tego zakresu, Ricky W. Griffin, twierdzący, że są „to dane przedstawione w sposób mający jakieś znaczenie”[37]. Z kolei według Jana Madeja informacja to „wszystkie papierowe i elektroniczne bazy danych, kartoteki, dokumenty oraz dyspozycje ustne, które są generowane, przekazywane i gromadzone w systemie informacyjnym przedsiębiorstwa”[38]. W optyce Anny Skowronek-Mielczarek i Zbigniewa Leszczyńskiego „za informacje można uznać dane, które po określonym przetworzeniu nabierają sensu, niosą określoną wiedzę oraz umożliwiają wyciąganie wniosków”[39]. Jak widać, wszystkie cztery przywołane powyżej definicje odnoszą się w znacznej mierze do analizy i przetwarzania treści składających się na informacje. W takim ujęciu informacja stanowi zbiór przetworzonych danych, wytworzony w określonej formie i przekazany w konkretnym celu. Według Andrzeja Drozda informacja to „powiadomienie o czymś, zakomunikowanie czegoś, wiadomość, wskazówka, pouczenie” albo „każdy czynnik, dzięki któremu ludzie lub urządzenia automatyczne mogą bardziej sprawnie, celowo działać”[40]. Glynn Harmon zwraca uwagę, że „informacja to metaenergia – impuls energetyczny, który reguluje większe ilości energii w różnych rodzajach systemów biologicznych lub fizycznych oraz pomiędzy tymi systemami”[41]. Tadeusz Kifner z kolei zauważa, iż „informacja jest elementem wiedzy, faktem, wiadomością, komunikatem lub wskazówką gromadzoną, komunikowaną lub przekazywaną komuś za pomocą jakiegoś kodu lub języka”[42]. Leopold Ciborowski wskazuje, że „»informacja« jako nazwa symbolizuje pojęcia odnoszące się do dwóch rodzajów treści:

(1) materialnych – doznawanych, bezpośrednio i pośrednio, poprzez układ zmysłowy człowieka, które można nazywać »treściami doznań zmysłowych«;

[36] J.A.F. Stoner, R.E. Freeman, D.R. Gilbert, *Kierowanie*, Warszawa 2001, s. 589.
[37] R.W. Griffin, *Podstawy zarządzania organizacjami*, Warszawa 2000, s. 676.
[38] J. Madej, *Polityka bezpieczeństwa i system ochrony informacji w przedsiębiorstwie*, „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie” 2002, nr 604, s. 138.
[39] A. Skowronek-Mielczarek, Z. Leszczyński, *Controlling – analiza i monitoring w zarządzaniu przedsiębiorstwem*, Warszawa 2007, s. 37.
[40] A. Drozd, *Uprawnienie podmiotu zatrudniającego do pozyskiwania informacji o kandydacie na pracownika*, „Państwo i Prawo” 2000, nr 12, s. 66–77.
[41] G. Harmon, *The measurement of information*, „Information Processing and Management” 1984, no. 1–2, p. 193, cyt. za: B. Stefanowicz, *Informacja. Wiedza. Mądrość,* Warszawa 2013, s. 8.
[42] T. Kifner, *Polityka bezpieczeństwa i ochrony informacji*, Gliwice 1999, s. 14.

(2) niematerialnych – stanowiących wytwory ludzkiego myślenia, które można nazywać »treściami doznań umysłowych«" [43].

Nieco inny, bardziej pragmatyczny pogląd prezentuje Elżbieta Niedzielska, podkreślająca, że informacja jest „tym, co w jakiś sposób porządkuje rzeczy fakty, zjawiska, procesy itp., a mówiąc dokładniej – tym czymś, co danym (nieprzetworzonej, »surowej« liczbie, tekstowi, obrazowi, dźwiękom) przydaje ostatecznie treści znaczeniowej, wzbogacając naszą wiedzę o przedmiocie rozważań"[44]. Warto na tym etapie rozważań odnotować także stanowiska Mariusza Maciejewskiego oraz Leszka F. Korzeniowskiego. Pierwszy z autorów stwierdza, że jest to „utrwalony w dowolny sposób (także w pamięci człowieka) komunikat (wiedza, świadomość) o jakimś fakcie"[45]. Natomiast L.F. Korzeniowski uważa, że „informacja jest to treść przekazywana przez komunikat, umożliwiająca zrozumienie sensu (znaczenia) danych i relacji między nimi"[46]. Podobny zakres treściowy temu pojęciu nadaje Edward Kowalczyk, pisząc, że informacja to „różnorodna, szeroko rozumiana treść wiadomości, wykorzystana w celowym działaniu lub zachowaniu"[47]. W opinii przedstawiciela nauk społecznych Mirosława Marciniaka informacja oznacza „wytworzoną w naszych umysłach sumę znaczeń, nadanych bodźcom odebranym przez organizm z otoczenia. Dodajmy – odebranych świadomie i tak też zinterpretowanych"[48]. Mimo że – jak zauważa Tomasz Szewc – generalnie „w nauce prawa unika się bliższego określenia pojęcia informacji, zadowalając się jego znaczeniem potocznym jako komunikatu – wiadomości, wyrażonych w dowolny sposób"[49], to część reprezentujących nauki prawne[50] badaczy jednak kwestię tę odejmuje.

---

[43] L. Ciborowski, *Pojęciowa interpretacja terminu „informacja" i jej pochodnych*, „Zeszyty Naukowe AON" 2010, nr 4, s. 89.

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

[45] M. Maciejewski, *Prawo informacji – zagadnienia podstawowe*, [w:] *Prawo informacji. Prawo do informacji*, W. Góralczyk jr. (red.), Warszawa 2006, s. 31

[46] L.F. Korzeniowski, *Firma w warunkach ryzyka gospodarczego,* Kraków 2002, s. 129.

[47] E. Kowalczyk, *O pojęciu informacji,* Warszawa 1981, s. 23.

[48] M. Marciniak, *Informacja w procesie decydowania politycznego*, „Rocznik Nauk Politycznych" 2010, nr 1, s. 43.

[49] T. Szewc, *Publicznoprawna ochrona informacji*, Warszawa 2007, s. 4.

[50] W literaturze prawniczej zaznacza się, że sposób pojmowana informacji w aktach prawa międzynarodowego bywa odmienny od tego stosowanego w prawie wewnętrznym. Jako przykład w tym kontekście Andrzej Redelbach przytacza definicję przyjętą przez Komitet Ministrów Rady Europy, w której informację rozumie się jako „każde oświadczenie o stanie faktycznym, każdą opinię w formie tekstu, dźwięku lub obrazu". A. Redelbach, *Prawa naturalne, prawa człowieka, wymiar sprawiedliwości. Polacy wobec Europejskiej Konwencji Praw Człowieka*, Toruń 2000, s. 257.

I tak Barbara Kunicka-Michalska wskazuje, że informację „rozumieć należy jako wiadomość lub sumę wiadomości o osobie albo o stanie rzeczy, dotyczącą faktów, stanowiącą logiczną całość”[51]. Ciekawe ujęcie przedstawia także inna przedstawicielka wspomnianych nauk prawnych Izabela Bernatek-Zaguła, która analizując informację jako kategorię prawną, wypracowała bardzo konkretne i czytelne jej ujęcie (nawiązujące po części do ustaleń cytowanego wcześniej M. Marciniaka), zgodnie z którym „informacja to wytworzona w umyśle człowieka suma znaczeń, nadanych bodźcom odebranym przez niego z otoczenia, mającym dla niego znaczenie i wnoszącym do jego świadomości element nowości, czyli zmniejszającym jego niewiedzę”[52].

Na zakończenie powyższych rozważań, przed zaprezentowaniem autorskiej definicji informacji, warto przywołać tę sformułowaną przez jednego z wybitnych znawców problematyki, Piotra Sienkiewicza, który określił ją 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”[53]. W świetle przedstawionych uwag, w ramach ich rekapitulacji, możliwe jest, zdaniem autora, postrzeganie informacji jako specyficznego dobra o charakterze niematerialnym, którego istotę określają treści czerpane ze świata zewnętrznego w postaci wiadomości (komunikatów) dotyczących faktów zdarzeń i cech dotyczących określonych obiektów i procesów, które łączone w procesie intelektualnego ich przetwarzania w określone nowe całości zmniejszają niewiedzę i towarzyszącą jej niepewność. W takim ujęciu informacja to pewien docierający do odbiorcy ciąg sygnałów werbalnych i niewerbalnych, który w zależności od indywidualnych możliwości i potrzeb jest modyfikowany i wykorzystywany. Przyjmując powyższą definicję informacji, należy podkreślić wyraźnie różnice pomiędzy informacją a pojęciami pokrewnymi: sygnałem, znakiem, komunikatem, daną, wiadomością, wiedzą. Wspomniane terminy odnoszące się do różnych kategorii zjawisk informacyjnych często są używane w sposób zamienny i nieprecyzyjny. Istnieje zatem konieczność

[51] B. Kunicka-Michalska, *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości. Rozdział XXX i XXXIII Kodeksu karnego. Komentarz*, Warszawa 2000, s. 391.
[52] I. Bernatek-Zaguła, *Informacja jako kategoria prawna,* „Dyskurs Prawniczy i Administracyjny” 2018, nr 1, s. 27.
[53] P. Sienkiewicz, *Ewaluacja informacji w społeczeństwie informacyjnym*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług” 2011, nr 67, s. 127.

przywołania ich definicji i opisu tak, by tworzyły nie tylko pewien logiczny układ semantyczny, ale stwarzały również możliwość jak najbardziej adekwatnych ich zastosowań. Za bardzo przydatną w tym względzie uznać należy systematyzację sporządzoną przez cytowanego już wcześniej E. Kowalczyka, która obejmuje charakterystykę następujących pojęć:

- sygnał – zmienne w czasie w sposób ciągły lub dyskretny zjawisko fizyczne (zaburzenie fizyczne) występujące i wyraźnie określone w pewnym przedziale czasu i zlokalizowane w danym punkcie przestrzeni;
- znak – rozumiany jako sygnał elementarny, przyporządkowany pewnej elementarnej treści (np. przyporządkowany danej literze alfabetu);
- wiadomość – ciąg znaków;
- komunikat – wiadomość, ale z uporządkowanymi logicznie w jakimś języku treściami elementarnymi, którym odpowiadają znaki[54].

Zważywszy na fakt, że jednym z najczęściej popełnianych błędów (niestety nie tylko w języku potocznym) jest zamienne stosowanie pojęcia „dane" i „informacje", ważne jest również podkreślenie zasadniczych różnic, które dotyczą tych dwu terminów[55]. Dana, jako jednostka danych, jest to jeden lub kilka symboli użytych do reprezentowania czegoś. Jak wskazują Mariusz Grabowski oraz Agnieszka Zając „dane reprezentują fakty. W systemach zarządzania wspomaganych komputerowo dane są kodowane za pomocą odpowiednich symboli. Mogą być rejestrowane, przetwarzane i przesyłane. Dane są przesyłane do świadomości odbiorcy w postaci komunikatu, zatem każdy komunikat zawiera dane. Choć same dane nie mają znaczenia ani celu, to dobór odpowiednich symboli może narzucać lub sugerować ich określoną interpretację"[56].

[54] Zob. E. Kowalczyk, dz. cyt., s. 22–23.
[55] Zob. tabela 1.
[56] M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji*, s. 16, https://www.cri.agh.edu.pl/uczelnia/tad/PSI11/art/Dane_informacje_wiedza.pdf [dostęp 18.04.2021 r.].

Tabela 1. Wybrane definicje danych i informacji zaczerpnięte z literatury

Autorzy	Definicje danych	Definicje informacji
Avison and Fitzgerald (1995)	Dane reprezentują nieustrukturyzowane fakty (s. 12).	Informacja ma znaczenie… pochodzi z wyselekcjonowania danych, ich podsumowania i prezentacji w taki sposób, by były użyteczne dla odbiorcy (s. 12).
Clare and Loucopoulos (1987)	Fakty zgromadzone z obserwacji lub zapisów dotyczących zjawisk, obiektów lub ludzi (s. 2).	Wymagania do podejmowania decyzji. Informacje są produktem istotnego przetwarzania danych (s. 2).
Galland (1982)	Fakty, koncepcje lub wyniki w postaci, która może być komunikowana i interpretowana (s. 57).	Informacje to to, co powstaje w wyniku pewnych działań myślowych człowieka (obserwacji, ana-liz) z sukcesem zastosowanych do danych, by odkryć ich istotę lub znaczenie (s. 127).
Hicks (1993, 3rd ed.)	Reprezentacja faktów, koncepcji lub instrukcji w sposób sformalizowany, umożliwiający komunikowanie, interpretację lub przetwarzanie przez ludzi lub urządzenia automatyczne (s. 668).	Dane przetworzone tak, by miały znaczenie dla decydenta w konkretnej sytuacji decyzyjnej (s. 675).
Knight and Silk (1990)	Numery reprezentujące obserwowalne obiekty lub zagadnienia (fakty) (s. 22).	Znaczenie dla człowieka związane z obserwowanymi obiektami i zjawiskami (s. 22).
Laudon and Laudon (1991)	Surowe fakty, które mogą być kształtowane i formowane, by stworzyć informacje (s. 14).	Dane, które zostały ukształtowane lub uformowane przez człowieka w istotną i użyteczną postać (s. 14)
Maddison (red.) (1989)	Język naturalny: podane fakty, z których inni mogą dedukować, wyciągać wnioski. Informatyka: znaki lub symbole, w szczególności w transmisji w systemach komunikacji i w przetwarzaniu w systemach komputerowych; zwykle, choć nie zawsze, reprezentujące informacje, ustalone fakty lub wynikającą z nich wiedzę; reprezentowane przez ustalone znaki, kody, zasady konstrukcji i strukturę (s. 168).	Zrozumiała, użyteczna, adekwatna komunikacja w odpowiednim czasie; jakikolwiek rodzaj wiedzy o rzeczach i koncepcjach w świecie dyskusji, która jest wymieniana pomiędzy użytkownikami; to treść, która ma znaczenie, a nie jej odwzorowanie (s. 174).
Martin and Powell (1992)	Surowce życia organizacji; składają się z rozłącznych numerów, słów, symboli i sylab odwołujących się do zjawisk i procesów biznesu (s. 10).	Informacje pochodzą z danych, które zostały przetworzone tak, by stały się użyteczne w podejmowaniu decyzji w zarządzaniu (s. 10).

Źródło: M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji*, s. 8, https://www.cri.agh.edu.pl/uczelnia/tad/PSI11/art/Dane_informacje_wiedza.pdf [dostęp: 20.12.2020 r.].

Tabela 2. Podstawowe różnice między informacją a wiedzą

Informacje	Wiedza
Przetworzone dane	Pozwala na podjęcie działań
Jasna, rzeczowa, prosta i uporządkowana	Mętna, niejasna, częściowo nieuporządkowana
Łatwa do wyrażenia w formie pisemnej	Intuicyjna, trudna do przekazania, wyrażenia ustnego lub zilustrowania
Uzyskana z danych przez kondensowanie, poprawianie, kontekstualizację i wyliczanie	Tkwi w powiązaniach, rozmowach, intuicji wynikającej z doświadczeń oraz ludzkiej umiejętności porównywania sytuacji, problemów i rozwiązań
Nie zależy od właściciela	Jest zależna od właściciela
Radzą sobie dobrze z nią systemy informatyczne	Wymaga kanałów nieformalnych
Podstawa zrozumienia dużej ilości danych	Podstawa inteligentnego podejmowania decyzji, przewidywania, projektowania, planowania, diagnozowania i intuicyjnego oceniania
Wynika z danych; sformalizowana w bazach danych, książkach, instrukcjach i dokumentach	Tworzona w umysłach; przedmiot zespolonej wymiany; wynika z doświadczenia, sukcesów i pomyłek
Sformalizowana, wychwycona i objaśniona; pozwala na wielokrotne wykorzystanie	Pojawia się w umysłach ludzi w wyniku doświadczeń

Źródło: D. Bogdanow, *Zarządzanie informacją w jednostkach samorządu terytorialnego*, Opole 2016, s. 43.

Wiadomość oznacza ciąg sygnałów o znaczeniu przedmiotowym lub symbolicznym o charakterze obiektywnym. Informacja to zinterpretowane dane. Informacja w stosunku do wiadomości stanowi kategorię wtórną o charakterze subiektywnym. Ilość informacji, jaką niesie wiadomość, zależy od stopnia wiedzy odbiorcy. Jeżeli treści w niej ujęte są mu znane, to nie zmniejsza ona jego niewiedzy (entropii). Natomiast kiedy zawiera treści mu nieznane, poziom jego niewiedzy zostaje zredukowany. Inaczej rzecz ujmując, to odbiorca określa, czy wiadomość jest powtórzeniem czegoś, co już wie, czy też jest dla niego nowością. W tym drugim przypadku wiadomość staje się informacją. Jeżeli chodzi o wiedzę[57], to według definicji, której autorami są Thomas H. Davenport oraz Laurence Prusak, jest „to płynne połączenie ukształtowanego doświadczenia, wartości, informacji kontekstowej i ekspertyzy, które zapewniają model oceny oraz pozwalają wcielić nowe

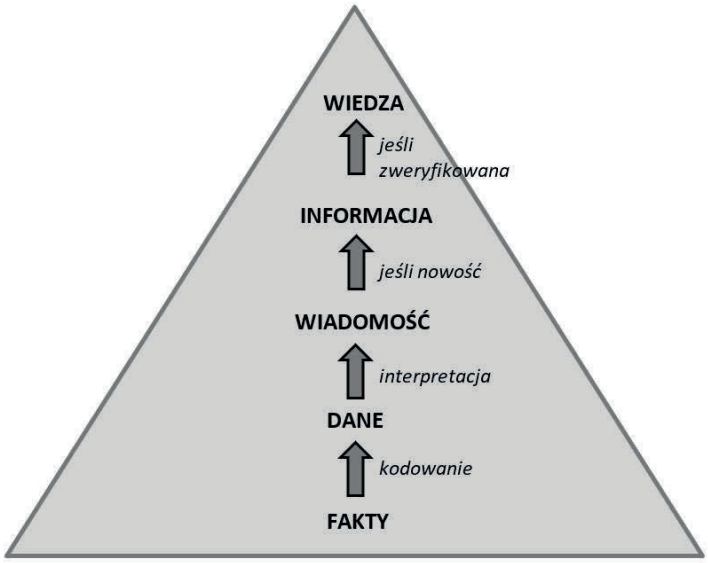
[57] Zob. tabela 2.

doświadczenia i informacje. Swój początek i odniesienie znajduje w umysłach ludzi posiadających wiedzę. Jest osadzona w dokumentach, repozytoriach, procedurach, procesach, praktykach i normach organizacyjnych”[58]. Podobnie postrzega istotę wiedzy Amrit Tiwana, dla którego jest ona konglomeratem kontekstowych doświadczeń, wartości, informacji oraz umiejętności wyznaczającym ramy do oceny, zrozumienia i przyswajania nowych doświadczeń i informacji[59]. Wiedza budowana jest w oparciu o dane[60], wiadomości i informacje[61], które docierają do odbiorcy, a następnie są przez niego kodowane, interpretowane i weryfikowane w ujęciu kontekstualnym oraz praktycznym. W ramach wspomnianej weryfikacji sprawdza się, czy wnioski powstałe w procesie interpretacji są zgodne z rzeczywistością oraz odrzuca się informacje nieistotne i empirycznie nieweryfikowalne.

Istotnym dla właściwego traktowania i rozumienia przedstawianych powyżej pojęć jest posługiwanie się ich hierarchią. W literaturze przedmiotu nazywana jest ona piramidą lub hierarchią wiedzy albo piramidą lub hierarchią informacji[62]. Można również spotkać się przy opisie tej hierarchii (piramidy) z akronimem DIKW, pochodzącym od pierwszych słów poszczególnych składowych w języku angielskim: *data* (dane), *information* (informacja), *knowledge* (wiedza) i *wisdom* (mądrość). Wprawdzie z prowadzonych rozważań nie wynika, aby można było wskazać jakąś definicję informacji o charakterze uniwersalnym, ale na ich kanwie należy dostrzec istnienie szeregu odrębnych podejść, które w minionym stuleciu, jak wskazuje Andrzej Dąbrowski, zaowocowały koncepcjami:

– informacji statystycznej;
– informacji matematycznej;
– informacji algorytmicznej;
– informacji kwantowej;
– informacji jako stanu podmiotu działania;
– informacji semantycznej[63].

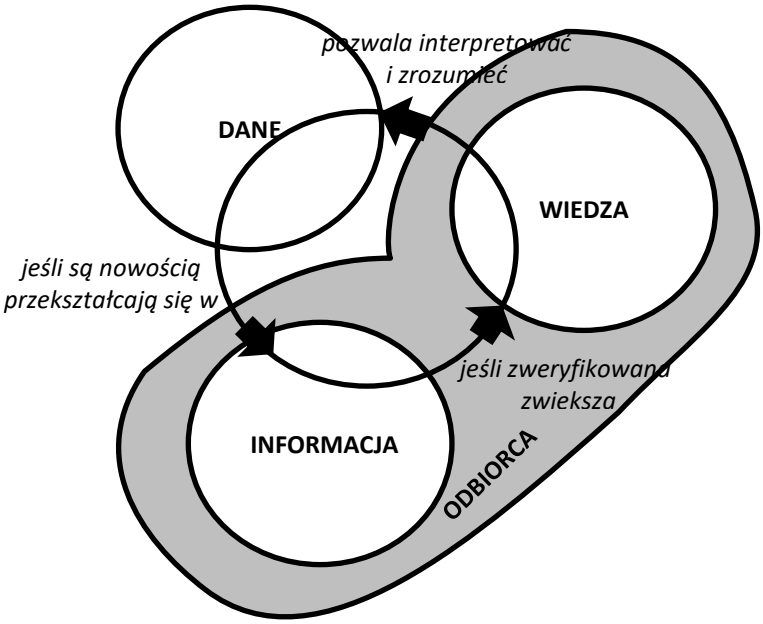
[58] T.H. Davenport, L. Prusak, *Working Knowledge*, Boston 1998, p. 5.
[59] Zob. A. Tiwana, *Przewodnik po zarządzaniu wiedzą*, Warszawa 2003, s. 60.
[60] Zob. rys. 2.
[61] Zob. rys. 3.
[62] Zob. rys. 4.
[63] Zob. A. Dąbrowski, *Filozofia informacji Luciano Floridiego (ekspozycja nieformalno-logiczna)*, „Zagadnienia Naukoznawstwa” 2015, nr 4, s. 448.



Rysunek 2. Kształtowanie się wiedzy
Źródło: M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji*, s. 17, https://www.cri.agh.edu.pl/uczelnia/tad/PSI11/art/Dane_informacje_wiedza.pdf [dostęp 18.04.2021 r.].

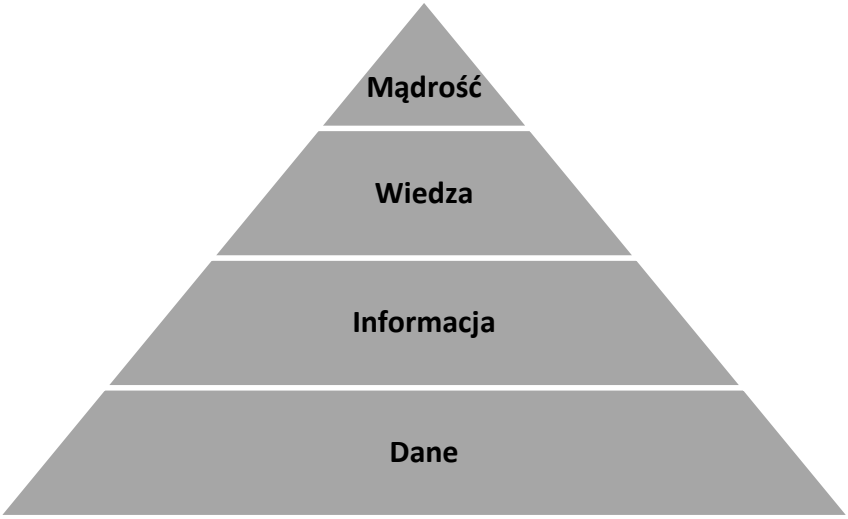
Z kolei L. Floridi przedstawia trzy spojrzenia na kwestię teorii informacji: redukcjonistyczne, antyredukcjonistyczne oraz nieredukcjonistyczne. Pierwsze podejście (redukcjonistyczne) zakłada możliwość stworzenia podstawowej, jednolitej teorii informacji. U podstaw takiej zunifikowanej teorii leżeć ma jedno proste pojęcie informacji, które stanowić będzie o rodzinie innych pojęć. Teoria taka miałaby mieć charakter hierarchiczny i inkluzywny (zawierać bowiem powinna większość dotychczasowych koncepcji informacji). Wprawdzie, jak zauważa L. Floridi, nie dysponujemy jeszcze taką teorią, są jednak jej zwolennicy. Drugie spojrzenie (antyredukcjonistyczne) kładzie nacisk na różnorodność tkwiącą zarówno w naturze pojęcia informacji, jak i w różnych zjawiskach informacyjnych. Zwolennicy takiego stanowiska bronią radykalnej nieredukowalności tych zjawisk, podkreślając, że można mówić jedynie o podobieństwie różnych pojęć informacji. Trzecia podejście (nieredukcjonistyczne) zastępuje redukcjonistyczny model hierarchiczny modelem rozproszonej sieci powiązanych ze sobą za sprawą wzajemnych i dynamicznych wpływów pojęć informacji[64].

[64] Zob. tamże, s. 449.



Rysunek 3. Zależności między danymi, informacją i wiedzą

Źródło: M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji*, s. 18, https://www.cri.agh.edu.pl/uczelnia/tad/PSI11/art/Dane_informacje_wiedza.pdf [dostęp 18.04.2021 r.].



Rysunek 4. Hierarchia DIKW

Źródło: M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji*, s. 5, https://www.cri.agh.edu.pl/uczelnia/tad/PSI11/art/Dane_informacje_wiedza.pdf [dostęp 18.04.2021 r.].

Ewa Wędrowska jako najbardziej fundamentalne i spójne wymienia oraz charakteryzuje następujące teorie informacji:

- matematyczne, zgodnie z którymi informacja traktowana jest jako wielkość fizyczna, z jednej strony, oraz statystyczna własność źródła – z drugiej. Informacja jest miarą czyjejś swobody wyboru podczas selekcji możliwych komunikatów. Teorie te koncentrują się na ilościowych aspektach pojęcia informacji, pomijają natomiast czynniki semantyczne i pragmatyczne;
- semantyczne, rozpatrujące treść, znaczenie wiadomości oraz wzajemne relacje pomiędzy zbiorami znaków a realnymi obiektami czy zjawiskami, jakie te znaki opisują. Wspólną bazą koncepcji semantycznych jest odnoszenie się do strony znaczeniowej wiadomości, czyli właściwości tak formalnych, jak i nieformalnych znaków tworzących wiadomość oraz ich funkcji w procesie komunikowania się;
- pragmatyczne, traktujące informację jako czynnik treściowy, który staje się informacją, gdy może być wykorzystywany dla efektywnego osiągnięcia celów odbiorcy;
- infologiczne, oparte na założeniu, że działalność człowieka wymaga wiedzy, która powstaje dzięki informacjom reprezentowanym przez dane. Istota tych koncepcji wiąże się ze znaczeniem komunikatu, który jest minimalnym (wystarczającym) zbiorem danych umożliwiającym przekaz jednoznacznej treści[65].

Z kolei H. Batorowska wskazuje na istnienie koncepcji:

- tożsamościowej, według której informacja jest identyfikacją wielości dokonywaną poprzez nadanie wielości charakteru jedności;
- filozoficznej, traktującej informację jako odwzorowanie (odbicie) różnorodności cechującej istniejącą rzeczywistość;
- ilościowej, skoncentrowanej na badaniu zjawisk informacyjnych pod kątem ustalania w nich zmian stopnia nieokreśloności w zależności od wyróżnionego stanu danego układu;
- jakościowej (indologicznej), koncentrującej się na własnościach i znaczeniu informacji postrzeganych w aspektach użytkowych[66].

Odnosząc się do przeprowadzonych charakterystyk i analiz, należy w kontekście głównego celu badawczego, jakim jest ustalenie zasadniczych

[65] Zob. E. Wędrowska, dz. cyt., s. 49–55.
[66] Zob. O. Wasiuta, R. Klepka, dz. cyt., t. 1, s. 428–429.

pojęć związanych z bezpieczeństwem informacyjnym, zauważyć, że uwaga teoretyków i praktyków nauki o informacji do początku lat 90. XX w. skupiała się na badaniu: użytkowników i pracowników informacji naukowej, źródeł informacji, warsztatu bibliograficzno-dokumentacyjnego, systemów informacyjnych, organizacji działalności informacyjnej, efektywności i automatyzacji procesów informacyjnych, języków informacyjno-wyszukiwawczych oraz ogólnych problemów nauki o informacji[67]. Ponieważ jednak na przełomie stuleci doszło do gwałtownego rozwoju technologii informacyjnych oraz upowszechnienia dostępu do Internetu, zrodziło to istotne zmiany w dziedzinie tworzenia, przetwarzania oraz dystrybucji informacji. Nowe narzędzia i metody wykorzystywane w procesach informacyjnych spowodowały nie tylko konieczność zmian w systemie kształcenia użytkowników informacji, ale wpłynęły także – na co zwraca uwagę Barbara Sosińska-Kalata – na wygenerowanie nowych obszarów badań w nauce o informacji. Znalazły się wśród nich m.in.: analiza domen wiedzy, architektura informacji, repozytoria cyfrowe, badanie użytkowników, badania ilościowe wykorzystania informacji, ekonomia informacji, etyka informacji, humanistyka cyfrowa, komunikacja człowieka z maszyną, komunikacja naukowa, nowe media i media masowe, organizacja wiedzy, polityka informacyjna, technologia informacyjna, metodologia nauki o informacji, usługi informacyjne, zarządzanie informacją i wiedzą, źródła informacji, zachowania informacyjne, kompetencje informacyjne[68].

Także ekologia informacji, poszerzając zakres swoich zainteresowań, szuka rozwiązań dotyczących tego, jak skutecznie:

– dbać o jakość i odpowiednią ilość informacji;
– postępować z informacją napływającą;
– bronić się przed niekorzystnym oddziaływaniem informacji;
– chronić informację przed niszczycielskim działaniem ludzkim.

Jako szczególnie istotne i niepokojące ekologia informacyjna traktuje zjawisko nadmiaru informacji. W ocenie badaczy[69] ma ono charakter rozwojowy, czemu sprzyja masowa dystrybucja informacji o niskiej jakości, bez cech przydatnych do rozwiązywaniu problemów. Środkami zaradczymi i ochronnymi przed oddziaływaniem takiej informacji powodującej przeciążenie

[67] Zob. M. Dembowska, *Nauka o informacji naukowej (informatologia). Organizacja i problematyka badań w Polsce*, Warszawa 1991, s. 2–3.
[68] Zob. B. Sosińska-Kalata, *Obszary badań współczesnej informatologii (nauki o informacji)*, „Zagadnienia Informacji Naukowej – Studia Informacyjne" 2013, nr 2 (102), s. 28–32.
[69] Zob. W. Babik, *Ekologia informacji*…, s. 92.

informacyjne według ekoinfologów powinny być przede wszystkim działania kształtujące odpowiednie umiejętności i postawy, w szczególności zaś:

- wyrabianie umiejętności rozróżniania informacji rozrywkowej od informacji wartościowych;
- kształtowanie zdolności do świadomego ograniczenia konsumpcji informacji zaspokajającej prymitywne potrzeby (sensacje, plotki, tania rozrywka);
- kształtowanie umiejętności filtrowania informacji i nadawania etykiet, ułatwiających ich katalogowanie i wartościowanie;
- opanowywanie umiejętności organizowania informacji poprzez nadawanie im odpowiedniej rangi oraz priorytetów.

W ramach higieny i profilaktyki informacyjnej ważne są również działania ukierunkowane na:

- usuwanie nadmiaru informacji z infosfery;
- akcje informacyjne i edukacyjne mające na celu zwracanie uwagi na niedobór informacji dobrej jakości;
- inspirowanie i zachęcanie do angażowania się w działalność na rzecz ochrony środowiska informacyjnego człowieka;
- kształtowanie kultury informacyjnej jako jednego z aspektów kultury osobistej.

Odnosząc się do powyższych uwag dotyczących informatologii i infoekologii w kontekście bezpieczeństwa informacyjnego, można powiedzieć, że chociaż wymienione nauki nie podejmują wprost (poza ujmowanym przez W. Babika aspektem bezpieczeństwa informacji) zagadnień z tego zakresu, to jednak ich dorobek oraz wskazywane w przedstawianych analizach obszary zainteresowań dostarczają istotnych ustaleń oraz wytyczają drogi do rozwiązywania szeregu problemów związanych z tym wymiarem bezpieczeństwa.

Konkludując, należy zauważyć, że badacze zajmujący się teorią informacji w większości są zgodni co do tego, że informacja jako pojęcie pierwotne jest niedefiniowalna w sensie normatywnym[70]. Również wyznaczanie zakresu przedmiotowego dla terminu „informacja" nastręcza dużo trudności. Dzieje się tak dlatego, że cech mogących stanowić podstawę wyznaczania zakresu przedmiotowego dla tego terminu jest w rzeczywistości wiele. Jak wskazuje M. Hetmański, „informacja" to nazwa generalna mająca charakter abstrakcyjny o zakresie wyznaczanym nie przez tylko jedną cechę

[70] Zob. J. Unold, *Zarządzanie informacją w cyberprzestrzeni,* Wrocław 2015, s. 19.

konstytutywną, lecz na ogół przez zbiór kilku cech, w tym także tych mających charakter konsekutywny. Specyfika i bogactwo leksykalne tej nazwy budowane jest w oparciu o przejmowanie szeregu cech wraz z ich definicjami z różnych dyscyplin naukowych należących do odmiennych działów nauki[71].

Takie szerokie i ulegające zmianom znaczenie rodzi konieczność dochowania szczególnej staranności w zakresie właściwego posługiwania się tym pojęciem na różnych płaszczyznach publicznego dyskursu. Inaczej rzecz ujmując, zakres przedmiotowy pojęcia „informacja" jest niestały i niejednoznaczny, musi być w związku z tym – stosownie do istniejącego stanu wiedzy i potrzeb – „udokładniany". Nie zamyka to jednak drogi do ujęć opisowych i intuicyjnych, nie podważa również znaczenia informacji wynikającego z faktu, iż tworzy ona zasoby pozwalające na systematyczne zmniejszanie niepewności przez pogłębianie wiedzy o otaczającym człowieka świecie i o nim samym. W związku z takim stanem rzeczy trzeba zaakceptować funkcjonowanie wiele określeń terminu informacja. Chociaż dyskusja o istocie oraz rozumieniu informacji jest ciągle kontynuowana i być może przyczyni się do stworzenia jakiejś mającej cechy uniwersalności koncepcji, to jednak jako realistyczną i jednocześnie racjonalną trzeba przyjąć opinię, że – ze względu na specyfikę różnych dyscyplin naukowych i złożoność form życia społecznego – równolegle funkcjonować będzie wiele teoretycznych i praktycznych podejść do informacji posługujących się specyficznymi (indywidualnymi) założeniami i definicjami, mającymi odrębne własności oraz zastosowania.

1.2. Klasyfikacja informacji

Klasyfikacja informacji jest procesem, w ramach którego dokonuje się jej oceny, charakterystyki i systematyzacji według określonych kryteriów w celu odpowiedniego jej wykorzystania i traktowania. Istota wspomnianej klasyfikacji polega na grupowaniu wzajemnie powiązanych informacji, określaniu znaczenia tych grup dla podmiotu klasyfikującego oraz przypisywaniu poszczególnym grupom ujednoliconych etykiet ułatwiających i usprawniających ich wytwarzanie, przetwarzanie, gromadzenie, odszukiwanie, analizę, przekaz oraz odbiór. Klasyfikacja informacji wymaga znajomości ich lokalizacji,

[71] Zob. M. Hetmański, dz. cyt., s. 24.

treści, objętości i kontekstu. Zasadniczym celem klasyfikowania informacji jest ustalenie jej znaczenia dla danego podmiotu. Jest to połączone z projektowaniem i tworzeniem systemów wytwarzania, dostępu i dystrybucji informacji, a tam, gdzie to jest konieczne, także systemów jej ochrony[72]. W dyskursie naukowym oraz w ramach utylitarnego wykorzystywania informacji stosuje się różnorodne podejścia klasyfikacyjne. Mają one zarówno charakter ogólny, jak i bardziej szczegółowy, a nawet, co zrozumiałe, wąsko specjalistyczny. Rozpoczynając od tych najbardziej ogólnych podziałów, należy przywołać pogląd L. Floridiego, który wyróżnia cztery rodzaje informacji: informacje o czymś, informacje jako coś, informacje do czegoś, informacje w czymś[73]. Marian Cieślarczyk z kolei dzieli informację na tę, która:

– znajduje się w umysłach ludzi;
– jest zgromadzona w szeroko rozumianych bazach danych;
– ma charakter bieżący[74].

Maciej Mrozowski proponuje rozróżniania trzech typów informacji:

– informacje proste (wszelkiego rodzaju zbiory i bazy danych);
– informacje przetworzone (informacje zinterpretowane, z przypisanym znaczeniem i przekształcone w wiedzę);
– informacje zastosowane (wykorzystane w praktyce społecznej)[75].

Justyna Stochaj wyróżnia:

– informacje aktywne – wywołujące u odbiorców konkretne reakcje;
– informacje pasywne – niepowodujące reakcji u odbiorców[76].

Przy pomocy kryterium znaczenia informację dzieli się na bardzo ważną, ważną i nieistotną, kryterium wiedzy pozwala natomiast sklasyfikować informację jako pewną i niepewną[77].

[72] Zob. *Klasyfikacja informacji*, „Bezpieczeństwo Informacji. Biuletyn Tematyczny" 2006, nr 1, s. 4, http://security.dga.pl/biuletyn/DGA_BIULETYN_TEMATYCZNY_01_06.pdf [dostęp: 9.12.2020 r.].
[73] Zob. A. Dąbrowski, *Filozofia informacji…*, s. 449.
[74] Zob. M. Cieślarczyk, *Psychospołeczne i prakseologiczne aspekty bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne w XXI wieku*, M. Kubiak, S. Topolewski (red.), Siedlce-Warszawa 2016, s. 53–54.
[75] Zob. M. Mrozowski, *Media masowe. Władza, rozrywka i biznes*, Warszawa 2001, s. 394.
[76] Zob. M. Deja, A. Rożej, J. Stochaj. J. Stolarski, *Organizowanie i monitorowanie przepływu informacji w jednostkach administracyjnych*, Warszawa 2015, s. 14–17.
[77] Zob. W. Fehler, *Informacja jako przedmiot polityki…*, s. 168.

Wśród ogólnych klasyfikacji informacji mieści się również ta zaprezentowana przez Romana Kwećkę, który wyodrębnia:

- informacje zewnętrzne przejawiające się w funkcji sterowania układem decyzyjnym lub funkcji wpływu otoczenia na dany obiekt;
- informacje wewnętrzne – odzwierciedlające stan wiedzy układu decyzyjnego o obiektach oddziaływania lub uwarunkowaniach zewnętrznych;
- informacje zwrotne – będące reakcją obiektów oddziaływania lub układu decyzyjnego na informacje zewnętrzne[78].

Bardziej rozbudowany podział oparty o miarę treści, autorstwa B. Stefanowicza, wyróżnia informacje:

- faktograficzne – opisujące stan danego obiektu przez wskazanie jego cech i ich wartości w danym czasie;
- komparatywne – ukazujące stan danego obiektu w porównaniu z czymś;
- semantyczne, określające znaczenie (semantykę) przypisywane danemu obiektowi;
- normatywne, charakteryzujące normy nakładane na rozpatrywane obiekty lub wyznaczające warunki ich funkcjonowania;
- klasyfikacyjne (taksonomiczne), obejmujące kryteria rozpoznawania klasy, do której należy dany obiekt, lub służące rozpoznaniu tego obiektu wśród innych obiektów;
- strukturalne, opisujące budowę obiektów;
- przestrzenne, opisujące usytuowanie obiektu w przestrzeni (służące także do uzyskiwania odpowiedzi na pytania, gdzie znajduje się obiekt, skąd pochodzi lub dokąd zmierza);
- imperatywne, zawierające treści o charakterze nakazowym;
- kwerencyjne, zawarte w komunikatach służących do uzyskiwania odpowiedzi na pytania typu: czy? kto? co? jaki? ile? dlaczego? jak dużo?;
- fatyczne, służące do nawiązania lub podtrzymania rozmowy (zwroty typu „nieprawdaż", „czy wiesz", „słuchaj", „wyobraź sobie" itp.)[79].

[78] Zob. R. Kwećka, *Bezpieczeństwo informacyjne*, [w:] *Podstawy bezpieczeństwa narodowego (państwa)*, J. Pawłowski (red.), Warszawa 2017, s. 403.
[79] Zob. B. Stefanowicz, *Informacja. Wiedza...*, s. 28–32.

W bardziej zawężonym zakresie, na gruncie nauki o zarządzaniu, Jerzy Kisielnicki wyodrębnia:

- informację pokrzepiającą (odnoszącą się do bieżącej sytuacji organizacji i mającą przekonywać, że zachodzące zmiany przebiegają zgodnie z założeniami);
- informację rozwojową (dotyczącą oceny stanu lub przebiegu procesu zmian oraz pokazującą ewentualne trudności w tym procesie);
- informację ostrzegawczą (przedstawiającą określone zagrożenia powstałe lub mogące wystąpić w wyniku realizacji zmian w organizacji);
- informację planistyczną (odnoszącą się do przyszłości i pokazującą, jaka będzie wtedy sytuacja);
- informację operacyjną (określającą zmiany w organizacji i pozwalającą na ich porównanie z działalnością innych, podobnych organizacji);
- informację opiniodawczą (dotyczącą danych o bliższym i dalszym otoczeniu zmieniającej się organizacji);
- informację kontrolowaną (przekazywaną otoczeniu i odnoszącą się do zmian zachodzących w organizacji – np. wskaźniki, które zostały przez organizację osiągnięte)[80].

Opierając się na poglądach Katarzyny Materskiej, badającej problematykę zarządzania informacją i wiedzą, można podzielić informacje na:

- tworzone przez dany podmiot organizacyjny na potrzeby własne (strategie, sprawozdania, statystyki, zestawienia, plany rozwoju itp.);
- tworzone przez dany podmiot organizacyjny na potrzeby zewnętrzne (dla interesariuszy, klientów);
- powstające w otoczeniu podmiotu i pozyskiwane na drodze innej niż zakup (np. poprzez monitoring otoczenia czy transfer ze zbiorów otwartych dostępnych dla wszystkich);
- nabywane przez dany podmiot organizacyjny (bazy danych, dostęp do komercyjnych serwisów informacyjnych, analizy eksperckie, licencje)[81].

Prowadząca badania w zakresie jakości informacji w organizacjach zhierarchizowanych Sylwia Wojciechowska-Filipek wyszczególniła trzy grupy informacji. Pierwsza z nich wyodrębniona przy użyciu kryterium wrażliwości (cytowana autorka traktuje to kryterium jako miarę ważności informacji) obejmuje informacje:

[80] Zob. J. Kisielnicki, *Zarządzanie i informatyka*, Warszawa 2014, s. 25–26.
[81] Zob. K. Materska, *Zarządzanie informacją i wiedzą*, [w:] *Nauka o informacji*, W. Babik (red.), Warszawa 2016, s. 362.

– wrażliwe (które należy chronić, aby ich nieuprawnione ujawnienie lub zmanipulowanie nie spowodowało określonej szkody);
– niewrażliwe (niewymagające ochrony).

W ramach drugiej grupy informacji wydzielonej z zastosowaniem kryterium mierzalności przywoływana badaczka wyróżnia:

– informacje mierzalne, przedstawiane wartościami, które mają sens liczbowy;
– informacje niemierzalne, opisujące cechę lub cechy.

Trzecia grupa, wyodrębniona na podstawie miejsca i znaczenia w procesie decyzyjnym, obejmuje informacje:

– kluczowe, determinujące poszukiwanie optymalnych rozwiązań i stanowiące najważniejszy element procesu decyzyjnego;
– istotne (obiektywne i subiektywne) – wpływające znacząco na proces podejmowania decyzji;
– nieistotne, mające znikomy wpływ na podejmowane decyzje;
– rutynowe, pojawiające się cyklicznie w poszczególnych etapach działania organizacji.

Na gruncie prawnym funkcjonuje klasyfikacja informacji oparta o kryterium przedmiotowe, przy użyciu którego wyodrębnia się:

– informację publiczną (informacje o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne);
– informację o obywatelach (informacje dotyczące miejsca urodzenia, stanu cywilnego, miejsca zamieszkania, karalności itp.);
– informację niejawną (informacje, których nieuprawnione ujawnienie mogłoby wyrządzić szkody);
– informację o ochronie zdrowia (informacje niezbędne do prowadzenia polityki zdrowotnej państwa, podnoszenia jakości i dostępności świadczeń opieki zdrowotnej oraz finansowania zadań z zakresu ochrony zdrowia);
– informację oświatową (informacje dotyczące nauczycieli i uczniów oraz jednostek oświatowych);
– informację przestrzenną (opisane metadanymi zbiory danych przestrzennych oraz dotyczące ich usługi, środki techniczne, procesy i procedury);
– informację kryminalną (informacje dotyczące spraw będących przedmiotem czynności operacyjno-rozpoznawczych, wszczętego lub

zakończonego postępowania karnego, w tym postępowania w sprawach o przestępstwa skarbowe oraz dotyczące innych postępowań);
- informację o środowisku (informacje dotyczące stanu środowiska w rozbiciu na różne tworzące to środowisko czynniki);
- informację gospodarczą (informacje dotyczące podmiotów prowadzących działalność gospodarczą);
- informację dotyczącą zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (dane osobowe)[82].

W sferze klasyfikacji prawnych mieści się również wyodrębnianie przy użyciu kryterium legalności informacji:
- legalnych (wytworzonych, zdobytych, przetworzonych, przekazywanych zgodnie z prawem);
- nielegalnych (wytworzonych, zdobytych, przetworzonych, przekazywanych niezgodnie z prawem).

Blisko klasyfikacji prawnych mieści się także kategoryzacja informacji dokonywana z użyciem kryterium autoryzacji, która pozwala wyodrębnić:
- informacje formalne (potwierdzone przez uprawnione do tego podmioty [osoby]);
- informacje nieformalne (bez podania dokładnych źródeł i bez autoryzacji)[83].

Uzasadnione w powyższym kontekście jest również wymienienie podziału informacji na fałszywą i prawdziwą dokonywanego w oparciu o kryterium prawdy.

W ramach specjalistycznego nurtu klasyfikacji funkcjonuje podział odnoszący się do instytucji działających w sferze bezpieczeństwa państwa, sporządzony w oparciu o kryterium ważności i pilności przekazu. Obejmuje on:
- informacje błyskawiczne (o najwyższym stopniu pilności, zazwyczaj przekazywane w formie sygnałów);
- informacje priorytetowe (dotyczące operacji w toku);
- informacje rutynowe (obejmujące wszystkie wiadomości, których treść nie jest pilna i ważna)[84].

[82] Zob. I. Bernatek-Zaguła, *Informacja jako kategoria…*, s. 30–31.
[83] Zob. W. Fehler, *Informacja jako przedmiot polityki…*, s. 168.
[84] Zob. S. Wojciechowska-Filipek, *Zarządzanie jakością informacji w organizacjach zhierarchizowanych*, Warszawa 2015, s. 25–26.

Specjalistyczny aspekt kategoryzacji informacji to również kwestia jej znaczenia w procesie decyzyjnym. W tym kontekście przy użyciu kryterium miejsca w tym procesie informacje mogą być dzielone na:

– bezpośrednio przyczyniające się do podjęcia decyzji;
– pośrednio przyczyniające się do podjęcia decyzji;
– obojętne z punktu widzenia procesu podejmowania decyzji[85].

Wchodząc w obszar klasyfikacji opartej o kryteria szczegółowe, to przy użyciu:

– kryterium czasu ważności dzielimy informacje na posiadające trwałą ważność, ograniczony czas ważności, te o krótkotrwałym czasie ważności;
– kryterium dostępności wydzielamy informacje powszechnie dostępne oraz takie, które są dostępne wyłącznie dla podmiotów upoważnionych;
– kryterium stosunku do teraźniejszości wyodrębniamy informacje retrospektywne, teraźniejsze (bieżące) i prospektywne;
– kryterium formy przekazu (rodzaju nośnika informacji) dzielimy informacje na wizualną, audiowizualną, werbalną, pisemną, elektroniczną, przekazywaną przy pomocy mowy ciała;
– kryterium dokładności wyodrębniamy informacje precyzyjne, nieprecyzyjne oraz ogólne i szczegółowe;
– kryterium ochrony dzielimy informacje na jawne i chronione;
– kryterium zakresu ochrony wyodrębniamy informacje: ściśle tajne, tajne, poufne, zastrzeżone;
– kryterium własności klasyfikujemy informacje jako: prywatne, publiczne (państwowe) osobiste, grupowe, instytucjonalne[86].

Uznając przydatność i znaczenie przedstawionych klasyfikacji, trzeba stwierdzić, że na co dzień w skali powszechnej wyróżniania się zazwyczaj kilka kategorii informacji, co wynika z roli, jaką odgrywają w życiu społeczeństw. Wśród nich wymienić należy przede wszystkim takie kategorie, jak informacja polityczna, informacja gospodarcza, informacja naukowa, informacja kulturalna, informacja publiczna, informacja ekologiczna, informacja sportowa. Nie są to bynajmniej grupy rozdzielne, np. informacja polityczna

[85] Zob. Z. Ścibiorek, *Podejmowanie decyzji,* Warszawa 2003, s. 77–78.
[86] Zob. W. Fehler, *Informacja jako przedmiot polityki…*, s. 168–169.

może być jednocześnie informacją gospodarczą, a naukowa ekologiczną i/lub gospodarczą.

Podsumowując – klasyfikacja informacji to ważny i powszechnie stosowany instrument w procesie budowania wiedzy i zarządzania informacją, którego znaczenie systematycznie wzrasta. Jest tak dlatego, że w obliczu lawinowego przyrostu informacji narzędzie to stwarza możliwość skutecznego prowadzenia jej selekcji. Dzięki temu można wyodrębniać informacje o odpowiadających danemu podmiotowi parametrach spośród tych, które są nieużyteczne, nieaktualne czy wręcz niebezpieczne. Klasyfikacja informacji przy zastosowaniu odpowiednio dobranych kryteriów obok prowadzenia selekcji jakościowej i ilościowej tworzy także podstawy do odpowiedniego traktowania wcześniej wyodrębnionych kategorii informacji, pozwalając m.in. na właściwe budowanie użytecznych zasobów informacyjnych oraz skuteczne przeciwdziałanie zagrożeniom generowanym przez informacje fałszywe czy zmanipulowane. Klasyfikacja pozwala także na skuteczne chronienie informacji wrażliwych (w tym poufnych i tajnych). Jest zatem ważnym instrumentem budowania podstaw bezpieczeństwa informacyjnego oraz bezpieczeństwa informacji.

1.3. Funkcje i cechy informacji

Zgodnie z definicją słownikową funkcja w rozumieniu pozamatematycznym to: „zadanie, które spełnia lub ma spełnić jakaś osoba lub rzecz, czyjeś stanowisko lub zakres obowiązków, możliwość wykonania określonej operacji przez urządzenie lub program komputerowy, wzajemny stosunek zjawisk, z których jedno wynika z drugiego”[87]. Najbardziej ogólną, a jednocześnie bardzo pojemną merytorycznie funkcją informacji jest zmniejszanie niepewności i niewiedzy[88]. M. Cieślarczyk, powołując się na Jerome’a S. Brunera, wymienia m.in. funkcje: regulacyjno-porządkującą, skłaniania do decyzji (zwiększającą stopień pewności), progowo-wyzwalającą (bodźcową), składnika wiedzy[89].

[87] *Słownik języka polskiego PWN* (wersja internetowa), https://sjp.pwn.pl/sjp/funkcja;2558721.html [dostęp:12.12.2020 r.].
[88] Zob. C.E. Shannon, *The Mathematical Theory of Communication*, Illinois 1945, p. 17.
[89] Zob. M. Cieślarczyk, dz. cyt., s. 53.

W zakresie charakterystyki funkcji informacji szczególnie bogaty dorobek ma nauka o zarządzaniu. Jacek Cyprjański wymienia cztery rodzaje wspomnianych funkcji:

– funkcję generowania zasobów wiedzy;
– funkcję decyzyjną;
– funkcję sterowania;
– funkcję towaru[90].

Syntetyczne zestawienie funkcji na tle definicji informacji zaproponował Janusz Czekaj w rozważaniach poświęconych metodom zarządzania informacją[91]. Zbigniew Malara i Jerzy Rzęchowski, wymieniając ogólne funkcje realizowane przez informacje, wskazują na wspieranie procesu zmian, umożliwianie komunikowania się pracowników i kierownictwa, wzbogacanie wiedzy indywidualnej, nawiązywanie więzi z otoczeniem[92]. W bardziej szczegółowym ujęciu powiązanym z funkcjami zarządzania wspomniani badacze wyodrębniają:

– funkcję planistyczną;
– funkcję organizacyjną;
– funkcję motywacyjną;
– funkcję kontrolną.

Funkcja planistyczna umożliwia ułożenie algorytmów postępowania z uwzględnieniem posiadanych zasobów. Funkcja organizacyjna określa sposób realizacji zaplanowanych działań. Funkcja motywacyjna wiąże się z używaniem informacji do skłaniania odbiorców do podejmowania działań zgodnych z celami podmiotu dostarczającego informacji. Funkcja kontrolna urzeczywistnia się poprzez zbieranie oraz wykorzystywanie informacji do sprawdzania, czy realizacja celów (zadań) jest zgodna z założeniami[93].

[90] Zob. J. Cypryjański, *Możliwości szacowania wartości informacji ex ante a funkcje informacji w organizacji*, „Prace Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2005, s. 284, http://www.swo.ue.katowice.pl/swo-2005/zarzadzanie-wiedza-i-rozwiazania-bi/mozliwosci-szacowania-wartosci-informacji-ex-ante-a-funkcje-informacji-w-organizacji.html [dostęp: 15.06.2021 r.].
[91] Zob. tabela 3.
[92] Zob. Z. Malara, J. Rzęchowski, *Zarządzanie informacją na rynku globalnym. Teoria i praktyka*, Warszawa 2011, s. 22–23.
[93] Zob. M. Deja, A. Rożej, J. Stochaj. J. Stolarski, dz. cyt., s. 14–17.

Tabela 3. Zestawienie wybranych określeń informacji i odpowiadających im funkcji

Autorzy	Określenie informacji	Główne funkcje informacji
Wiener (1961)	Treść zaczerpnięta ze świata zewnętrznego w procesie naszego dostosowywania się do niego i przystosowywania się do niego naszych zmysłów.	Odwzorowanie przeszłości, teraźniejszości i przyszłości. Tworzenie i zmiana rzeczywistości.
Greniewski (1982)	Wiadomość uzyskiwana przez człowieka poprzez obserwację lub czynność umysłową, podlegająca przekazowi w układzie nadawca – odbiorca.	
Gackowski (1977, s. 37)	Właściwości sygnału lub wiadomości polegające na zmniejszaniu nieokreśloności sytuacji lub jej dalszego rozwoju.	
Wierzbicki (1981, s. 9)	Treść zaczerpnięta ze świata zewnętrznego, która zwiększa wiedzę lub zmniejsza niewiedzę decydującego, niepewność i nieokreśloność sytuacji decyzyjnej.	
Lyons (1984, s. 60)	Treść o określonym znaczeniu o czymś, dla kogoś i ze względu na coś, wyrażana za pomocą znaków językowych lub/i pozajęzykowych.	Prezentacja zdarzeń, stanów, rzeczy, obiektów itp. z punktu widzenia przeszłości, teraźniejszości lub przyszłości.
Kasprzak (1971)	Odbicie tego, co istnieje w rozumieniu materialnym (tzw. relacja odbicia), oraz czynnik określający w pewnym stopniu formę (postać) przyszłych rzeczy i zjawisk (tzw. relacja realizacji).	Identyfikacja i antycypacja. Zmniejszanie stopnia nieokreśloności. Określanie stopnia zorganizowania systemów.
Mesner (1971)	Dane o procesach i zjawiskach gospodarczych, wykorzystywane w procesie podejmowania decyzji.	Identyfikacja i rozwiązywanie problemów.

Źródło: J. Czekaj, *Metody zarządzania informacją w przedsiębiorstwie,* Kraków 2000, s. 17.

Zajmujący się ekonomiką informacji Józef Oleński wskazuje, że w każdym systemie społeczno-gospodarczym można wyspecyfikować cztery funkcje informacji:

– informacyjną, polegającą na odwzorowaniu rzeczywistości w formie informacji i tworzeniu zasobów wiedzy (efektywne spełnianie tej funkcji wymaga dobrego rozpoznania zasobów wiedzy użytkownika

informacji oraz jego potrzeb informacyjnych, identyfikacji języka użytkownika oraz identyfikacji homogenicznych zbiorów użytkowników);
– decyzyjną, polegającą na dostarczeniu decydentom informacji niezbędnych do podejmowania decyzji;
– sterującą, polegającą na wywoływaniu określonych zachowań;
– konsumpcyjną – polegająca na funkcjonowaniu informacji jako dobra konsumpcyjnego wytwarzanego na potrzeby rynku[94].

Zgodnie z stanowiskiem prezentowanym przez S. Wojciechowską-Filipek informacji można przypisać następujący zestaw funkcji:
– informacyjną, obejmującą dostarczenie informacji na dany temat;
– decyzyjną, polegającą na dostarczaniu decydentom informacji niezbędnych do rozstrzygnięć władczych;
– sterującą, przejawiającą się wywoływaniem określonych zachowań u odbiorców informacji;
– konsumpcyjną, przejawiającą się w tym, że informację można na różny sposób zużywać (konsumować) i zbywać;
– kulturotwórczą, obejmującą przekazywanie informacji między ludźmi, co jest jednym z istotnych składników rozwoju kulturowego społeczeństw;
– demokratyzującą, realizowaną poprzez szeroki dostęp obywateli do informacji poszerzający i umacniający zakres faktycznego realizowania przez nich roli suwerena;
– składnika wiedzy, wiążącą się z tym, że informacja jest jednym z podstawowych elementów tworzenia i modyfikowania wiedzy[95].

B. Stefanowicz wskazuje na następujące funkcje: informacyjną, sterującą, łagodnej siły, budulca wiedzy, kulturotwórczą, integracyjną, dezintegracyjną, demokratyzującą, opiniotwórczą, wychowawczą, atrybutu władzy, zasobu, kapitału, towaru, motywacyjną. Charakteryzując bliżej te funkcje, warto podkreślić, że:
– funkcja informacyjna jest związana z tym, że każda informacja prezentuje opis pewnego wycinka rzeczywistości, przedstawia jego stan i dostarcza określonych wiadomości go dotyczących;
– funkcja sterująca informacji wiąże się z tym, że każde działanie poprzedza podjęcie decyzji. Jego istotą jest dokonywanie świadomych

[94] Zob. J. Oleński, *Ekonomika informacji*, Warszawa 2001, s. 34.
[95] Zob. S. Wojciechowska-Filipek, dz. cyt., s. 30.

wyborów. Aby były one świadome i poprawne, muszą być oparte na odpowiednich informacjach;
– funkcję „łagodnej siły" należy wiązać z tym, że informacja jest specyficznym czynnikiem, w którym kryje się pewna siła. Nie jest to energia oddziałująca na człowieka w sensie fizycznym, lecz czynnik wpływający na jego postawę, decyzje i działania poprzez oddziaływanie na umysł;
– funkcja informacji jako budulca wiedzy przejawia się w tym, że informacja pozwala kreować, powiększać oraz modyfikować istniejące zasoby wiedzy;
– funkcja kulturotwórcza wiąże się z tym, że informacja pozwala budować nowe elementy kultury duchowej, w szczególności nowe pojęcia i terminy wzbogacające język, którym porozumiewają się członkowie danych społeczności. Informacja jest także nośnikiem pozwalającym przekazywać wiedzę o kulturze w czasie i przestrzeni, dzięki czemu możliwe jest poznawanie dorobku kulturowego wcześniejszych pokoleń;
– funkcja integracyjna polega na tym, że w kontaktach społecznych informacja stanowi spoiwo łączące jednostki z otoczeniem. Człowiek jako istota społeczna dobrowolnie poszukuje kontaktów z innymi ludźmi i m.in. na podstawie wymienianych informacji kształtuje różne rodzaje wspólnot;
– funkcja dezintegrująca realizowana jest przede wszystkim poprzez upowszechnianie informacji stygmatyzującej, fałszującej rzeczywistość, zawierającej treści poniżające, nawołującej do wrogości czy eksponującej podziały poglądów w celu wywołania polaryzacji postaw;
– funkcja demokratyzująca wiąże się z tym, że dzięki swobodzie dostępu do informacji i jawności życia publicznego społeczeństwo może kontrolować przebieg zdarzeń oraz wyrażać swoje opinie. Istotne jest także to, że jednym z warunków funkcjonowania demokracji jest poddawanie władzy ocenie. Do takiej oceny potrzebna jest pełna i wiarygodna informacja o podejmowanych przez władzę działaniach;
– funkcja opiniotwórcza wiąże się z tym, że to w oparciu o informację każdy człowiek tworzy indywidualny obraz oraz oceny otaczającej go rzeczywistości. Co istotne, wspomniana funkcja realizowana jest zarówno w odniesieniu do zdarzeń z przeszłości, jak i przyszłości;
– funkcja wychowawcza przejawia się w tym, że informacja wpływa na kształtowanie osobowości człowieka. Jej odbiór i analiza pobudza do

odpowiedniej reakcji, zmusza także do wyboru celu działania oraz sposobu jego osiągnięcia;
- funkcja atrybutu władzy materializuje się poprzez to, że informacja służy do sprawnego decydowania, a więc także sprawowania władzy. Ze sprawowaniem władzy wiąże się prawo do posiadania i gromadzenia informacji w zakresie, jakiego nie mają podmioty będące przedmiotem oddziaływań władczych;
- funkcja zasobu przejawia się w tym, że informacje tworzą zasoby, mające swoją wartość i wymagające poniesienia kosztów na ich pozyskanie. Mogą być one wykorzystywane do osiągnięcia określonych celów przez posiadacza (dysponenta) informacji;
- funkcja kapitału wiąże się z tym, że informacja jest elementem składowym kapitału rozumianego jako ogół rzeczy, ludzi, środków finansowych i innych czynników materialno-technicznych i psychospołecznych;
- funkcja towaru wiąże się z tym, że informacja jest przedmiotem wymiany i ma swoją cenę;
- funkcja motywacyjna przejawia się w tym, że ludzie i organizacje na bazie informacji definiują cele działania, formułują pożądane ich wyniki, oceniają, czy będą one użyteczne, a nabywając przeświadczenia, że wyniki te są osiągalne, przystępują do działania na rzecz ich uzyskania[96].

W zbliżony sposób funkcje informacji ujął Tomasz R. Aleksandrowicz, wymieniając:
- funkcję modelowania, opisu (informacja to opis rzeczywistości, pokazujący złożoność i różnorodność danej rzeczywistości);
- funkcję decyzyjną (informacja służy jako bodziec do podejmowania działań oraz osiągania celów);
- funkcję sterującą (informacja stanowi podstawę planowania i podejmowania decyzji);
- funkcję rozwoju wiedzy;
- funkcję kapitałotwórczą;
- funkcję konsumpcyjną (informacja jest traktowana jako towar);
- funkcję kulturotwórczą[97].

[96] Zob. B. Stefanowicz, *Informacja,* Warszawa 2004, s. 65–81.
[97] T.R. Aleksandrowicz, *Bezpieczeństwo informacyjne państwa*, „Studia Politologiczne" 2018, nr 49, s. 38.

Tabela 4. Przegląd funkcji informacji w organizacjach

Funkcje informacji	Istota funkcji
Powiadamiająca	Informacja uzupełnia wiedzę o rzeczywistości – obiektach, zdarzeniach i procesach.
Decyzyjna	Informacja pomaga w podejmowaniu trafnych i przydatnych decyzji. Kluczową aktywnością informacyjną jest przetwarzanie i analiza informacji w celu redukcji niepewności.
Sterująca	Informacja kształtuje zachowania odbiorców w taki sposób, by ich działania były jak najbardziej dostosowane do zaprojektowanych celów.
Komunikacyjna	Informacja umożliwia komunikowanie pracowników i kierownictwa, nawiązywanie kontaktów z otoczeniem.
Wspieranie zmian	Informacja przybliża i ułatwia zrozumienie potrzeb i logiki wprowadzanych zmian w procesach zarządzania organizacją.
Integrująca	Informacja łączy ludzi i instrumenty ich aktywności. Umożliwia funkcjonowanie organizacji jako pewnej spójnej całości tworzących ją elementów.
Kulturotwórcza	Informacja przenosi wzorce zachowań, założenia i wartości wspólne dla określonej zbiorowości.
Zasób strategiczny	Informacja jako zasób niematerialny ma nie mniejszy wpływ na powodzenie organizacji niż zasoby finansowe, materialne i ludzkie.
Stymulacyjna (tworzenie wiedzy)	Informacja jest poddawana procesom tworzenia, organizowania i przetwarzania, by generować nową wiedzę w procesie organizacyjnego uczenia się.
Czynnik przewagi konkurencyjnej	Informacja ułatwia opanowanie pewnych kompetencji, które decydują o sukcesie i przewadze w danej dziedzinie działalności.
Kontrolna	Informacja jest źródłem kontroli procesów i członków organizacji.
Wspieranie relacji z klientami	Informacja daje możliwość uwzględniania opinii, życzeń, a nawet współuczestniczenia klientów w procesach powstawania nowych produktów.
Broń przeciw konkurencji	Informacja może być wykorzystana jako czynnik destabilizujący i destrukcyjny (np. poprzez wprowadzanie w błąd) w odniesieniu do podmiotu, którego dotyczy.
Antycypacyjna	Informacja jest podstawą prognozowania, przygotowywania planów i strategii organizacji.

Źródło: K. Materska, *Informacja w organizacjach społeczeństwa wiedzy*, Warszawa 2007, s. 85.

W zwartej, tabelarycznej formie podstawowy zbiór funkcji informacji w kontekście działalności organizacji przedstawia K. Materska[98]. Biorąc pod uwagę treści poglądów i stanowisk wcześniej zaprezentowanych, można stwierdzić, że współcześnie do najważniejszych funkcji informacji należą:

– funkcja informacyjna, polegająca na odwzorowywaniu rzeczywistości oraz dostarczaniu wiadomości przyczyniających się do budowania i modyfikowania wiedzy;
– funkcja decyzyjna, polegająca na dostarczaniu danych i informacji potrzebnych w procesach podejmowania decyzji;
– funkcja sterująca, polegająca na wywoływaniu określonego zachowania użytkownika informacji;
– funkcja konsumpcyjna, polegająca na używaniu informacji w celu bezpośredniego zaspokajania ludzkich potrzeb.

Obok spełnianych funkcji informacja posiada także określone cechy, które są czynnikiem pomagającym bliżej zrozumieć, czym ona jest. Wspomniane cechy umożliwiają także kategoryzację informacji oraz wpływają na sposób jej wykorzystywania[99].

Ogólne cechy informacji (niematerialność i materialność) wskazuje T.R. Aleksandrowicz, pisząc, że informacja „ma wymiar niematerialny i należy odróżnić ją (jej treść) od nośnika, na którym została utrwalona (np. zapis na papierze czy plik komputerowy), jej źródła bezpośredniego (wypowiedź polityka) czy pośredniego (cytat tej wypowiedzi w mass mediach). Niekiedy informacja może funkcjonować wyłącznie w postaci niematerialnej, choćby jako plotka powtarzana z ust do ust. Możliwa jest także sytuacja, w której informacja ma wymiar wyłącznie materialny – np. nowy procesor komputerowy”[100]. Krzysztof Liderman zwraca uwagę, że informacja jest:

– towarem, i to często mającym znaczenie strategiczne;
– podstawowym elementem procesów biznesowych;
– instrumentem służącym do sterowania procesami wytwórczymi i usługowymi[101].

W internetowej *Encyklopedii zarządzania* można znaleźć następującą listę cech informacji: dostępność, aktualność, rzetelność, kompletność porównywalność, jednoznaczność, przetwarzalność, koszt, szczegółowość,

[98] Zob. tabela 4.
[99] Zob. tabela 4.
[100] T.R. Aleksandrowicz, *Bezpieczeństwo informacyjne*…, s. 35.
[101] Zob. K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 17.

adresowalność, użyteczność, priorytetowość, wartość, poufność, klarowność. W rozwiniętym opisie można je przedstawić następująco:

– dostępność informacji oznacza możliwość uzyskania danej kategorii informacji przez użytkownika;
– aktualność określa, czy informacja dotyczy bieżącego stanu rzeczywistości oraz to, jaki czas minął od zaistnienia stanu (sytuacji) opisywanego przez daną informację;
– rzetelność oznacza, że informacja jest prawdziwa, wszystkie jej elementy znajdują odzwierciedlenie w rzeczywistości, a źródła pochodzenia są wiarygodne;
– kompletność jest określana przez ilościowe różnice między informacją pierwotną a tą otrzymaną przez użytkownika;
– porównywalność oznacza możliwości przeprowadzenia analizy porównawczej w stosunku do innych informacji z różnych okresów;
– jednoznaczność to ograniczenie możliwości różnych interpretacji danej informacji;
– przetwarzalność to zdolność do przekształcania w nowe formy treściowe;
– koszt oznacza wartość wydatków ponoszonych w odniesieniu do określonej informacji (pozyskanie, gromadzenie, przetwarzanie, ochrona itp.);
– szczegółowość to liczba detali, jakie zawiera informacja w stosunku do opisywanego obiektu, zdarzenia czy zjawiska;
– adresowalność ma być rozumiana jako przeznaczenie dla konkretnego odbiorcy i dostosowane do jego indywidualnych potrzeb;
– użyteczność oznacza zdolność do zaspokojenia konkretnych potrzeb użytkownika informacji;
– priorytetowość to cecha nakazująca szczególne traktowanie informacji, np. pod względem wagi, znaczenia, pilności przekazu itp.;
– wartość może mieć charakter materialny lub niematerialny i wiąże się ze znaczeniem danej informacji dla jej posiadacza, użytkownika, wytwórcy;
– poufność oznacza dostępność tylko dla zdefiniowanych grup użytkowników i zablokowanie dostępu dla nieupoważnionych;
– klarowność to jasność i zrozumiałość[102].

[102] Zob. *Encyklopedia zarządzania*, https://mfiles.pl/pl/index.php/Cechy_informacji [dostęp: 16.04.2021 r.].

Kornel B. Wydro oraz Magdalena Olender-Skorek dokonują podziału cechy informacji na:

– fenomenologiczne (uniwersalne względem dowolnych obszarów analizy informacji);
– użytkowe (istotne z punktu widzenia użytkownika);
– ekonomiczne.

Następnie wspomniani autorzy, zaznaczając, że lista cech informacji ma charakter rozbudowany, jako najbardziej rozpoznawalne z nich wskazują:

– niezużywalność (użycie informacji nie powoduje jej zniszczenia, a przy powielaniu i przenoszeniu nie jest ona zużywana);
– możliwość akumulowania w bardzo długim okresie;
– niepełną podzielność;
– niewyczerpywalność;
– nieprzywłaszczalność (replika informacji nie różni się niczym od wzorca i ma tę samą wartość);
– zsubiektywizowaną wartość (ta sama informacja może mieć różne znaczenie dla różnych użytkowników);
– zależność wartości od momentu użycia[103].

Tomasz Galewski w syntetycznej charakterystyce właściwości informacji dokonanej w kontekście analizy barier informacyjnych wskazuje, że:

– konsumpcja informacji nie powoduje jej zużywania się, nie istnieje zatem potrzeba ponownego ubiegania się o informację, którą już mamy, chyba że nastąpiła jej utrata w procesie zapominania;
– użyteczność danej informacji może podlegać dezaktualizacji;
– możliwe jest powielanie informacji teoretycznie nieskończoną ilość razy;
– występuje duże zróżnicowanie informacji – każda kolejna nie stanowi dokładnej kopii poprzedniej;
– informacja ma charakter dobra o charakterze doświadczalnym, trudno jest określić jej wartość przed uzyskaniem do niej dostępu;

[103] Zob. M. Olender-Skorek, K.B. Wydro, *Wartość informacji*, https://www.researchgate.net/publication/266661782_Wartosc_informacji [dostęp: 10.06.2021 r.]. Zob. także: K.B. Wydro, *Badania nad istotą informacji, jej właściwościami i stosowanymi technikami informacyjnymi – próba systematyzacji w obszarze wiedzy o informacji*, Warszawa 2007, s. 40–44, https://docplayer.pl/17644783-Badania-nad-istota-informacji-jej-wlasciwosciami-i-stosowanymi-technikami-informacyjnymi-proba-systematyzacji-w-obszarze-wiedzy-o-informacji.html [dostęp: 10.06.2021 r.].

– dobra informacyjne mogą generować duże koszty ewentualnego przerzucenia się na inne ich rodzaje, rodzi to tzw. efekt zamknięcia, w ramach którego odbiorca pozostaje przy danym produkcie informacyjnym ze względu na przyzwyczajenia, umiejętności, brak chęci do przyswajania nowych informacji[104].

M. Hetmański, analizując kwestie cech informacji, zwraca uwagę na to, że ich wyznaczanie jest możliwe i uzasadnione zarówno na poziomie podstawowym, jak i uzupełniającym. Jednak dodaje, że definiowanie oraz sporządzenie w miarę pełnych ich list w sytuacji wieloznaczności i nieostrości pojęcia „informacja" nie jest proste i nie może zakończyć się pełnym sukcesem, czyli przyjęciem jakiegoś uniwersalnego ich zbioru. Wspomniany autor wyróżnia dwie grupy cech informacji: konstytutywne oraz konsekutywne. Zbiór cech konstytutywnych, czyli tych, bez których nie można mówić o informacji jako takiej (chociaż nie muszą one występować wszystkie razem w każdej definicji czy koncepcji informacji), stanowią:

– cechy rzeczy kształtowanych i/lub przekazywanych („informacyjność");
– cechy stanów rzeczy ukształtowanych, sformowanych czy odwzorowanych („informacja");
– cechy relacji kształtowania, przekazywania („informowanie").

Wymienione trzy cechy konstytutywne, jak podkreśla przywoływany badacz, wyznaczone są na drodze etymologiczno-syntaktycznej w tym znaczeniu, że ich sens wynika z łacińskiego pierwowzoru terminu informacja[105]. Z kolei zbiór właściwości konsekutywnych obejmuje:

– cechy różnicy (ale także podobieństwa) w obrębie rzeczy i zdarzeń;
– cechy prawdopodobieństwa zdarzeń, które łączy się z przekazywaną oraz otrzymywaną informacją w rozumieniu ilościowym;
– cechy redukcji niepewności będącej następstwem wyboru w stosunku do prawdopodobieństwa, jakie charakteryzuje zjawiska informacyjne;
– cechy znaczenia (interpretacji) przypisanej nośnikowi informacji – znakowi lub komunikatowi[106].

Badacze zajmujący się zagadnieniem cech informacji często analizują tę kwestię także w kontekstach jakości. Lista właściwości wpływających na

[104] Zob. T. Galewski, *Psychologiczne bariery informacyjne w społeczeństwie informacyjnym*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Informatica" 2012, nr 29, s. 187–188.
[105] Zob. M. Hetmański, dz. cyt., s. 28–29.
[106] Zob. tamże, s. 39–40.

wspomnianą jakość informacji według J. Stochaj obejmuje: obiektywność, komunikatywność, kompatybilność, kompletność, dostępność, znaczenie, aktualność, prawdziwość, ciągłość, dokładność; szczegółowość, przetwarzalność, niski koszt pozyskania, wiarygodność; przydatność, terminowość, jednoznaczność, niepowtarzalność[107]. Znaczenie cechy jakości dla zaspokajania potrzeb informacyjnych podkreśla również cytowany już wcześniej T. Galewski. Według tego autora na kwestię jakości informacji powinniśmy patrzeć przede wszystkim w ujęciu inherentnym, czyli w kontekście jej odpowiedniości do potrzeb użytkownika, a najważniejsze atrybuty jakościowe informacji to:

- prawdziwość, zawierająca się w poprawnym opisywaniu stanu określonej rzeczywistości;
- aktualność, czyli opisywanie teraźniejszego stanu pewnej rzeczywistości (lub ostatniego możliwego do rozpoznania jej stanu), może to odnosić się do czasu, kiedy informacja jest odbierana, i stanu rzeczywistości, kiedy była tworzona;
- wiarygodność, będąca miarą prawdziwości i aktualności (gdy nie daje się określić wiarygodności informacji wprost, ustala się ją na podstawie wiarygodności jej źródła);
- przyswajalność, charakteryzująca się tym, że odbiorca może ją wykorzystać bez wykonywania dodatkowych operacji przekształcających;
- relewancja, czyli ważność przypisywana informacji przez użytkownika.

Z. Malara i J. Rzęchowski, odnosząc się do wartości rynkowej informacji, wskazują takie cechy, jak:

- wiarygodność, oznaczającą pewne źródło pozyskania, aktualność, dojrzałość, tolerancję błędu informacyjnego i jego naprawialność;
- funkcjonalność, uwzględniającą charakter użytkowy, pomocny w osiąganiu celów i procesów decyzyjnych;
- użyteczność, mierzoną reakcją oddziaływania na rynek i jego uczestników oraz osiągania założonych celów w procesach zarządzania;
- wydajność, określoną przez czas, transmisję, implementację i tworzone nowe zasoby wiedzy, podejmowane później procesy decyzyjne i przewidywalność zmian w otoczeniu;
- uniwersalność, uwzględniającą sposób, czas i metody pojawienia się informacji na rynku, sposób jej ujawnienia, modyfikacje, ochronę

[107] Zob. M. Deja, A. Rożej, J. Stochaj. J. Stolarski, dz. cyt., s. 8.

i określony stopień bezpieczeństwa, jej wartość, dotyczącą obecnych i przyszłych okresów[108].

Do istotnych cech informacji (za Julitą Włodarczyk) można zaliczyć:

– różnorodność;
– zdolność do przenoszenia w czasie i przestrzeni (zarówno w sposób zaplanowany, jak i samorzutny);
– przetwarzalność (transformowanie, zniekształcanie, uzupełnianie, fałszowanie itp.);
– niezużywalność (informacja nie zużywa się w procesach, w których jest wykorzystywana, może być używana wielokrotnie czy symultanicznie, może jednak zostać zapomniana, zdeformowana albo zaginąć czy ulec zniszczeniu wraz z nośnikiem);
– mierzalność (informacja może być mierzona entropią, można ilość informacji ujmować także w jednostkach obliczeniowych, np. w bitach);
– ograniczoną podzielność (złożona informacja może być przekazywana we fragmentach, ale informacja prosta jest niepodzielna);
– redundancję (nadmiarowość – kilkakrotne powtarzanie tych samych wiadomości lub ich części, niekiedy redundancja informacji jest korzystna, ponieważ ułatwia ich odbiór podmiotom o zawężonych zdolnościach percepcyjnych);
– asymetrię (nierównomierny rozkład informacji daje przewagę podmiotom dysponującym określonymi informacjami nad podmiotami, które nią nie dysponują)[109];
– nieprzywłaszczalność (informacja może być doświadczana, ale nie może być posiadana, posiadany może być jedynie jej nośnik);
– użyteczność (zdolność do zaspokajania potrzeb informacyjnych);
– kosztowność (wiążąca się z kosztami finansowymi, osobowymi i czasowymi pozyskiwania, wytwarzania i użytkowania informacji)[110].

Kompleksową próbę zestawienia cech informacji w ujęciu formalnym, merytorycznym oraz kosztowo-efektywnościowym podjęli Ryszard Borowiecki

[108] Zob. Z. Malara, J. Rzęchowski, dz. cyt., s. 25.
[109] Jednym ze sposobów ograniczenia asymetrii informacyjnej i zwiększenia zakresu dostępu może być dostarczanie informacji w formie dobra publicznego przez państwo w ustalonym przez nie zakresie.
[110] Zob. J. Włodarczyk, *Informacja i jej znaczenie dla konsumentów – wybrane aspekty*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2006, nr 38, s. 244–246.

oraz Janusz Czekaj[111] w książce poświęconej zarządzaniu zasobami informacyjnymi w przedsiębiorstwie. Przywoływana już wcześniej S. Wojciechowska-Filipek, analizując przydatność informacji w procesach decyzyjnych, zwraca uwagę na takie cechy, jak:

– dokładność (wiarygodne, solidne odwzorowanie rzeczywistości);
– aktualność (obecność jak najświeższych danych odwzorowujących dany stan lub obiekt);
– kompletność (zawartość optymalnej ilości szczegółów);
– odpowiedniość (przydatność dla odpowiednich podmiotów)[112].

Tabela 5. Zestawienie najczęściej występujących w literaturze cech informacji

Cechy informacji		Opis cechy
I. Cechy formalne		
Agregacja		Poziom syntezy informacji
Jednoznaczność		Polega na stosowaniu jednoznacznego języka oraz precyzyjnym definiowaniu pojęć
Komunikatywność		Ilość pracy niezbędnej do nadania informacji formy umożliwiającej odbiorcy podejmowanie decyzji
Objętość		Wielkość obszaru niezbędnego do zapisania informacji na nośniku
Porównywalność		Możliwość porównania z innymi informacjami
Przyswajalność		Objętość informacji, którą użytkownik jest w stanie przyjąć
Redundantność		Posiadanie przez informacje pewnego nadmiaru, który nie wpływa na wzbogacenie treści
Rozwlekłość		Posiadanie przez informacje dodatkowych, zbędnych treści
II. Cechy motoryczne (treściowe)		
Dotyczące czasu	Aktualność	Zgodność informacji ze stanem rzeczywistym w danym momencie czasu
	Dostępność	Dostęp do informacji w czasie, kiedy informacja jest potrzebna
	Szybkość	Czas dostarczenia informacji od zaistnienia zdarzenia
	Wiek	Czas od wystąpienia zdarzenia, którego obrazem jest informacja, do momentu jej wykorzystania
Dotyczące zdarzenia	Celowość	Cecha czyniąca informację podstawą wyznaczania zamierzeń prowadzących do osiągania celu
	Decyzyjność	Sposób, w jaki informacja wpływa na podejmowane decyzje

[111] Zob. tabela 5.
[112] Zob. S. Wojciechowska-Filipek, dz. cyt., s. 32–33.

	Przydatność	Mierzona zmianą prawdopodobieństwa celu w wyniku posiadania danej informacji
	Sensowność	Ograniczająca różnorodność zachowania się systemu w kierunku jego dostosowania do otoczenia
Dotyczące zakresu	Dokładność	Stopień uwzględnienia szczegółów
	Elastyczność	Zdolność do zaspokajania różnych potrzeb
	Ilość	Ilość informacji zmniejszająca stopień niepewności w procesie decyzyjnym
	Kompletność	Gdy użytkownik nie jest zmuszony do poszukiwania dodatkowych informacji przy podejmowaniu decyzji
	Pełność	Likwidowanie niepewności w procesie podejmowania decyzji
	Precyzyjność	Zastosowanie w informacji jasno zdefiniowanej terminologii
	Prospektywność	Zdolność informacji do przewidywania przebiegu przyszłych zdarzeń
	Retrospektywność	Zdolność do prezentowania informacji zwrotnej o wynikach uprzednio podjętych decyzji
Dotyczące obiektywności	Prawdziwość	Zgodność treści z rzeczywistym przebiegiem opisywanego zdarzenia
	Rzetelność	Brak zniekształceń intencjonalnych w informacji
	Spójność	Brak w informacji treści wzajemne sprzecznych
	Wiarygodność	Brak deformacji w treści informacji
	Wierność	Gdy kopia informacji jest taka sama jak oryginał
	Źródłowość	Pochodzenie informacji z obserwacji bezpośredniej
III. Cechy kosztowo-efektywnościowe		
Wartość		Zmiana cenności decyzji na skutek posiadania informacji
Efektywność		Zdolność do wywołania określonych efektów
Kosztowność		Nakłady pieniężne potrzebne do uzyskania informacji
Opłacalność		Różnica pomiędzy cennością informacji a jej kosztem
Pracochłonność		Nakład pracy potrzebny do uzyskania i wykorzystania informacji

Źródło: R. Borowiecki, J. Czekaj, *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki*, Warszawa 2010, s. 125–126.

W. Babik, uznany badacz z zakresu nauki o informacji, wskazuje na istnienie dwóch zestawów atrybutów informacji: technicznego i informacyjnego. Do pierwszego z nich zalicza objętość oraz nośnik. W zestawie drugim umieszcza:

– prawdziwość, rozumianą jako opisywanie rzeczywistości lub jej elementów w dopuszczalnych granicach błędu;

– aktualność, pojmowaną jako opis obecnego stanu rzeczywistości lub ostatniego możliwego do rozpoznania jej stanu z perspektywy odbiorcy informacji;
– wiarygodność, traktowaną jako konsekwencję wiarygodności źródła informacji;
– pełność;
– przyswajalność, oznaczającą, że informacja jest dostępna dla odbiorcy bez konieczności wykonania dodatkowych operacji przekształcających;
– użyteczność, oznaczającą to, że informacja odpowiada potrzebom odbiorcy[113].

W podsumowaniu należy zaznaczyć, że informacje mogą pełnić szereg licznych i różnorodnych funkcji oraz dysponują cechami, które w zależności od nasilenia ich występowania, kształtu jakościowego oraz spontanicznej czy zaplanowanej konfiguracji wywierają wpływ na pełnione przez te informacje role. Posiadane cechy uzewnętrzniają się także w ramach różnorodnych funkcji informacji. Zarówno funkcje, jak i cechy informacji nie zależą w pełni od informacji jako takiej. W znacznej mierze kształtowane są one bowiem przez wytwórców i użytkowników informacji stosownie do ich potrzeb. Na kształt funkcji i cech informacji wpływają również stosowane przez jej użytkowników systemy organizacyjne i techniczne, w ramach których dokonuje się pozyskiwania, przetwarzania, przesyłania czy przechowywania informacji.

1.4. Informacja jako zasób

Znaczenie, wartość informacji oraz jej rola w funkcjonowaniu różnego typu podmiotów indywidualnych i zbiorowych (organizacji, państw) jest, jak już kilkakrotnie wcześniej wspominano, przedmiotem wielowątkowych dociekań badawczych. Jedną z refleksji badawczych umożliwiających lepsze rozpoznanie i identyfikację znaczenia informacji jest traktowanie jej jako zasobu. W ujęciu leksykalnym zasób to „pewna ilość czegoś nagromadzona w celu wykorzystania w przyszłości; zapas, rezerwa”[114]. W prawie identyczny sposób termin ten definiuje internetowa *Encyklopedia zarządzania*, w której pojęcie zasobu postrzega się jako „ilość czegoś, co zostało zebrane,

[113] Zob. W. Babik, *Środowisko informacyjne człowieka*, [w:] *Nauka o informacji*, W. Babik (red.), Warszawa 2016, s. 66–67.
[114] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/ [dostęp: 20.04.2021 r.].

nagromadzone w celu wykorzystania w przyszłości; to coś, co mamy, zapas, rezerwa”[115]. Zasoby umiejscawia się w ramach czasowych. Gromadzone są one przez dany podmiot w celu ich wykorzystania w działaniach bieżących oraz przyszłych. Definiuje się je również jako rezerwy. Według J. Stochaj zasób to „ilość określonej rzeczy lub poziom zmiennej. Zasoby odnoszą się do konkretnego czasu – jest to ilość danej zmiennej w określonym czasie. Gromadzone są przez jednostki administracyjne w celu ich wykorzystania w bliskiej lub dalszej przyszłości”[116]. Za interesujące należy uznać stanowisko B. Stefanowicza, który uważa, że zasób „to pewna ilość czegoś, co zostało zebrane, nagromadzone w celu wykorzystania w przyszłości. Jest to swego rodzaju rezerwa, zapas. Jest to coś, co może faktycznie lub potencjalnie być wykorzystane przez kogokolwiek, kiedykolwiek, gdziekolwiek i dla jakichkolwiek celów”[117]. Analiza przedstawionych definicji ujawnia, że w wielu przypadkach ich autorzy w sposób nieuzasadniony traktują pojęcie „zasobu” jako synonim „zapasu”. Należy więc podkreślić, że jest to spojrzenie zbyt wąskie i nie oddające w pełni istoty tego pojęcia. W związku z tym uprawnione jest zaproponowanie pojmowania zasobu jako określonego zbioru pozostających w dyspozycji danego podmiotu środków materialnych i niematerialnych, którymi on rozporządza zarówno w zakresie bieżącej działalności, jak i potrzeb perspektywicznych (wydzielając czy oznaczając stosownie do potrzeb zasoby rezerwowe albo awaryjne). Jeżeli zanalizować znaczenie pojęcia „zasoby informacyjne”, to autorzy przywoływanej wcześniej *Encyklopedii zarządzania* uważają, że jest to „pewna ilość informacji znajdująca się w posiadaniu firmy i jej pracowników, wykorzystywana do pracy oraz podejmowania strategicznych decyzji”[118]. Z kolei Adam Stabryła prezentuje pogląd, że „zasoby informacyjne to wszelkie będące w dyspozycji danego podmiotu zbiory wiadomości”[119].

Jacek Unold podkreśla, że „zasoby informacyjne stanowią zbiór danych przeznaczonych do przetwarzania oraz zbiór informacji dla decydentów odpowiednich poziomów zarządzania”[120]. Agnieszka Pawłowska wskazuje, że zasobami informacyjnymi „są wszelkie dane, informacje oraz techniki

[115] *Encyklopedia zarządzania*, https://mfiles.pl/pl/index.php/Zas%C3%B3b [dostęp: 21.04.2021 r.].
[116] M. Deja, A. Rożej, J. Stochaj, J. Stolarski, dz. cyt., s. 18.
[117] B. Stefanowicz, *Informacja…*, s. 78.
[118] *Encyklopedia zarządzania*, https://mfiles.pl/pl/index.php/Zas%C3%B3b [dostęp: 21.04.2021 r.].
[119] A. Stabryła, *Podstawy zarządzania firmą*, Warszawa 1995, s. 240.
[120] J. Unold, *Systemy informacyjne marketingu*, Wrocław 2009, s. 81.

informacyjne, które mają wymierną wartość i które mogą być użyte do produkcji określonego dobra lub usługi”[121]. S. Wojciechowska-Filipek uważa z kolei, że informacja to zasób niezbędny do funkcjonowania oraz rozwoju gospodarki i społeczeństwa. Tworzą go wszelkie zbiory informacji zgromadzone oraz przechowywane w danym miejscu i czasie przy użyciu technologii oraz organizacji umożliwiających ich wykorzystanie przez dysponujące nimi podmioty[122]. Tadeusz Gospodarek, pisząc o całościowo rozumianym zasobie informacyjnym, stwierdza, że tworzą go „wirtualne zasoby informacyjne, operacyjne zasoby informacyjne oraz ludzkie zasoby informacyjne związane z operacjami na informacjach i wspomagające podejmowanie decyzji w układzie ekonomicznym”[123]. Warto przywołać także prawne określenie zasobu informacyjnego, które odnaleźć można w Ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej. Zgodnie z artykułem 9a przywoływanej ustawy zasób informacyjny to informacje publiczne o szczególnym znaczeniu dla rozwoju innowacyjności w państwie i rozwoju społeczeństwa informacyjnego, które ze względu na sposób przechowywania i udostępniania pozwalają na ich ponowne wykorzystywanie w sposób użyteczny i efektywny[124]. Wspomniana już wcześniej J. Stochaj w swoich rozważaniach na temat przepływu informacji i zasobów w jednostkach administracyjnych podkreśla, że zasoby informacyjne należą do tych najważniejszych (obok zasobów ludzkich, finansowych oraz rzeczowych) i stanowią „właściwości obiektów, które służą podejmowaniu decyzji w jednostkach administracyjnych. Do zasobów informacyjnych zalicza się także dane, które pozyskuje się zarówno z otoczenia zewnętrznego, jak i z samej jednostki”[125]. Korzystając z przedstawionych przykładów opisu i charakterystyki tego, czym jest zasób (zasoby) informacyjny, można przyjąć, że zasoby informacyjne to będące w posiadaniu bądź dyspozycji danego podmiotu zbiory danych i informacji zgromadzonych i przetwarzanych w systemach informacyjnych oraz umysłach ludzkich, mające wymierną wartość i przydatność do celów działania danego podmiotu. Odnosząc się do czynników kształtujących wartość zasobów informacyjnych, cytowana już wcześniej

[121] A. Pawłowska, *Zasoby informacyjne w administracji publicznej w Polsce. Problemy zarządzania*, Lublin 2002, s. 76.
[122] Zob. S. Wojciechowska-Filipek, dz. cyt., s. 22.
[123] T. Gospodarek, *Elastyczność zasobu informacyjnego*, [w:] *Elastyczność organizacji*, R. Krupski (red.), Wrocław 2008, s. 131.
[124] Zob. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, Dz.U. 2019, poz. 1429.
[125] M. Deja, A. Rożej, J. Stochaj, J Stolarski, dz. cyt., s. 22.

J. Stochaj wskazuje na ich jakość i aktualność[126]. Jeżeli badamy klasyfikację zasobów informacyjnych, to J. Oleński wyróżnia następujące ich rodzaje: wiedzę ogólną, kwalifikacje zawodowe, infrastrukturalne zbiory informacji, infrastrukturalne systemy informacyjne państwa i organizacji ponadpaństwowych, zasoby informacyjne podmiotów społecznych i gospodarczych, zasoby informacyjne podmiotów tworzących sektor informacyjny gospodarki narodowej[127]. Z. Malara i J. Rzęchowski przy zastosowaniu kryterium źródeł pochodzenia wyszczególniają następujące kategorie zasobów informacyjnych:

– zasoby ogólnodostępne zewnętrzne, składające się z informacji pozyskiwanej z aktów prawnych, radia, telewizji, prasy, Internetu, ogłoszeń, raportów, reklam, książek, informacji zdobywanej podczas konferencji i rozmów;
– zasoby ogólnodostępne wewnętrzne, wytwarzane przez poszczególne podmioty w ramach ich działalności na potrzeby własne, ale bez ograniczeń w zakresie ich rozpowszechniania;
– zasoby wewnętrzne niedostępne powszechnie, obejmujące informacje o różnym stopniu tajności (poufności), wykorzystywane do działalności danego podmiotu, np. strategie działania, innowacyjne projekty, analizy rynkowe itp.[128]

Jedną z bardziej kompleksowych, a jednocześnie syntetycznych klasyfikacji zasobów informacyjnych przedstawia cytowany już T. Gospodarek. Wymieniony badacz wskazuje na istnienie trzech rodzajów zasobów informacyjnych: wirtualnego, operacyjnego i ludzkiego. Wirtualny zasób informacyjny stanowią wszystkie informacje składające się na wiedzę i mądrość układu organizacyjnego w danym czasie, nadające się do wykorzystania w procesach realizowanych przez ten układ. Wspomniany zasób można podzielić na: wewnętrzny, będący własnością intelektualną układu (wiedza, sposób organizacji), oraz zewnętrzny, udostępniony układowi do wykorzystania (sygnały lub informacje). Operacyjny zasób informacyjny to wszystkie systemy i urządzenia techniczne, oprogramowanie, technologie zapisu, przetwarzania, transmisji danych umożliwiające automatyzację operacji na informacjach w danym układzie. Operacyjny zasób informacyjny składa się z:

– lokalnego systemu informatycznego (hardware, software systemowe, sieć LAN);

[126] Zob. tamże.
[127] J. Oleński, *Elementy ekonomiki informacji*, Warszawa 2000, s. 161.
[128] Zob. Z. Malara, J. Rzęchowski, dz. cyt., s. 21–22.

– systemu łączności (telekom, Internet, sieć WAN, inne systemy dzierżawione);
– systemów wymiany danych (protokoły, procedury, standardy);
– systemów ochrony danych (procedury, protokoły, zabezpieczenia dostępu);
– systemów zabezpieczeń przed awariami (hardware i software);
– systemów zabezpieczeń przez atakami z zewnątrz (hardware, software, procedury).

Ludzki zasób informacyjny to wszystkie osoby związane z operacjami na informacjach w układzie odpowiadające za utrzymanie całego zasobu informacyjnego w stanie gotowości do użycia oraz osoby decydujące o wykorzystaniu go w procesach realizowanych przez ten układ. Inaczej mówiąc, ludzki zasób informacyjny to wydzielona grupa z zasobu osobowego układu związana z: serwisem sprzętowym i telekomunikacyjnym, programowaniem i serwisem software, zarządzaniem wiedzą i informacją, twórczością, programowaniem i instruowaniem oraz podejmowaniem decyzji z użyciem zasobu informacyjnego[129]. Zasoby informacyjne – jak stwierdza Dorothy E. Denning – mają wartość wymienną i operacyjną. Wartość wymienna uzależniona jest od wartości rynkowej i jest wymierna (jest to cena, jaką nabywca gotów jest zapłacić za dany zasób). Wartość operacyjną określają natomiast pożytki możliwe do uzyskania dzięki korzystaniu z zasobów informacyjnych. Jednak w większości przypadków trudno jest w jednostkach pieniężnych określić wartość wymiernych korzyści w odniesieniu do danych zasobów informacyjnych. Wynika to m.in. z tego, że ich wartość dla zainteresowanych stron może być bardzo różna. Generalnie jednak, jak wskazuje wspomniana D.E. Denning, dla zainteresowanego podmiotu stanowi ona funkcję sześciu czynników: jego poglądów i zobowiązań, możliwości, dostępności danego zasobu dla niego i dla innych oraz integralności zasobu i czasu. Najważniejsze są poglądy i zobowiązania, które przyczyniają się do działań i procesów mających znaczenie dla danego zainteresowanego zasobem podmiotu. Na możliwości składa się wiedza, umiejętności i narzędzia. Dostępność jest miarą możliwości wykorzystania zasobu w sposób właściwy i ma związek z tajnością i poufnością. Chodzi o to, czy zasoby można obejrzeć, przetwarzać, zmieniać, kopiować, rozprowadzać lub sprzedawać, gdyż ich wartość pozostaje w prostej zależności od dostępności dla zainteresowanych. W przypadku integralności

[129] T. Gospodarek, dz. cyt., s. 131–132.

chodzi o to, czy zasoby stanowią całość, czy są dobre, dokładne, kompletne, prawdziwe i wiarygodne. Jeżeli analizujemy czynnik czasu, to istotny jest fakt, że wartość zasobu może z upływem czasu zarówno maleć, jak i wzrastać. W ocenie zasobów informacyjnych należy uwzględniać także ich wartość rzeczywistą oraz potencjalną[130].

B. Stefanowicz, charakteryzując zasoby informacyjne, zauważa, że:

– mają one swoją wartość, ale wymagają także ponoszenia określonych kosztów w trakcie pozyskiwania;
– mogą być używane do osiągania założonych celów;
– bywają obiektem kradzieży;
– są niewyczerpywalne[131].

Dla bardzo wielu podmiotów zasoby informacyjne to zasoby o charakterze strategicznym. Zgodnie z definicją Mirosława Rajzera zasoby strategiczne „to zasoby umożliwiające osiąganie korzyści w długim okresie, od których zależy funkcjonowanie przedsiębiorstwa i które nie są w sposób doskonały zastępowalne”[132]. Podobne stanowisko prezentuje Rafał Krupski, wskazując, że na miano strategicznych zasługują te zasoby, które są:

– wartościowe dla danego podmiotu w obszarze jego działań na rzecz wykorzystywania szans i unikania zagrożeń;
– rzadkie w kontekście posiadania ich przez konkurentów;
– trudne do skopiowania;
– nie do zastąpienia (brak jest ich ekwiwalentnych substytutów)[133].

Według propozycji Marka Kunasza zasób strategiczny charakteryzują takie właściwości, jak:

– trwałość (odzwierciedlająca odporność na deprecjonujący wpływ czasu);
– trudność w zakresie imitacji (odzwierciedlająca stopień niemożności skopiowania danego zasobu);
– niedoskonała substytucyjność (niemożność zastąpienia przez inny zasób o zbliżonych cechach);
– możliwość kupna (przywłaszczenia);
– własność (oznaczająca pozostawanie we władaniu danego podmiotu)[134].

---

[130] Tamże, s. 25–28.
[131] Zob. B. Stefanowicz, *Informacja…*, s. 78.
[132] M. Razjer, *Strategie dywersyfikacji przedsiębiorstw*, Warszawa 2001, s. 191.
[133] Zob. R. Krupski, *Cechy zasobów strategicznych. Teoria i badania empiryczne,* „Prace Naukowe Wałbrzyskiej Wyższej Szkoły Zarządzania i Przedsiębiorczości” 2014, t. 29 (4), s. 6.
[134] Zob. M. Kunasz, *Zasoby przedsiębiorstwa w teorii ekonomii*, „Gospodarka Narodowa” 2006, nr 10, s. 39.

Wartą przywołania klasyfikację cech zasobów strategicznych sporządził również Mariusz Bratnicki. Według tego autora jako strategiczny powinniśmy postrzegać zasób: „cenny, rzadki, kosztowny do naśladowania, trwały, posiadany przez firmę, niepodatny na substytucję, lepszy od posiadanych przez konkurentów, skodyfikowany, uosabiany przez uczestników tworzenia strategii, podatny organizacyjnie na wykorzystanie, ważny”[135]. Uogólniając przedstawione stanowiska, można przyjąć, że zasób strategiczny danego podmiotu to zbiór elementów materialnych i niematerialnych (w tym także zespołów ludzkich), który zarówno w działalności bieżącej, jak i prospektywnej zapewnia temu podmiotowi podstawy stabilności i osiąganie sukcesów w obszarze wykorzystywania szans i unikania zagrożeń. Zasadnicze cechy takiego zasobu to:

– posiadanie wyróżniających (rzadkich) cech użytkowych;
– brak (lub bardzo ograniczone) możliwości skopiowania;
– brak jego ekwiwalentnych substytutów.

Opierając się na rozważaniach Katarzyny Materskiej[136], należy stwierdzić, że nie każdy zgromadzony, przechowywany, wykorzystywany przez dany podmiot zbiór informacji stanowi zasób strategiczny. Informacje tworzące zasób strategiczny, jak sygnalizuje wspomniana badaczka, powinny:

– rozszerzać posiadaną wiedzę o rzeczywistości;
– skutecznie wspierać procesy zmian;
– umożliwiać i usprawniać komunikowanie się;
– umożliwiać podejmowanie optymalnych decyzji;
– usprawniać nawiązywanie relacji z otoczeniem;
– tworzyć przewagę nad konkurentami (rywalami).

Generalizując, trzeba podkreślić, że zasób informacyjny, aby mógł być uznany za strategiczny, musi charakteryzować się szeregiem specyficznych cech. Ich szczegółowy katalog określają i dopasowują do swoich potrzeb podmioty tworzące zasoby informacyjne i nimi zarządzające. Należy pamiętać, że posiadanie zasobów informacyjnych generuje określone koszty, które muszą zostać poniesione, jeżeli zainteresowany podmiot chce dysponować zasobami

[135] M. Bratnicki, *Kompetencje przedsiębiorstwa. Od określenia kompetencji do zbudowania strategii*, Warszawa 2000, s. 62.
[136] Zob. K. Materska, *Rozwój koncepcji, informacji i wiedzy jako zasobu organizacji,* https://www.academia.edu/2269216/Rozw%C3%B3j_koncepcji_informacji_i_wiedzy_jako_zasobu_organizacji?auto=download [dostęp: 25.04.2020 r.].

o adekwatnym do jego potrzeb rozmiarze i jakości. Podstawowa lista tych kosztów dotyczy:

– pozyskiwania i uzupełniania (modyfikacji) zasobów;
– przetwarzania zasobów na wiedzę;
– przechowywania i utrzymywania zasobów w sposób umożliwiający niczym niezakłócone korzystanie z nich;
– zarządzania zasobami;
– ochrony zasobów.

Reasumując przedstawione analizy, można stwierdzić, że zasoby informacyjne, sytuujące się w grupie zasobów odnawialnych, przez wiele podmiotów są traktowane nie tylko jako wysoce użyteczne, ale coraz częściej jako zasoby strategiczne. Zasoby informacyjne, podobnie jak i inne zasoby, mają swoją wartość, ale wymagają również ponoszenia kosztów na ich pozyskiwanie, utrzymanie i efektywną eksploatację. Mogą być one wykorzystywane do skutecznego osiągania różnorodnych i skomplikowanych celów. Warunkiem podstawowym jest jednak odpowiednie ich kształtowanie oraz zarządzanie, co – zważywszy na specyfikę informacji tworzącej rdzeń tych zasobów – nie jest zadaniem łatwym. Podkreślenia wymaga również to, że zarządzanie zasobami informacyjnymi zaliczanymi do zasobów strategicznych wymaga przemyślanego sterowania określonymi procesami, w szczególności zaś tymi, które dotyczą:

– pozyskiwania odpowiednich (tak pod względem ilości, jak i jakości) informacji;
– gromadzenia, przechowywania i ochrony informacji;
– alokacji i dystrybucji informacji;
– przetwarzania i eksploatacji informacji.

Jest to zadanie o wysokim stopniu złożoności, albowiem zasoby informacyjne zalicza się do aktywów, które są zmienne co do wartości w zależności od czasu i otoczenia. W odniesieniu do tych zasobów (w tym także mających strategiczny charakter) tworzyć należy strategie informacyjne, synchronizujące działania ich posiadaczy w zakresie postępowania z tymi zasobami. W szczególności dotyczyć powinny one zarządzania informacją, kształtowania systemów informacyjnych oraz używanych technologii. Każdy zasób informacyjny posiadany przez dany podmiot powinien być chroniony (strategiczny zasób informacyjny w szczególności). Poziom ochrony powinien pozostawać w odpowiednich proporcjach zarówno w stosunku do poziomu zagrożeń, jak i znaczenia zasobu. Ochrona zasobów informacyjnych powinna

uwzględniać realne i potencjalne zagrożenia wewnętrzne i zewnętrzne. W związku z tym musi obejmować szerokie spektrum przedsięwzięć dotyczących wszystkich procesów związanych z tworzeniem, użytkowaniem, modyfikowaniem, transferem, wyłączeniem z użycia (czasowym lub trwałym) lub likwidacją danego zasobu informacyjnego. Ponieważ jednym z podstawowych wyznaczników wartości zasobów informacyjnych jest ich funkcjonalność i użyteczność, to ich ochrona musi być skuteczna, ale nie może ograniczać wspomnianej funkcjonalności i użyteczności. Jednocześnie zasoby informacyjne podmiotu nie mogą zostać roztrwonione i poddane degradacji, np. wskutek utraty aktualności, co w praktycznym działaniu wymaga sformułowania i realizowania odpowiedniej polityki gospodarowania tym zasobami.

2. Społeczeństwo informacyjne

2.1. Geneza i pojęcie społeczeństwa informacyjnego

Termin „społeczeństwo informacyjne" (jap. *johoka shakai* – społeczeństwo komunikujące się przez komputery) do obiegu naukowego wprowadził japoński antropolog Tadao Umesao[137], publikując w 1963 roku artykuł o ewolucyjnej teorii społeczeństwa opartego na przetwarzaniu informacji. Do popularyzacji tego pojęcia przyczynił się również japoński teoretyk mediów Kenichi Koyama, używając go w książce *Introduction to Information Theory* (*Wprowadzenie do teorii informacji*), która ukazała się w 1968 roku. Nie można pominąć także zasług kolejnego badacza z Japonii, Yoneji Masudy[138], który dokonał analizy i opisu zmian zachodzących w obrębie społeczeństwa opartego na sektorze informacji oraz telekomunikacji i w 1980 roku przedstawił wyniki swych dociekań w dziele *The Information Society as Post-Industrial Society*

[137] Tadao Umesao (1920–2010), japoński antropolog. Przez dziesięciolecia pracował jako profesor na Uniwersytecie w Kioto. Współzałożyciel i dyrektor Narodowego Muzeum Etnologii w Osace. W opracowaniu *Teoria przemysłu informacyjnego. Świt nadchodzącej ery przemysłu ektodermalnego* opublikowanym w 1963 r. stwierdził, że po erze agrarnej i wieku przemysłowym nadchodzi czas powstania wokół branży informacyjnej nowego społeczeństwa. Jeden z jego koronnych argumentów za takim rozwojem sytuacji opierał się na tezie, że wraz z rozwojem środków masowego przekazu i komputerów informacja stanie się ważnym czynnikiem ekonomicznym.

[138] Yoneji Masuda (1905–1995), japoński socjolog, którego pomysły na temat informacji i komunikacji wywarły znaczący wpływ na konceptualizację idei społeczeństwa informacyjnego. Jako jeden z jej pionierów bywa często nazywany „ojcem społeczeństwa informacyjnego". Jego działalność zawodowa wywarła zasadniczy wpływ na określenie strategicznych kierunków rozwoju japońskiego społeczeństwa technologicznego. We współpracy z Komitetem Komputeryzacji Y. Masuda nakreślił narodowy plan utworzenia społeczeństwa informacyjnego do 2000 roku. Była to strategia, która zakładała stworzenie pierwszego na świecie społeczeństwa informacyjnego na bazie informatyzacji Japonii oraz rozwijania społeczeństwa opartego na wiedzy.

(*Społeczeństwo informacyjne jako społeczeństwo postindustrialne*). W Europie problematyką społeczeństwa informacyjnego jako jedni z pierwszych zainteresowali się francuscy socjologowie Alain Minc i Simon Nora, którzy zawarli swoje uwagi na ten temat w przekazanym w 1978 r. prezydentowi Francji Giscardowi d'Estaing raporcie zatytułowanym *L'informatisation de la societé*. Chociaż pojawienie się pojęcia „społeczeństwo informacyjne" można lokować w latach sześćdziesiątych XX wieku, to aż do połowy lat 90. funkcjonowało ono przede wszystkim w środowiskach naukowych. W publicznym użyciu termin ten zaczyna pojawiać się w roku 1993, a w następnych latach jest już powszechnie stosowany w wielu dokumentach i opracowaniach.

Szczególnie wybitne zasługi w dziedzinie rozwoju społeczeństwa informacyjnego w Europie należy przypisać Martinowi Bangemannowi[139]. W latach 1993–99 był on komisarzem Unii Europejskiej ds. Polityki Przemysłowej, Technologii Informatycznych i Telekomunikacji, a w grudniu 1993 r. stanął na czele grupy roboczej, której zadaniem było przygotowanie ekspertyzy mającej wskazać, jakie działania należy podjąć, aby móc budować społeczeństwo informacyjne na obszarze UE[140]. Efektem prac wspomnianego zespołu ekspertów był raport zatytułowany *Europa i globalne społeczeństwo informacyjne: zalecenia dla Rady Europy* (*Europe and the Global Information Society: Recommendations to the European Council*). W czerwcu 1994 r. został on przedstawiony Radzie Europejskiej i od tego czasu znany jest jako *Raport Bangemanna*. Autorzy tego opracowania wnioskowali do kierowniczych gremiów UE o podjęcie działań umożliwiających tworzenie nowych, dynamicznie rozwijających się sektorów gospodarki oraz wykonanie odpowiednich przedsięwzięć legislacyjnych na rzecz takiego ujednolicenia przepisów prawnych, aby umożliwić powstanie konkurencyjnego ogólnoeuropejskiego rynku usług informacyjnych. Dokument przygotowany przez zespół M. Bangemanna wskazywał dwie główne sfery, w których należałoby, zdaniem jego autorów, rozpocząć budowę

[139] Martin Bangemann, niemiecki polityk (ur. 1934), który w latach 1985–1988 był szefem Wolnej Partii Demokratycznej (FDP). Od 1973 do 1984 w różnych rolach zasiadał w Parlamencie Europejskim (m.in. w latach 1976–1979 był wiceprzewodniczącym, a od 1979 do 1984 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.

[140] Należy zaznaczyć, że rok przed opublikowaniem *Raportu Bangemanna* Komisja Europejska przedstawiła dokument o nazwie *Biała Księga wzrostu, konkurencyjności, zatrudnienia. Wyzwanie i droga do XXI wieku*, w którym po raz pierwszy pojawiła się europejska wizja społeczeństwa informacyjnego.

europejskiego społeczeństwa informacyjnego. Pierwsza to rozwijanie świadomości społecznej, ze szczególnym naciskiem na sektor małych i średnich przedsiębiorstw, administrację państwową oraz młode pokolenie obywateli UE. Druga 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. Autorzy raportu zaproponowali również podjęcie intensywnych działań na rzecz 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[141]. We wspomnianym dokumencie podkreślono, że infrastruktury informacyjne są tworami bez granic w środowisku otwartego rynku, w związku z czym społeczeństwo informacyjne posiada globalne rozmiary[142]. W odpowiedzi na przywoływany raport UE zainicjowała kolejne prace eksperckie ukierunkowane 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. Generalnie przełomowość *Raportu Bangemana* polegała na tym, że:

- upowszechnił on na gruncie europejskim pojęcie społeczeństwa informacyjnego;
- spowodował, że problematyka społeczeństwa informacyjnego stała się obszarem zainteresowania kierowniczych gremiów UE i jej państw członkowskich;
- uchwycił podstawowe wyzwania stojące przed Europą w związku z gwałtownym rozwojem technologii informacyjnych;
- sformułował propozycje dotyczące działań UE na rzecz sprostania pojawiającym się wyzwaniom i spożytkowania tworzącego się społeczeństwa

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

[142] Zob. J. Małkowski, *Społeczeństwo informacyjne w Unii Europejskiej,* s. 9, https://alebank.pl/wp-content/uploads/2010/04/eds.2008.k4.007-013.pdf [dostęp: 20.04.2020 r.].

informacyjnego dla przyspieszenia wzrostu gospodarczego i rozwoju cywilizacyjnego[143].

Należy pamiętać, że ideą społeczeństwa informacyjnego dość wcześnie zainteresowano się także w Stanach Zjednoczonych. Jak zauważa Katarzyna Garwol, pojawienie się w 1965 roku Intelsatu – pierwszego systemu komunikacyjnego o zasięgu globalnym – wywołało ożywioną dyskusję nad kwestiami wykorzystywania nowoczesnej techniki dla dobra ogólnospołecznego. W rezultacie w latach 70. XX wieku w USA podjęto prace legislacyjne i organizacyjne mające na celu upowszechnienie idei społeczeństwa informacyjnego[144]. Ważnym efektem tej dyskusji było opublikowanie w 1979 roku przez Narodową Akademię Nauki USA raportu, w którym sygnalizowano nadejście nowej cywilizacji informacyjnej, opartej na rozwoju techniki cyfrowej[145]. Administracja amerykańska przygotowała także zmiany w systemie prawnym i podatkowym oraz ograniczyła interwencję publiczną w zakresie budowy społeczeństwa informacyjnego. W konsekwencji za jego rozwój odpowiadać zaczął biznes i nauka. Dopiero w 1993 roku, za rządów prezydenta Billa Clintona opublikowano dokument zatytułowany *Narodowa infrastruktura informacyjna* (*National Information Infrastructure*). W opracowaniu tym nakreślona została amerykańska koncepcja budowy narodowej infrastruktury sieci informacyjnych (infostrad), wskazano w nim także na konieczność zapewnienia powszechnego i komercyjnego dostępu do nowoczesnych technologii. Newralgiczne znaczenie dla rozwoju społeczeństwa informacyjnego w USA miał ogłoszony w 1997 r. raport *Struktura światowej elektronicznej gospodarki*, wytyczający główne kierunki i obszary działania w tej sferze. Po podpisaniu tego dokumentu przez prezydenta B. Clintona zyskał on rangę dokumentu państwowego, a hasła Globalnej Infrastruktury Informacyjnej oraz Globalnej Elektronicznej Gospodarki stały się immanentnymi składnikami amerykańskiej strategii rozwoju[146]. Jak wskazuje Paweł A. Nowak, w rezultacie tych działań w 2006 roku ponad połowa ze stu amerykańskich firm o największym kapitale działała w obszarze

[143] Zob. W. Fehler, *Społeczeństwo informacyjne jako składnik procesu globalizacji*, [w:] *Problemy polityki bezpieczeństwa wobec procesów globalizacji*, J. Świniarski, J. Tymanowski (red.), Toruń 2003, s. 26.
[144] Zob. K. Garwol, *Droga do powstania społeczeństwa informacyjnego we współczesnych demokracjach*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2010, nr 57, s. 104–105.
[145] Zob. M. Kęsy, *Społeczeństwo informacyjne w rozwoju cywilizacyjnym ludzkości*, „Dydaktyka Informatyki" 2011, nr 6, s. 79.
[146] Zob. W. Fehler, *Społeczeństwo informacyjne*…, s. 27.

telekomunikacji oraz informatyki. Kolejne ekipy administracji amerykańskiej konsekwentnie propagowały i wspierały zasadę rozwijania społeczeństwa informacyjnego w USA, traktując je jako motor postępu i źródło korzyści ekonomicznych oraz instrument umacniania przywództwa technicznego w świecie zachodnim. Potwierdza to światowy rynek technologii informacyjno-komunikacyjnych i jego amerykańscy liderzy, tacy jak Microsoft, IBM, Apple, HP, Oracle, Google czy Facebook[147].

Przyjęte przez Stany Zjednoczone kierunki działania stanowiły nowe wyzwanie dla państw UE. Dostrzegając konieczność stworzenia gospodarki będącej w stanie konkurować z USA, podjęły one wysiłki na rzecz dalszego rozwoju społeczeństwa informacyjnego. W ich ramach w marcu 2000 roku przyjęto strategię lizbońską, której dalekosiężnym celem było uzyskanie do 2010 r. przez gospodarkę UE statusu najbardziej konkurencyjnej gospodarki na świecie. Jako jeden z kluczowych instrumentów do osiągnięcia tego zamierzenia strategia wskazywała dalszy dynamiczny rozwój społeczeństwa informacyjnego. Priorytet ten znalazł swoje odzwierciedlenia w planie działania (*action plans*) *e-Europe 2002 – Społeczeństwo informacyjne dla wszystkich*. W ramach zawartych w tym dokumencie ustaleń państwa członkowskie zobowiązały się do:

– wprowadzenia obywateli Europy, szkół, przedsiębiorstw i administracji publicznej w erę cywilizacji informacyjnej;
– wspierania rozwoju nowych technologii informacyjnych;
– polepszenia jakości życia oraz organizacji społeczeństwa i gospodarki.

Dążąc do osiągnięcia wskazanych powyżej celów, Komisja Europejska określiła dziesięć priorytetowych obszarów działania, obejmujących:

– szerokie wprowadzenie Internetu i urządzeń multimedialnych do procesów edukacyjnych;
– obniżenie kosztów dostępu do Internetu;
– intensyfikację działań w sferze e-gospodarki;
– budowę i udostępnienie szybkich łącz internetowych dla potrzeb badaczy i studentów;
– stworzenie europejskiej infrastruktury dla szerokiego korzystania z kart elektronicznych w różnego rodzaju aplikacjach;

[147] Zob. P.A. Nowak, *Rozwój społeczeństwa informacyjnego na świecie*, https://si.lodzkie.pl/rozwoj-spoleczenstwa-informacyjnego-na-swiecie/ [dostęp: 12.04.2020 r.].

– zbudowanie rozwiązań umożliwiających korzystanie z rozwoju społeczeństwa informacyjnego przez niepełnosprawnych;
– wykorzystanie nowych technik w dziedzinie transportu;
– zapewnienie warunków do finansowania innowacyjnych projektów w dziedzinie technologii informatycznych;
– zwiększenie wysiłków na rzecz upowszechnienia usług sieciowych w służbie zdrowia;
– zapewnienie skutecznych narzędzi dostępu do informacji sektora publicznego oraz umożliwienie wzajemnego przepływu informacji między sektorami władzy[148].

W 2005 roku oceniono, że tempo wdrażania strategii lizbońskiej jest niewystarczające i w związku z tym dokonano jej odnowienia poprzez redefinicję celów. Jednym z efektów tych zabiegów był kolejny plan działania *e-Europe 2005*, który koncentrował się na możliwościach wykorzystania sieci telekomunikacyjnych przez sektor publiczny, rozbudowie sieci teleinformatycznych w celu przeciwdziałaniu wykluczeniu cyfrowemu oraz upowszechnianiu szeroko rozumianych e-usług. Kolejny etap przyspieszania tego procesu stanowiła strategia sektorowa *i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia*.

Jednocześnie rozpoczęto prace nad strategią długookresową. W dokumencie *Europa 2020 – Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu* zaznaczono, że strategia ta powinna umożliwić UE osiągnięcie wzrostu:

– inteligentnego (dzięki rozwojowi wiedzy i innowacji);
– trwałego (opartego na ekologicznej, efektywnej w zarządzaniu zasobami oraz bardziej konkurencyjnej gospodarce);
– spójnego (dzięki przyrostowi zatrudnienia oraz zwiększeniu spójności społecznej i terytorialnej)[149].

W ramach wspomnianej strategii budowa społeczeństwa informacyjnego w Europie nie została określona jako samoistny cel, lecz wpisano ją w siedem projektów przewodnich:

– *Unia innowacji* – (poprawa warunków ramowych i dostępu do finansowania badań i innowacji);

[148] Zob. W. Fehler, *Społeczeństwo informacyjne*..., s. 27–28.
[149] Zob. Komunikat (KOM (2010), 2020 wersja ostateczna) – *Europa 2020: Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu*, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=LEGISSUM:em0028 [dostęp: 14.04.2020 r.].

– *Młodzież w drodze* (polepszenie rezultatów systemów kształcenia oraz ułatwienie wkraczania młodzieży na rynek pracy);
– *Europejska agenda cyfrowa* (upowszechnienie szybkiego Internetu oraz umożliwienie korzystania z dobrodziejstw jednolitego rynku cyfrowego gospodarstwom domowym i przedsiębiorstwom);
– *Europa efektywnie korzystająca z zasobów* (uwolnienie kwestii wzrostu gospodarczego od wykorzystania zasobów poprzez rozwój gospodarki niskoemisyjnej, szerokie korzystanie z odnawialnych źródeł energii, modernizację transportu oraz zwiększenie efektywności energetycznej);
– *Polityka przemysłowa w erze globalizacji* (poprawa otoczenia biznesu, wspieranie rozwoju bazy przemysłowej zdolnej do konkurowania na rynkach światowych);
– *Program na rzecz nowych umiejętności i zatrudnienia* (modernizacja rynków pracy, poprawa pozycji pracobiorców na drodze permanentnego podnoszenia kwalifikacji, zwiększenie współczynnika aktywności zawodowej i lepsze dopasowanie popytu do podaży na rynku pracy, także dzięki zwiększonej mobilności siły roboczej);
– *Europejski program walki z ubóstwem* (zapewnienie spójności społecznej i terytorialnej tak, aby pożytki ze wzrostu gospodarczego i zatrudnienia były szeroko dostępne, a osoby ubogie i wykluczone społecznie miały zapewnione aktywne i godne uczestnictwo w życiu społecznym)[150].

19 maja 2010 roku Komisja Europejska ogłosiła jako pierwszą z tych przewodnich inicjatyw *Europejską agendę cyfrową*. Agenda ta przyjęła za cel zagwarantowanie sprawiedliwego, otwartego i bezpiecznego jednolitego rynku cyfrowego, opartego na zapewnieniu konsumentom i przedsiębiorcom łatwiejszego dostępu do towarów i usług cyfrowych w całej Europie, stworzeniu warunków do rozwoju sieci i usług cyfrowych oraz maksymalizacji wzrostu gospodarczego związanego z gospodarką cyfrową[151]. Reasumując, można stwierdzić, że konsekwentny rozwój społeczeństwa informacyjnego jest trwale zakotwiczony w świadomości administracji Unii Europejskiej i stanowi jeden z kluczowych obszarów jej działań. Należy w tym kontekście zauważyć, że w połowie lutego 2020 Komisja Europejska pod przewodnictwem

[150] Tamże.
[151] Zob. *Europejska agenda cyfrowa*, https://www.europarl.europa.eu/factsheets/pl/sheet/64/europejska-agenda-cyfrowa [dostęp: 14.04.2020 r.].

Ursuli von der Leyen ogłosiła nową strategię *Europa na miarę ery cyfrowej*. Główne cele tej strategii to:

- takie ukształtowanie przepisów w zakresie ochrony danych, aby zapewniły one wszystkim możliwość kontroli danych osobowych i jednocześnie pomagały przedsiębiorcom;
- zapewnienie ochrony danych osobowych obywateli UE także przez państwa spoza Unii;
- łatwiejszy dostęp konsumentów i przedsiębiorstw do towarów sprzedawanych przez Internet;
- sprawnie funkcjonujący rynek zakupów i sprzedaży na równych zasadach dla wszystkich;
- opracowywanie zasad odpowiadających tempu rozwoju technologicznego i wspierających rozwój infrastruktury;
- zagwarantowanie, aby europejska gospodarka, przemysł i zatrudnienie w pełni czerpały korzyści z możliwości stwarzanych przez cyfryzację;
- dążenie do stanu, w którym UE będzie wzorem społeczeństwa, któremu dane zapewniają większe możliwości[152].

Licząca już prawie 60 lat historia społeczeństwa informacyjnego obfituje w liczne próby zdefiniowania jej istoty, choć brak jest definicji powszechnie akceptowanej. W *Vademecum bezpieczeństwa informacyjnego* społeczeństwo informacyjne jest przedstawiane jako „społeczeństwo, w którym kluczowym elementem działalności społeczno-ekonomicznej i zmian jest informacja i w którym dzięki rozwojowi technologicznemu możliwe jest generowanie informacji, jej gromadzenie, przetwarzanie oraz przechowywanie bez względu na odległość, czas i wielkość, co przeobraża istotnie sposób życia i pracy ludzi”[153]. W stanowisku przyjętym na kongresie informatyków polskich w grudniu 1994 r. określono społeczeństwo informacyjne jako „społeczeństwo charakteryzujące się przygotowaniem i zdolnością do użytkowania systemów informatycznych, skomputeryzowane i wykorzystujące usługi telekomunikacji do przesyłania i zdalnego przetwarzania informacji”[154]. Według Piotra Sienkiewicza społeczeństwo informacyjne to „system społeczny, ukształtowany

[152] *Europa na miarę ery cyfrowej. Zapewnienie ludziom dostępu do technologii najnowszej generacji*, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_pl# policy-areas [dostęp: 10.11.2020 r.].
[153] O. Wasiuta, R. Klepka, dz. cyt., t. 2, s. 380.
[154] Raport I Kongresu Informatyki Polskiej, Poznań 1994, cyt. za: J.S. Nowak, *Społeczeństwo informacyjne – geneza i definicje*, [w:] *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*, P. Sienkiewicz, J.S. Nowak (red.), Katowice 2008, s. 25.

w procesie informacji, w którym systemy informacyjne i zasoby informacyjne determinują społeczną strukturę zatrudnienia, wzrost zamożności społeczeństwa (dochodu narodowego) oraz stanowią podstawę orientacji cywilizacyjnej"[155]. W ujęciu 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"[156]. 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"[157]. W zakończeniu przeglądu definicji jako jedną z celniejszych można przywołać tę autorstwa Tomasza Gobana-Klasa, zgodnie z którą „społeczeństwo informacyjne to społeczeństwo, które nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz środki te są podstawą tworzenia dochodu narodowego i dostarczają źródła utrzymania większości społeczeństwa"[158]. Generalizując, można uznać, że społeczeństwo informacyjne tworzą następujące substraty:

– techniczny, obejmujący informacyjną infrastrukturę techniczną rozumianą jako całość urządzeń służących gromadzeniu, przetwarzaniu, przechowywaniu i udostępnianiu informacji oraz powiązań procesowych, w tym kanałów przesyłania danych łączonych w rozmaite konfiguracje;

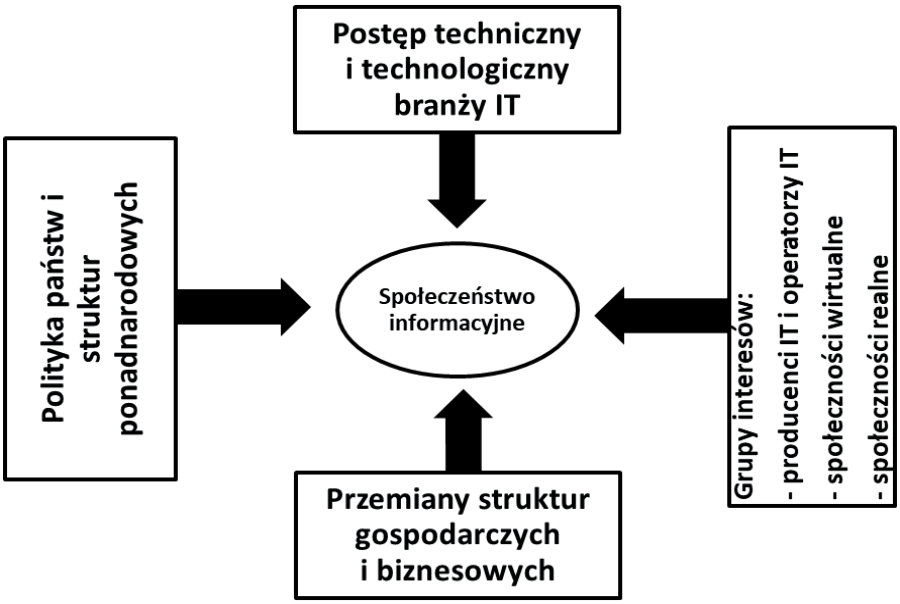
[155] P. Sienkiewicz, *Teorie rozwoju społeczeństwa informacyjnego*, [w:] *Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego. Dylematy cywilizacyjno-kulturowe*, L.H. Haber (red.), Kraków 2002, s. 506–507.

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

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

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

– ekonomiczny, obejmujący informacyjny wymiar gospodarki, czyli te gałęzie produkcji i usług, które bazują na informacji i technikach informacyjnych oraz zajmują się wytwarzaniem informacji, a także ich dystrybucją;
– społeczny, obejmujący osoby korzystające w szerokim zakresie w działalności zawodowej, edukacyjnej oraz codziennej egzystencji z technologii informacyjnych i możliwości z nimi związanych;
– kulturowy, obejmujący kulturę informacyjną rozumianą jako określony stopień akceptacji informacji jako zasobu utylitarnego o charakterze strategicznym, a także odpowiedni poziom umiejętności w zakresie korzystania i wytwarzania informacji, w tym opanowanie umiejętności związanych z obsługą urządzeń informatycznych.



Rysunek 5. Główne siły kształtujące społeczeństwo informacyjne
Źródło: M. Goliński, *Społeczeństwo informacyjne: problemy definicyjne i problemy pomiaru*, „Dydaktyka Informatyki" 2004, nr 1, s. 46.

Konkludując, należy podkreślić (co pokazują powyższe rozważania), że sporządzenie mającej cechy uniwersalności definicji pojęcia „społeczeństwo informacyjne" jest bardzo trudne. Niemniej jednak, sprowadzając do wspólnego mianownika najczęściej powtarzające się elementy dostępnych ujęć charakteryzujących istotę tego społeczeństwa, takie jak nowoczesne formy

komunikowania się, powszechna komputeryzacja, wykorzystanie technologii informatycznych i telekomunikacyjnych do uzyskiwania, gromadzenia, analizowania i przekazywania informacji, szybki przyrost ilości i znaczenia wiedzy oraz wysoki stopień zaawansowania technologicznego opartej na tej wiedzy gospodarki, rozbudowana sieć teleinformatyczna, można sformułować pogląd, że społeczeństwo informacyjne to typ formacji społeczno-gospodarczej ukształtowanej na bazie rozwoju nowoczesnych technologii teleinformatycznych, dysponującej rozbudowanymi i wysokowydajnymi środkami przetwarzania informacji i komunikowania, będącymi zasadniczą podstawą wytwarzania dochodu narodowego i dostarczającymi środków utrzymania dużej części społeczeństwa. Jednym z podstawowych wyróżników społeczeństwa informacyjnego jest rozbudowana nowoczesna sieć teleinformatyczna i telekomunikacyjna oraz obszerne i szeroko dostępne różnego rodzaju publiczne zasoby informacyjne.

2.2. Cechy i funkcje społeczeństwa informacyjnego

Społeczeństwo informacyjne przejawia wiele cech tradycyjnych społeczeństw, ale ma też wiele cech nowych. W encyklopedii politologii wskazuje się na pięć płaszczyzn różniących społeczeństwo informacyjne od społeczeństwa industrialnego:

- ekonomiczną, którą charakteryzuje odejście od gospodarki opartej na przemyśle w kierunku gospodarki bazującej na usługach;
- ról zawodowych, przejawiającą się w dominacji inżynierów, specjalistów, ekspertów, naukowców;
- orientacji technicznej, przejawiającą się w sterowaniu rozwojem technicznym i jego planowaniu;
- procesów decyzyjnych zdominowanych przez „technologie intelektualne" (systemy wspomagania decyzji) i decydowanie sieciowe;
- ewaluatywną, związaną z kluczowym znaczeniem wiedzy teoretycznej jako źródła innowacji[159].

Jak wskazuje Tomasz Goban-Klas, jako jeden z pierwszych wykaz cech społeczeństwa informacyjnego sporządził Daniel Bell, wymieniając wśród nich:

[159] *Encyklopedia politologii. Pojęcia, teorie i metody*, M. Żmigrodzki, M. Sokół (red.), t. 1, Warszawa 2016, s. 631–632.

– centralne znaczenie wiedzy teoretycznej jako źródła polityki i innowacji;
– dominację specjalistów i naukowców w strukturze zawodowej społeczeństwa;
– dominację sektora usług w gospodarce;
– rozwój sektora czwartego (finanse, ubezpieczenia itd.) oraz sektora piątego (zdrowie, nauka, oświata);
– zorientowania na społeczną kontrolę rozwoju techniki;
– podejmowanie decyzji politycznych i społecznych poprzez tworzenie technologii intelektualnych[160].

Z kolei Maria Nowina-Konopka zwraca uwagę w szczególności na takie właściwości społeczeństwa informacyjnego, jak:

– wytwarzanie informacji (masowość wytwarzania, masowe zapotrzebowanie oraz masowy sposób wykorzystywania informacji);
– przechowywanie informacji (możliwości nieograniczonego gromadzenia i magazynowania informacji);
– przekazywanie informacji (przekaz informacji bez barier czasowych i przestrzennych);
– pobieranie informacji (możliwość odebrania zamieszczanych w Internecie informacji przez wszystkich zainteresowanych);
– wykorzystywanie informacji (masowe, otwarte, nieograniczone korzystanie z Internetu jako źródła informacji)[161].

Piotr Gutowski z kolei opisuje społeczeństwo informacyjne jako:

– „społeczeństwo pracujące w konkurencyjnej gospodarce opartej na wiedzy, której trzon stanowią usługi;
– społeczeństwo zdolne do samofinansowania się i do wprowadzania innowacji;
– społeczeństwo wykorzystujące techniki informacyjne, mające wysoko rozwiniętą świadomość informatyczną, informacyjną i technologiczną;
– społeczeństwo zdolne do łatwego przekwalifikowania się;
– społeczeństwo, w którym dużą rolę odgrywają naukowcy i specjaliści wysokiej klasy;
– społeczeństwo równych szans (niezależnie od miejsca zamieszkania

[160] Zob. T. Goban-Klas, *Media i komunikowanie masowe: teorie analizy prasy, radia, telewizji i Internetu*, Warszawa 2005, s. 290.
[161] Zob. M. Nowina-Konopka, *Istota i rozwój społeczeństwa informacyjnego,* [w:] *Społeczeństwo informacyjne, istota, rozwój, wyzwania*, M. Witkowska, K. Cholawo-Sosnowska (red.), Warszawa 2006, s. 20–21.

obywatele mający takie same szanse na zdobywanie wiedzy – e-learning czy pracę – telepraca)”[162].

Aneta Kisiel wśród cech społeczeństwa informacyjnego wyróżnia:

– dużą szybkość przepływu informacji;
– możliwość podejmowania wymiany informacji w dowolnym czasie i miejscu;
– odseparowanie kosztów przesyłania informacji od odległości, na jaką się ją przesyła;
– zwiększenie rangi tzw. technologii intelektualnych (w tym m.in. analiz baz danych) jako podstawy różnorakich procesów decyzyjnych;
– względne ograniczenie ekonomicznej roli własności intelektualnej wskutek łatwości kopiowania oraz bezpłatnej redystrybucji dóbr intelektualnych;
– przyrost nowych form wypowiadania i twórczości;
– wzrost ilości informacji zniekształconych, zmanipulowanych, mających charakter dezinformacyjny, powiązany z brakiem zdolności odbiorców do weryfikacji jakości takich informacji;
– wkraczanie technologii cyfrowych do wielu dziedzin życia, generujące ich uzależnienie od komputerów oraz cyfrowego obiegu informacji[163].

Natomiast Marian Kęsy do wyróżniających cech społeczeństwa informacyjnego zalicza:

– posiadanie rozwiniętych i wydajnych środków wytwarzania, przetwarzania, przechowywania i przekazywania informacji;
– wysoką rangę technologii informacyjnej w odniesieniu do funkcjonowania firm, zatrudnienia i utrzymania jednostek oraz ich duży wpływ na budżety państwowe i domowe;
– wywieranie przez technologie informacyjne wpływu na poziom wskaźników rozwoju gospodarczego[164].

Stosunkowo najbardziej kompletną listę cech współczesnego społeczeństwa informacyjnego przedstawił Marian Golka, który wskazał w jej ramach na:

– wzrost znaczenia wiedzy teoretycznej jako źródła innowacji;

---

[162] P. Gutowski, *Podstawowe cechy, funkcje i determinanty kreujące społeczeństwo informacyjne w nowoczesnej gospodarce*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług” 2009, nr 46, s. 98.

[163] Zob. A. Kisiel, *Społeczeństwo informacyjne – wybrane przykłady szans i zagrożeń*, „Studies & Proceedings of Polish Association for Knowledge Management” 2011, t. 51, s. 119.

[164] M. Kęsy, *Społeczeństwo informacyjne w rozwoju…*, s. 76.

– zwiększającą się rangę technologii intelektualnych (w tym analiz baz danych) jako narzędzia wspierającego podejmowanie decyzji;
– dużą dyfuzyjność technologii informacyjnych oraz szybki transfer informacji powodujący kompresję czasu i przestrzeni;
– możliwość ciągłej, całodobowej wymiany i korzystania z informacji (bez uwzględniania stref czasowych i powiązania kosztów transmisji informacji z parametrem odległości);
– zwiększenie różnorodności sposobów wypowiadania się i twórczej ekspresji oraz pojawienie się tzw. rzeczywistości wirtualnej;
– szeroki dostęp do podstawowych usług informatycznych;
– pojawienie się nadmiaru informacji, zwiększające się możliwości manipulacji informacyjnej oraz dezinformacji, deficyty w zakresie selekcji i weryfikacji informacji;
– postępujący odwrót od przetwarzania informacji w umysłach ludzi na rzecz ich przetwarzania w komputerach;
– konieczność ciągłego dokształcania się w zakresie obsługi urządzeń cyfrowych związana z ich systematycznym doskonaleniem oraz przenikaniem technologii cyfrowych do niemal wszystkich dziedzin życia;
– zmiany w morfologii życia społecznego obejmujące m.in. wytwarzanie się nowych podziałów społecznych i nowych struktur społecznych;
– przemiany w komunikacji międzyludzkiej, zmiany w zakresie relacji społecznych oraz zacieranie granic rozdzielających sferą prywatną od publicznej[165].

Jeżeli chodzi o funkcje realizowane przez społeczeństwo informacyjne, to za przywoływaną już wcześniej M. Nowiną-Konopką można wymienić:

– funkcję edukacyjną (realizowaną w ramach globalnego upowszechniania wiedzy naukowej oraz uświadamiania wagi i znaczenia podnoszenia kwalifikacji);
– funkcję komunikacyjną (materializująca się w postaci budowy nowych płaszczyzn nawiązywania więzi społecznych);
– funkcję socjalizacyjną i aktywizacyjną (realizowaną w aspekcie inkluzji osób obciążonych ograniczeniami w zakresie możliwości swobodnego funkcjonowania w życiu społecznym czy zawodowym);

[165] Zob. M. Golka, *Czym jest społeczeństwo informacyjne?*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2005, nr 4, s. 258–260.

– funkcję partycypacyjną (związaną z tworzeniem warunków do prowadzenia debat publicznych oraz wykorzystaniem sieci do innych form aktywności politycznej, np. wyborczej);
– funkcję organizatorską (obejmującą tworzenie warunków dla rozwoju konkurencyjności na rynku teleinformatycznym oraz umożliwienie pełnego funkcjonowania w jego obrębie wszystkich grup społecznych);
– funkcję ochronno-kontrolną (mającą na celu ochronę obywateli i instytucji państwowych przed przestępczością informacyjną oraz budowę i nadzorowanie przejrzystych standardów funkcjonowania społeczeństwa informacyjnego)[166].

W nieco bardziej rozbudowanym kształcie, przedstawionym przez Piotra Gutowskiego, społeczeństwo informacyjne spełnia następujące funkcje:
– edukacyjną (związaną z możliwościami prowadzenia różnych form kształcenia i nauczania na odległość);
– komunikacyjną (realizowaną dzięki możliwości porozumiewania się i przekazywania informacji w dowolny sposób, w dowolnym czasie i z dowolnego miejsca przy zastosowaniu różnych urządzeń i technik);
– socjalizacyjną (dotycząca umożliwiania podtrzymywania, nawiązywania i zacieśniania relacji międzyosobniczych);
– aktywizującą (związaną z wyłączaniem do aktywnego życia w sposób dostosowany do ich stanu zdrowia osób niepełnosprawnych, schorowanych i starszych);
– partycypacyjną (umożliwiającą prowadzenie różnych debat publicznych, uczestniczenie w życiu politycznym, w tym także poprzez głosowanie za pomocą Internetu);
– organizatorską (tworzenie poprzez odpowiednie działania polityczne, ekonomiczne i prawne warunków prorozwojowych opartych na walorach społeczeństwa informacyjnego);
– ochronną i kontrolną (wiążącą się z możliwościami oddziaływania na różne sfery bezpieczeństwa)[167].

Analizując funkcje społeczeństwa informacyjnego, należy podkreślić, że powstanie i rozwój tej formacji społeczno-ekonomicznej przyniósł i niesie ze sobą wiele pozytywnych zmian w różnych sferach.

[166] Zob. M. Nowina-Konopka, dz. cyt., s. 21–22.
[167] Zob. P. Gutowski, dz. cyt., s. 98–99.

W obszarze ekonomicznym środki i instrumenty dostępne społeczeństwu informacyjnemu przyczyniają się do wzrostu innowacyjności i efektywności gospodarowania, kreowania nowych obszarów działalności gospodarczej, budowania przewagi konkurencyjnej i coraz silniejszych globalnych więzi gospodarczych. W nowej, informacyjnej epoce poprawiło się funkcjonowanie rynków wewnętrznych, ponieważ konkurencja globalna wymusiła prokonsumenckie nastawienie firm, które, nie chcąc tracić klientów, coraz bardziej dbają o jakość i przystępność swoich ofert. Wprawdzie dla producentów w konkurującym świecie otoczenie rynkowe stało się bardziej niepewne, ale motywuje to ich do uzupełniania oferty nie tylko o produkty lepszej jakości, ale również o te zupełnie nowe. Oprócz wzrostu znaczenia konkurencyjności, efektywności i innowacyjności dostrzec należy również postępujące skokowo ułatwienia w dziedzinie komunikacji i współpracy między partnerami gospodarczymi dzięki wykorzystywaniu coraz bardziej wydajnych i przyjaznych technologii informacyjnych i komunikacyjnych. Bardzo wyraźny dodatni wpływ wywarły na sferę ekonomiczną (zwłaszcza na handel i bankowość) rozwiązania z zakresu usług e-commerce i e-banking. Usługi te umożliwiają użytkownikom łatwą i docierająca do szerokiego grona odbiorców prezentację ofert oraz przeprowadzanie w sposób sprawny i nieliczący się z czasem oraz odległościami dużej ilości transakcji. Właściwości społeczeństwa informacyjnego dają także możliwość zwiększenia obszaru i zasięgu działalności gospodarczej bez konieczności fizycznej obecności na nowych rynkach. Ograniczają również, poprzez rozwój kanałów sprawnej wymiany informacji i dóbr materialnych, rolę pośredników. Rozwój społeczeństwa informacyjnego generuje także zwiększenie poziomu wydatków inwestycyjnych w gospodarce, tworzenie nowych miejsc pracy oraz zwiększanie aktywności gospodarczej ludzi. Szczególne znaczenie w tym kontekście odgrywa telepraca, która dla wielu osób, na przykład wychowujących dzieci, oddalonych od dużych ośrodków z miejscami pracy, jest szansą na inkluzję gospodarczą i społeczną.

W aspekcie kulturowym należy wskazać na wzrost możliwości pozyskiwania informacji i zdobywania wiedzy umożliwiającej lepsze poznanie innych kultur. Ważne jest również, w ramach procesu dyfuzji kulturowej, kształtowanie pozytywnych zachowań i preferencji w oparciu o łatwy dostęp do wartościowych treści i przesłań aksjologiczno-poznawczych zawartych w różnych formach twórczości artystycznej (np. literatura, film, malarstwo, muzyka). Rozwój i upowszechnianie technik komunikowania zdecydowanie

wzmacnia potencjał relacyjności i poszerza pola doświadczeń współczesnego człowieka. Przykładem w tej materii jest chociażby powstawanie grup społecznych skupionych wokół portali społecznościowych i forów internetowych. Wirtualne społeczności umożliwiają także dzielenie się opiniami poprzez blogi czy skrzynki e-mail na temat wydarzeń kulturalnych czy propagowanie wiedzy z zakresu szeroko rozumianej kultury. Ważnym aspektem oddziaływania społeczeństwa informacyjnego w sferze kulturowej są także zwiększające się możliwości wspierania i udzielania pomocy dla różnych form twórczości (w tym także tej o charakterze amatorskim). Dzięki dostępności względnie tanich, lecz zaawansowanych technicznie urządzeń możliwy jest np. rozwój twórczości filmowej, dziennikarskiej czy wydawniczej.

W sferze ekologicznej społeczeństwo informacyjne stwarza warunki do redukcji negatywnego wpływu antropopresji na środowisko naturalne poprzez ograniczanie szkodliwych emisji, nadmiernego zużycia energii i zmniejszanie ilości przytłaczających form infrastruktury. Na przykład stosowanie elektronicznych czujników i odbiorników wraz z systemem przesyłu danych pozwala monitorować zużycie energii i regulować je stosownie do rzeczywistych potrzeb. Zamiana szeregów procesów fizycznych na wirtualne daje możliwość ograniczenia zużycia wielu dóbr oraz stwarza (np. dzięki zastosowaniu systemów monitorujących) lepsze możliwości zarządzania ochroną środowiska naturalnego i współpracy w tej dziedzinie. Dzięki narzędziom społeczeństwa informacyjnego możliwe stało się także wykorzystanie nowych form produkcji, umożliwiających np. redukcję ilości odpadów produkcyjnych, ograniczenie emisji szkodliwych substancji zanieczyszczających powietrze i wodę czy redukowanie ogólnego zużycia surowców. Jest to bardzo ważny element, odgrywający istotną rolę we wdrażaniu idei zrównoważonego rozwoju, której częścią jest organizacja produkcji w duchu sprzyjającym oszczędzaniu dóbr naturalnych (zwłaszcza tych nieodnawialnych). Społeczeństwo informacyjne dokonuje także przełomu w bardzo obciążającym środowisko transporcie drogowym, optymalizując go w różnych jego odmianach. Zintegrowane systemy inteligentnego zarządzania transportem pozwalają nie tylko coraz sprawniej transportować towary i ludzi, ale także ograniczać zatory na drogach oraz emisję spalin w aglomeracjach.

W sferze politycznej dzięki usprawnieniu i szybkości wymiany informacji zwiększa się zakres udziału społeczeństwa w życiu politycznym. Na przykład rozwiązania umożliwiające głosowanie za pośrednictwem sieci w perspektywie mogą podnosić frekwencję wyborczą, a przez to dostarczać

silniejszej legitymizacji rządzącym. Obywatele mogą także na bieżąco opiniować działania władzy politycznej, wyrażając swoje stanowiska np. w różnego rodzaju sondażach czy poprzez zabieranie głosu w mediach społecznościowych. Media te tworzą również możliwość stosunkowo łatwego i skutecznego organizowania się na masową skalę do wyrażania poglądów politycznych oraz wywierania nacisku. Inne pozytywy to poszerzanie prawa do publicznego informowania innych oraz do bycia informowanym, ułatwianie publicznej dyskusji oraz wysuwania i nagłaśniania różnych politycznych inicjatyw. Dla decydentów politycznych szczególnie ważne jest szybkie docieranie do pełniejszych informacji ułatwiających planowanie i podejmowanie decyzji oraz zwiększanie możliwości komunikowania się i oddziaływania informacyjnego na wyborców.

Blisko sfery politycznej mieści się sfera administracyjna państwa i jej sprawność. Jej funkcjonowanie ulega zdecydowanej poprawie m.in. dzięki większej dostępności i efektywności usług z zakresu e-administracji. Obywatele wyposażeni w e-podpisy mogą, zamiast tracić czas w kolejkach i wypełniać formularze w urzędach, wysyłać je z domu i tam czekać na odpowiedzi urzędów. Dzięki nowoczesnym systemom informatycznym wiele czasochłonnych czynności można wykonywać seryjnie lub online, tym samym zwiększając efektywność administracji. Bardzo istotnym walorem, jaki wiąże się z funkcjonowaniem społeczeństwa informacyjnego w sferze administracyjnej, jest możliwość opiniowania działania urzędów poprzez wpisywanie komentarzy na ich stronach oraz ułatwiony dostęp do zbiorów informacji publicznej.

W sferze społecznej, jak już wspominano, upowszechnia się telepraca wykonywana w domu, co umożliwia aktywizowanie zawodowe osób dotychczas mających zablokowany dostęp do rynku pracy. Zatrudnienie w tej formie pozwala również na obniżenie koncentracji ludzi w miejscach pracy, oszczędność czasu przeznaczonego na dojazdy, zmniejszenie zapotrzebowania na pomieszczenia biurowe oraz obciążenia środków transportu. Jego zaletą jest także elastyczność czasu pracy i możność dostosowania go do potrzeb pracownika.

W obszarze społecznym zwrócić trzeba uwagę także na rozwój e-edukacji. Obejmuje ona nie tylko nauczanie na odległość. E-edukacja to także: zdalne wyszukiwanie informacji oraz interaktywność w nauczaniu (osoby uczące się mogą zdobywać wiedzę, będąc w kontakcie z nauczycielem, ale także pracując z programem komputerowym), realizowanie nauczania

w różnym czasie, w różnych formach i miejscach (nauczanie szkolne, domowe, indywidualne), szerokie wsparcie nowoczesnymi formami pomocy naukowych (np. filmy czy programy komputerowe), które uatrakcyjniają i usprawniają proces nauczania.

Rewolucyjne zmiany następują także w zakresie jednego ze ważniejszych obszarów życia społecznego, jakim jest ochrona zdrowia. W społeczeństwie informacyjnym dzięki telemedycynie[168] możliwe stało się monitorowanie stanu zdrowia, prowadzenie konsultacji, dokonywanie diagnostyki, rehabilitacji czy wykonywanie zabiegów chirurgicznych na odległość. Telemedycyna dzięki nowym technologiom pozwala diagnozować i monitorować stan pacjentów w domu. Wyniki są wysyłane bezpośrednio do lekarzy, stawiających na ich podstawie wstępne diagnozy. Telemedycyna umożliwia również rodzinie opiekę nad osobami bliskimi bez konieczności stałego z nimi przebywania. Medycyna na odległość ma zastosowanie także w ratownictwie medycznym, np. przesyłanie danych dzięki systemom teleinformatycznym usprawnia niesienie pomocy poszkodowanym w wypadkach czy katastrofach. Pozytywnie na sferę społeczną wpływa także rozwój e-usług w postaci np. handlu elektronicznego, który pozwala lepiej organizować czas oraz daje dostęp do szeregu dóbr np. osobom niepełnosprawnym, mieszkańcom małych miejscowości oddalonym od centrów handlowych.

Generalnie zapewnienie lepszej edukacji, pracy, dostępu do świadczeń lekarskich czy medycznych, udziału w życiu publicznym jest na pewno pozytywnym skutkiem wdrażania rozwiązań dostępnych w społeczeństwie informacyjnym w sferze społecznej. Narzędzia właściwe dla tego społeczeństwa, w tym przede wszystkim Internet, mają również wpływ na budowanie kapitału społecznego. Budowanie tego kapitału pozwala z kolei na zapobieganie wykluczeniu społecznemu oraz tworzeniu obszarów ubóstwa.

W skompresowanej formie można przedstawić następujące główne zakresy walorów funkcjonowania społeczeństwa informacyjnego:

- przyspieszanie rozwoju kapitału intelektualnego i społecznego dzięki wykorzystaniu technologii informacyjnych i komunikacyjnych;
- realizacja swobodnego dostępu przy pomocy Internetu do globalnych zasobów informacji i wiedzy;

[168] Telemedycyna nazywana bywa również medycyną na odległość, ponieważ umożliwia świadczenie usług medycznych bez względu na bariery przestrzenne. W ramach telemedycyny wykorzystuje się elementy medycyny, informatyki i telekomunikacji.

– wzrost dostępności i efektywności usług publicznych dzięki wykorzystaniu technologii informacyjnych i komunikacyjnych;
– ugruntowanie zasad demokracji oraz poszerzanie zakresu partycypacji społecznej w życiu politycznym;
– przyspieszenie rozwoju nauki oraz tempa badań naukowych poprzez zautomatyzowane wytwarzanie, przetwarzanie, transfer, przechowywanie i wykorzystanie wszelkiego rodzaju wiedzy;
– udostępnianie nowych możliwości w sferze ochrony zdrowia;
– poszerzanie zasięgu i możliwości edukacyjnych;
– zmniejszanie zużycia surowców i energii, a tym samym redukowanie nadmiernej eksploatacji zasobów środowiska oraz ilości szkodliwych emisji zatruwających to środowisko;
– poszerzanie granic wolności i swobody informacyjnej;
– wcielanie prospołecznych zasad zarządzania publicznego;
– obniżenie kosztów działalności gospodarczej, większy zasięg dostęp do rynków, duża dostępność i większy wybór, sprzedaż internetowa;
– powstanie nowych możliwości związanych z zatrudnieniem;
– przełamanie bariery odległości poprzez stworzenie możliwości kontaktowania się ludzi (tak na podłożu prywatnym, jak i zawodowym) niezależnie od miejsca przebywania.

Rekapitulując, można stwierdzić, że funkcjonowanie i rozwój społeczeństwa informacyjnego to zagadnienie o dużym stopniu złożoności i jako takie musi być rozpatrywane interdyscyplinarnie, zarówno na gruncie nauk społecznych, jak i techniczno-ekonomicznych. Społeczeństwa informacyjnego wraz z jego mechanizmami wpływającymi na rozwój oraz bezpieczeństwo jednostek, państw i społeczności międzynarodowych nie powinno się traktować w kategoriach deterministycznych jako nowego, wspaniałego świata. O wiele bardziej racjonalne jest analizowanie tego fenomenu przy jednoczesnym zastosowaniu perspektywy optymistycznej, pesymistycznej i zrównoważonej[169]. Przy zastosowaniu pierwszego, optymistycznego spojrzenia wyłania się obraz społeczeństwa uwalniającego się od przymusu pracy, dysponującego dużą ilością czasu spożytkowywanego na indywidualny rozwój, posiadającego rozbudowujące się sieci komunikacji korzystnie wpływające na homeostazę społeczną. Perspektywa pesymistyczna pokazuje społeczeństwo zdezintegrowane i zindywidualizowane, poddawane coraz bardziej rozległemu

[169] Zob. W. Fehler, *Społeczeństwo informacyjne*…, s. 38.

nadzorowi i kontroli. W wersji zrównoważonej społeczeństwo informacyjne ze zmieniającą się strukturą zatrudnienia oraz coraz bardziej zawansowanymi technologiami we wszystkich sferach życia kształtuje elementy swej struktury społecznej ewolucyjnie, w sposób zachowujący równościowe, demokratyczne i wolnościowe zasady oraz humanistyczną aksjologię.

2.3. Zagrożenia i wyzwania w społeczeństwie informacyjnym

Jedną z istotniejszych kwestii związanych z funkcjonowaniem społeczeństwa informacyjnego są wyzwania i zagrożenia, jakie ono z sobą niesie. Rewolucja informacyjna, która się dokonała, stworzyła szereg nowych możliwości, ale zrodziła także określoną ilość sytuacji trudnych, niepewnych, czyli wyzwań. Istotny obszar funkcjonowania społeczeństwa informacyjnego to także zagrożenia. Sposób, w jaki odczytujemy, interpretujemy oraz podejmujemy wyzwania, a także stosunek do diagnozowania, minimalizowania i oddalania zagrożeń to jeden z ważniejszych (chociaż często niedocenianych) czynników mających wpływ na funkcjonowanie współczesnego społeczeństwa informacyjnego. Należy pamiętać, że obecnie, kiedy wkraczamy w erę sztucznej inteligencji, wszyscy ci, którzy będą posiadali dobre rozeznanie w mechanizmach działania społeczeństwa informacyjnego, uzyskają więcej korzyści i ustalą bezpieczniejsze reguły funkcjonowania jego nowej odmiany z dominacją wspomnianej sztucznej inteligencji. Jak słusznie zauważa Halina Świeboda, nowe technologie, będące podstawą istnienia społeczeństwa informacyjnego, generują zagrożenia ujawniające się w różnych obszarach ludzkiej działalności (ekonomicznej, społecznej, kulturowej, politycznej i in.). Ponadto jesteśmy zarzucani ogromną ilością informacji przy ograniczonych możliwościach ustalenia ich źródeł oraz prawdziwości. Sprzyja to zabiegom manipulacyjnym, które wpływają na postrzeganie otaczających nas struktur[170]. K. Garwol, odnosząc się do zasygnalizowanych powyżej kwestii, zwraca uwagę na fakt, że pojawienie się nowych urządzeń i technologii informacyjnych przyniosło zagrożenie uzależnieniem od komputera i Internetu, poczty e-mailowej

[170] Zob. H. Świeboda, *Percepcja społecznych konsekwencji rozwoju społeczeństwa informacyjnego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2011, nr 67, s. 222.

i krótkich wiadomości tekstowych (SMS), pornografii umieszczonej w sieci, gier komputerowych i technik multimedialnych. Ponadto doprowadziło to do często skrajnego uproszczenia słownictwa i oparcia go na internetowym i SMS-owym slangu. Jeszcze inne zagrożenia, które wskazuje przywoływana autorka, to internetowa przestępczość, choroby (np. wady wzroku czy wady postawy) powodowane wielogodzinnym korzystaniem z komputerów[171]. Inny badacz, Jan Kraft, wskazując na fundamentalne znaczenie nierównego dostępu do technik i technologii informacyjnych, zaznacza, że jest to zjawisko przekładające się na powstawanie nierówności społecznych i społecznego upośledzenia. Wspomniany autor, powołując się m.in. na prace Manuela Castellsa oraz Georga F. Gildera, eksponuje tezę, że brak dostępu do Internetu lub dostęp powierzchowny oznacza marginalizację w globalnym systemie sieciowym. W przedstawionych przez siebie ustaleniach J. Kraft wskazuje, że postępem cieszą się przede wszystkim osoby wykształcone, o wyższym statusie majątkowym, młodsze, mężczyźni i mieszkańcy miast. Ci beneficjenci sukcesu nowych technologii informatycznych tworzą grupy tzw. „digerati"[172]. Osoby pozostające poza tymi grupami są w większym lub w mniejszym stopniu cyfrowo wykluczone. Są one nie tylko pozbawione fizycznego dostępu do najnowszych technik i technologii, ale także nie korzystają w pełni z możliwości, jakie dostęp taki oferuje. To, jak zauważa przywoływany autor, pozwala wskazać na istnienie kilku poziomów wykluczenia:

– w obszarze posiadania dostępu do nowoczesnego sprzętu IT;
– w obszarze umiejętności posługiwania się nowymi technologiami;
– w obszarze korzystania z zasobów Internetu[173].

Mieczysław Lubański, opierając się na ustaleniach badaczy amerykańskich i brytyjskich, wskazuje, że zasadnicze zagrożenia w obrębie społeczeństwa informacyjnego to:

---

[171] Zob. K. Garwol, *Negatywny wpływ technologii teleinformatycznej na obywateli społeczeństwa informacyjnego, wybrane aspekty*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2011, nr 67, s. 246.

[172] Termin ten został użyty po raz pierwszy w styczniu 1992 r. w artykule J. Markoffa *Pools of Memory, Waves of Dispute*, zamieszczonym na łamach „New York Times". Oznacza on nową elitę digitalizacji, mediów społecznościowych, przemysłu komputerowego. Mianem tym są określani także liderzy opinii promujący wizję transformacji społecznej związanej z Internetem i technologiami cyfrowymi.

[173] Zob. J. Kraft, *Jakość dostępu i umiejętności użytkowników – nierozpoznane elementy wykluczenia cyfrowego społeczeństwie informacyjnym*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2009, nr 35, s. 106–107.

– nierówności związane z tworzeniem dwubiegunowego społeczeństwa, składającego się z osób posiadających dostęp do nowych technologii i tych, którzy takiego dostępu nie mają;
– zagrożenia dla prywatności;
– występowanie różnych form nadużyć informacyjnych;
– dezintegrujący wpływ na małe społeczności;
– zwiększone możliwości zagrożeń dla bezpieczeństwa informacyjnego różnych podmiotów;
– prymat technologii przekazu nad jego treścią;
– umacnianie dominacji kultury masowej;
– utrwalanie homogenizacji;
– odchodzenie od wartości związanych z służbą publiczną i odpowiedzialnością społeczną[174].

Z kolei Piotr Sienkiewicz w kontekście szans i zagrożeń dla demokracji w społeczeństwie informacyjnym wymienia: infoterroryzm, kulturę masową, e-dżihad, zwiększone możliwości indoktrynacji, nadmiar informacji, niedobór wiedzy, pokusę autorytaryzmu oraz syndrom orwellowski[175]. Według Anety Kisiel do zagrożeń wynikających z rozwoju społeczeństwa informacyjnego należy przede wszystkim:

– możliwość sprawowania przez władzę totalnej kontroli działań obywateli w sieci;
– brak gwarancji zachowania prywatności i skutecznej ochrony danych osobowych obywateli;
– uzależnianie się w rożnych formach od technologii informacyjnych;
– wyalienowanie społeczne powstające na gruncie ograniczania kontaktów osobistych z innymi ludźmi;
– zawodność infrastruktury IT;
– cyberprzestępczość[176].

Generalizując zagadnienie wyzwań i zagrożeń, można je w oparciu o istniejący dorobek badawczy uporządkować w ramach płaszczyzn: ekonomicznej, społecznej, kulturowej, politycznej, administracyjnej.

---

[174] Zob. M. Lubański, *Społeczeństwo informacyjne a cywilizacja informatyczna*, [w:] *Dylematy cywilizacji informatycznej,* A. Szewczyk (red.), Warszawa 2004, s. 36.
[175] Zob. P. Sienkiewicz, *Zagrożenia dla demokracji w społeczeństwie informacyjnym*, [w:] *Transformacja demokracji*, L.W. Zacher (red.), Warszawa 2011, s. 216.
[176] Zob. A. Kisiel, dz. cyt., s. 122–123.

W ekonomicznej sferze funkcjonowania społeczeństwa informacyjnego kluczowe wyzwania i zagrożenia wiążą się z:

- podatnością zwirtualizowanych rynków na wstrząsy wynikające m.in. z dogodnych warunków do działania kapitału spekulacyjnego, co grozi destabilizacją gospodarki światowej oraz zagraża bezpieczeństwu ekonomicznemu poszczególnych państw;
- bezrobociem generowanym przez rozwój komputeryzacji, automatyzacji i robotyzacji redukującej znaczenie ludzkiej siły roboczej;
- intensywnym rozszerzaniem władzy i zasięgu wpływów wielkich korporacji, które m.in. kreują nadmierną konsumpcję poprzez śledzenie i rozpoznawanie gustów klientów;
- utrwalaniem istniejących nierówności gospodarczych wynikających z ograniczonego dostępu do zdobyczy społeczeństwa informacyjnego części społeczności międzynarodowej;
- zwiększeniem niepewności dla producentów, ponieważ otoczenie rynkowe stanie się coraz bardziej turbulentne w wyniku pojawiania się konkurencyjnych producentów dysponujących najnowocześniejszymi technologiami, mogących nie tylko zaproponować produkty lepszej jakości, ale również zaoferować zupełnie nowe produkty, które zmienią zapotrzebowania klientów tak, że stare produkty i usługi staną się zbędne, co może zagrażać nawet całym gałęziom przemysłów.

Wśród zagrożeń i wyzwań w obszarze społecznym wymienić należy:

- depersonalizowanie więzi międzyludzkich w wyniku masowego przerzucania się na komunikowanie za pomocą środków technicznych;
- zanik postaw altruistycznych;
- instrumentalizację kontaktów interpersonalnych;
- indywidualizację życia społecznego;
- chaos i zagubienie informacyjne wynikające z napływu olbrzymich ilości błahych i bezużytecznych informacji;
- rozwój różnych form manipulacji informacyjnej;
- rozwój różnorodnych form cyberprzestępczości;
- dogodne warunki do rozwoju cyberterroryzmu;
- wyalienowanie społeczne związane z upowszechnianiem się telepracy, nauczania na odległość, elektronicznego handlu;
- uzależnienie wielu dziedzin życia społecznego (udział w życiu publicznym, edukacja, praca, ochrona zdrowia) od stanu infrastruktuy teleinformatycznej, szczególnie zaś od jej zawodności.

W sferze kulturowej wyzwania i zagrożenia wiążą się z:

- naruszaniem na dużą skalę praw autorskich w odniesieniu do różnych form twórczości artystycznej i intelektualnej;
- uzależnianiem się od technologii informacyjnych i związanych z nimi gadżetów;
- masową produkcją i rozpowszechnianiem różnorodnych tandetnych, kiczowatych, grafomańskich dzieł literackich, filmowych, muzycznych i in.;
- narastającą uniformizacją kulturową na skutek zwiększających się ciągle możliwości dyfuzji kulturowej;
- ekshibicjonizmem informacyjnym obejmującym upublicznianie informacji z różnych sfer życia prywatnego i intymnego;
- brakiem odpowiednich nawyków i przygotowania do właściwego postrzegania i oceny zagrożeń dla bezpieczeństwa kulturowego w wirtualnym świecie;
- krzewieniem i umacnianiem stereotypów kulturowych;
- uzależnieniem od Internetu traktowanego jako jedyny kanał komunikacji ze światem zewnętrznym;
- negatywnymi skutkami ograniczania kontaktów osobistych.

W sferze politycznej funkcjonowania społeczeństwa informacyjnego zagrożenia i wyzwania mogą powstawać na gruncie:

- przedstawiania społeczeństwu przez ośrodki władzy (lub grupy dążące do jej zdobycia) atrakcyjnych i przekonywujących, ale nieprawdziwych informacji na temat prowadzonych lub projektowanych działań politycznych;
- uzyskiwania i identyfikowania w sposób konfidencjonalny opinii obywateli na temat szczegółowych preferencji odnoszących się do różnych aspektów polityki;
- koniunkturalnego, obliczonego na doraźne potrzeby korygowania programów wyborczych przez partie polityczne zgodnie z preferencjami elektoratu wyliczonymi na podstawie metadanych;
- oddziaływania na decyzje wyborcze czy nastroje społeczne w danym państwie przez inne państwa na drodze zorganizowanych kampanii manipulacyjnych i dezinformacyjnych w mediach elektronicznych;
- skrytej ingerencji w elektroniczne systemy głosowania w celu zmiany wyników (np. w wyborach parlamentarnych, prezydenckich, samorządowych, referendach czy nawet wewnętrznych głosowaniach w parlamencie itp.);

– naruszania zasad tajności glosowania (ustalanie, kto jak głosuje);
– naruszania wolności informacyjnej jednostki związanej z rozwojem różnych form inwigilacji jej przekazu w relacjach międzyludzkich;
– ograniczenia w sferze ochrony prywatności, wynikające z wzrastających możliwości w zakresie kontroli i obserwacji tak zachowań społecznych, jak i jednostkowych.

Ważnym aspektem istnienia zagrożeń i wyzwań w społeczeństwie informacyjnym są także te związane z informatyzacją administracji publicznej. Rodzą się one m.in. na gruncie:

– wykradania poufnych informacji z urzędowych systemów informatycznych;
– wyłudzania nienależnych świadczeń;
– uzyskiwania w sposób nieuprawniony poświadczeń i dokumentów;
– słabości systemów udostępniania informacji publicznych;
– nielegalnego pozyskiwania danych osobowych;
– przeglądania i przetwarzania np. przez instytucje działające w sferze bezpieczeństwa wewnętrznego bez zgody obywateli i w oparciu o „naginanie prawa" danych o ich stanie majątkowym, kondycji zdrowotnej czy kontaktach towarzyskich;
– braku dostępu do usług administracyjnych z powodu awarii systemów informatycznych;
– pozyskiwania nadmiernej ilości informacji o obywatelach.

Reasumując, należy zauważyć, że rozwój społeczeństwa informacyjnego wywołał i nadal generuje szereg zasadniczo korzystnych zmian w każdej dziedzinie życia społecznego i jednostkowego. Dokonują się one jednak w różnym tempie ze względu na stopień zaawansowania technologicznego i organizacyjnego poszczególnych państw oraz skuteczność realizowanych strategii. Generalnie szybkie docieranie do informacji ułatwia podejmowanie decyzji. Pamiętać jednak należy, że w obiegu pełno jest bezwartościowych odpadów informacyjnych, a także informacji nieprawdziwych, niepełnych, dlatego trzeba umieć rozsądnie dobierać informacje. Społeczeństwo informacyjne, nasycone rozwiniętymi technologicznie środkami gromadzenia, wyszukiwania oraz przetwarzania informacji oraz komunikowania się, odczuwa także szereg negatywnych zjawisk mających charakter zagrożeń bądź też musi się mierzyć z sytuacjami określanymi jako wyzwania. Można je z mniejszym czy większym nasileniem zaobserwować w różnych sferach funkcjonowania społeczeństwa informacyjnego, od ekonomicznej po kulturową i polityczną. Ich istnienie

i rozwój rodzi ciągłą potrzebę poszukiwania środków i instrumentów oraz wypracowywania metod służących do identyfikacji, ograniczania i likwidowania zagrożeń oraz skutecznego podejmowania wyzwań.

2.4. Sztuczna inteligencja – nowy etap rozwoju infosfery

Analizując istotę, rozwój, a także cechy i funkcje infosfery, dostrzec można, że poza rewolucyjną zmianą wywołaną przez narodziny i rozwój społeczeństwa informacyjnego w pierwszej dekadzie XXI wieku rozpoczęła się kolejna rewolucja informacyjna. W jej ramach ludzką egzystencję na szeroką skalę zaczęła zmieniać sztuczna inteligencja. Sztuczna inteligencja (ang. *Artificial Intelligence*, AI) jako termin została wprowadzona do wąskiego obiegu naukowego w 1956 roku przez Johna McCarthy'ego, który w Dartmouth College (USA) zorganizował konferencję poświęconą perspektywom budowy i rozwoju inteligentnych maszyn. Celem badań rozpoczętych przez J. McCarthy'ego było osiągnięcie przez maszynę poziomu inteligencji człowieka do 1980 r. Prowadzone w kolejnych latach prace badawcze, wpisujące się w ówczesny trend obserwacji i odtworzenia schematów myślowych ludzkiego mózgu, zaowocowały powstawaniem pierwszych narzędzi, aplikacji i maszyn związanych z AI. W roku 1957 Frank Rosenblatt i Charles Wingman skonstruowali perceptron – prosty układ elektromechaniczny zdolny do rozpoznawania znaków alfanumerycznych dzięki odwzorowaniu procesu uczenia się na podstawie języków programowania[177], zaś w 1960 r. Bernard Widrow ukończył prace nad Madaline – pierwszym neurokomputerem, który znalazł zastosowanie komercyjne[178]. W kolejnych latach, z uwagi na fakt, że rezultaty osiągane przez konstruowane maszyny nie spełniały oczekiwań ówczesnych entuzjastów sztucznej inteligencji, zamrożono finansowanie projektów związanych z AI. Tzw. „zima AI" w połączeniu z niedoskonałościami technologicznymi narzędzi badawczych oraz brakiem możliwości praktycznego zastosowania już stworzonych rozwiązań przyczyniły się do niemal całkowitego zaniku zainteresowania tą dziedziną. Współpracę z badaczami kontynuowały wówczas jedynie

[177] Zob. K. Ficoń, *Sztuczna inteligencja. Nie tylko dla humanistów*, Warszawa 2013, s. 90.

[178] Madaline realizował zadania związane z adaptacyjnym przetwarzaniem sygnałów, co przełożyło się na możliwość jego realnego zastosowania w liniach telefonicznych, sonarach, modemach czy radarach.

instytucje wojskowe oraz przedsiębiorstwa komputerowe, które były w stanie sponsorować długotrwałe badania dające perspektywy komercyjnych zysków. Renesans zainteresowania AI nastąpił w latach 90. XX w. wraz ze wzrostem znaczenia eksploracji danych.

Pomimo że obecnie termin „sztuczna inteligencja" jest powszechnie stosowany, jego jednoznaczne zdefiniowanie nie jest proste. Taki stan rzeczy wynika przede wszystkim z tego, że sztuczna inteligencja jest dziedziną o interdyscyplinarnym charakterze, a w jej obrębie poruszanych jest wiele zróżnicowanych zagadnień m.in. z zakresu informatyki, neurologii, psychologii, kognitywistyki czy współczesnej filozofii. Niemniej jednak w ramach prowadzonych od ponad 60 lat badań podejmowane były liczne próby opisowego określenia jej istoty. Zgodnie z definicją słownikową sztuczna inteligencja to „dział informatyki badający reguły rządzące zachowaniami umysłowymi człowieka i tworzący programy lub systemy komputerowe symulujące ludzkie myślenie"[179]. Przynależność AI do nauk informatycznych podkreślają również Waldemar Furmanek, wskazując, że jest to „(…) gałąź informatyki, w ramach której zdalne komputery mogą wykonywać czynności będące zazwyczaj domeną ludzi, szczególnie tych wymagających użycia ludzkiego intelektu czy logiki"[180] oraz Krzysztof Różanowski, traktujący sztuczną inteligencję jako „dział informatyki zajmujący się konstruowaniem maszyn i algorytmów, których działanie posiada znamiona inteligencji. Rozumie się przez to zdolność do samorzutnego przystosowywania się do zmiennych warunków, podejmowania skomplikowanych decyzji, uczenia się, rozumowania abstrakcyjnego itp. Przedmiotem sztucznej inteligencji jest badanie i określanie reguł rządzących inteligentnymi zachowaniami człowieka i wykorzystanie ich w algorytmach i programach komputerowych potrafiących te zasady wykorzystywać"[181]. Z kolei Leszek Rutkowski, powołując się na Marvina Minsky'ego, Edwarda Feigenbauma oraz Roberta J. Schalkoffa, wskazuje, że:

– sztuczna inteligencja jest nauką o maszynach realizujących zadania, które wymagają inteligencji, gdy są wykonywane przez człowieka;

[179] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/szukaj/sztuczna%20inteligencja.html [dostęp: 12.06.2021 r.).
[180] W. Furmanek, *Piąta rewolucja przemysłowa. Eksplikacja pojęcia*, „Edukacja – Technika – Informatyka" 2018, nr 2 (24), s. 277.
[181] K. Różanowski, *Sztuczna inteligencja: rozwój, szanse i zagrożenia*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2007, nr 2, s. 111.

– sztuczna inteligencja to dziedzina informatyki dotycząca metod i technik wnioskowania symbolicznego przez komputer oraz symbolicznej reprezentacji wiedzy stosowanej podczas takiego wnioskowania;
– sztuczna inteligencja obejmuje rozwiązywanie problemów sposobami wzorowanymi na naturalnych działaniach i procesach poznawczych człowieka za pomocą symulujących je programów komputerowych[182].

Propozycja konsensualna w obszarze definiowania sztucznej inteligencji zbudowana jest w oparciu o ujęciu systemowe, w ramach którego zgodzono się, że jest to system oparty na koncepcji maszyny mogącej wpływać na środowisko poprzez formułowanie zaleceń, przewidywań lub podejmowanie decyzji dotyczących zadanego zestawu celów. W tym kontekście działanie sztucznej inteligencji można opisać jako wykorzystywanie danych wejściowych (maszynowych lub ludzkich) do postrzegania środowiska (rzeczywistego lub wirtualnego), kształtowanie modeli na podstawie prowadzonych obserwacji tego środowiska, a następnie interpretowanie stworzonych modeli w celu sformułowania określonych wyników – decyzji, zachowań lub zaleceń. Podobną definicję zawiera opracowanie grupy niezależnych ekspertów przygotowane na zlecenie Komisji Europejskiej. Zgodnie z nim: „Sztuczna inteligencja (AI) odnosi się do systemów zaprojektowanych przez ludzi, które, ze względu na złożony cel, działają w świecie fizycznym lub cyfrowym poprzez postrzeganie swojego środowiska, interpretację zebranych ustrukturyzowanych lub nieustrukturyzowanych danych, wyciągając wnioski z wiedzy uzyskanej z tych danych i dokonując wyboru najlepszych działań do podjęcia (zgodnie z wcześniej określonymi parametrami) dla osiągnięcia wyznaczonego celu. Systemy sztucznej inteligencji można również zaprojektować w taki sposób, aby uczyły się dostosowywać swoje zachowanie poprzez analizę wpływu poprzednich działań na otoczenie”[183]. Systemowe podejście do problematyki AI proponuje również Tomasz Zalewski, wskazując, że jest to „system, który pozwala na wykonywanie zadań wymagających procesu uczenia się i uwzględniania nowych okoliczności w toku rozwiązywania danego problemu i który może w różnym stopniu – w zależności od konfiguracji –

[182] Zob. L. Rutkowski, *Metody i techniki sztucznej inteligencji. Inteligencja obliczeniowa*, Warszawa 2005, s. 6.
[183] *Independent High Level Expert Group on Artificial Intelligence set up by The European Comission, A definition of Artificial Intelligence: main capabilities and scientific disciplines*, Bruksela 2019, s. 6. https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines [dostęp: 13.06.2021 r.].

działać autonomicznie i wchodzić w interakcję z otoczeniem”[184]. Podobne rozumienie analizowanego terminu odnaleźć można w jednym z komunikatów Komisji Europejskiej, gdzie wskazano, że „termin sztuczna inteligencja odnosi się do systemów, które wykazują inteligentne zachowanie dzięki analizie otoczenia i podejmowaniu działań do pewnego stopnia autonomicznie w celu osiągnięcia konkretnych celów”[185].

Wśród innych definicji wypracowanych w toku wieloletnich prac badawczych można znaleźć zarówno takie, które podkreślają powiązania sztucznej inteligencji z inteligencją człowieka, („sztuczna inteligencja to zdolność maszyny do naśladowania lub imitowania ludzkiej inteligencji”[186]), jak również kładące nacisk na możliwość wsparcia i rozwoju człowieka („zbiór technologii, które za pomocą inteligentnych maszyn pozwalają zwiększyć ludzkie możliwości, wykorzystując do tego wykrywanie (obrazów, dźwięków, mowy, tekstu, danych), rozumienie, działanie i uczenie się”[187]).

Bazując na przywołanych wyżej definicjach sztucznej inteligencji, można sformułować wniosek, że warunkiem zaklasyfikowania danego systemu do grupy AI jest jego zdolność do analizy danych i ich interpretacji tak, aby mógł udoskonalać swój system działania, czyli mieć zdolność uczenia się. Jednocześnie działanie uczącego się systemu może przyjmować zróżnicowane formy – może on bowiem tylko dostarczać dane i informacje, wykorzystywane później w dowolny sposób, może rekomendować podjęcie konkretnego działania (przy czym rekomendację tę można odrzucić lub zaakceptować), ale także może samodzielnie podejmować konkretne działania, które użytkownik może anulować lub zablokować. Różnice pomiędzy przedstawionymi formami działania sztucznej inteligencji można określić jako stopień jej autonomii. Niezależnie od stopnia autonomii uczące się systemy mogą wchodzić w interakcję z otoczeniem – zarówno ze światem cyfrowym, jak i ze światem fizycznym.

---

[184] T. Zalewski, *Definicja sztucznej inteligencji*, [w:] *Prawo sztucznej inteligencji*, L. Lai, M. Świerczyński (red.), Warszawa 2020, s. 14.

[185] *Sztuczna inteligencja dla Europy*, Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, http://data.consilium.europa.eu/doc/document/ST-8507-2018-INIT/pl/pdf [dostęp: 14.06.2021 r.].

[186] D. Flisak, *Sztuczna inteligencja – jak chronić prawa autorskie twórczości robotów*, „Rzeczpospolita” z dn. 22.05.2017 r.

[187] M. Skowroński, A. Gugała, S. Jurkiewicz i in., *Sztuczna inteligencja. Dobre praktyki, aspekty prawne i zastosowania w sektorze finansowym. Raport*, s. 6, http://fintechpoland.com/wp-content/uploads/2020/01/AI_raport_FIN.pdf [dostęp: 14.06.2021].

W skompresowanym ujęciu podstawowe różnice pomiędzy tradycyjnymi programami komputerowymi a programami AI zaprezentował Józef S. Zieliński[188]. W szerszym opisie tej kwestii wymieniony autor badania nad sztuczną inteligencją usystematyzował w obrębie dwóch nurtów. Pierwszy to tworzenie fizycznych urządzeń lub ich symulacja komputerowa, drugi to myślowe rozważania stanowiące podstawę tworzenia formalnych modeli rozwiązywanych przy zastosowaniu komputerów[189].

Tabela 6. Porównanie właściwości programów tradycyjnych i programów AI

Programy tradycyjne	Programy AI
Przetwarzanie numeryczne	Przetwarzanie symboliczne
Algorytmiczny zapis działań	Deklaratywny zapis wiedzy
Przetwarzanie wsadowe lub interaktywne	Interaktywne otoczenie programowe
Możliwość sprawdzania poprawności działania programu	Brak praktycznej możliwości pełnego sprawdzenia poprawności działania programu
Rozwój programu na podstawie specyfikacji	Rozwój programów na podstawie tworzenia prototypów i ich ulepszania
Przedstawianie i wykorzystanie danych	Przedstawianie i wykorzystanie wiedzy
Wykorzystanie baz danych	Wykorzystywanie baz wiedzy

Źródło: J.S. Zieliński, *Zarys badań nad sztuczną inteligencją*, [w:] *Inteligentne systemy w zarządzaniu. Teoria i praktyka*, J.S. Zieliński (red.), Warszawa 2000, s. 25.

Rekapitulujac powyższy fragment rozważań, można – dla dalszego zastosowania – przyjąć stanowisko, zgodnie z którym sztuczna inteligencja będzie traktowana jako dziedzina badań ukierunkowana na budowę takich systemów, które będą naśladować ludzką inteligencję. Do sfery AI zaklasyfikować można w szczególności takie obszary, jak: robotyka, sztuczne sieci neuronowe, systemy z bazą wiedzy, systemy eksperckie, rozpoznawanie obrazów, automatyczną naukę, rozumienie języka naturalnego, logikę rozmytą, algorytmy genetyczne i systemy hybrydowe[190]. Główne zadanie, jakie stawiają sobie prowadzący badania nad AI, można sprowadzić do konstruowania maszyn, systemów, aplikacji i programów komputerowych, które są

[188] Zob. tabela 6.
[189] J.S. Zieliński, *Zarys badań nad sztuczną inteligencją*, [w:] *Inteligentne systemy w zarządzaniu. Teoria i praktyka*, J.S. Zieliński (red.), Warszawa 2000, s. 25.
[190] Zob. W. Fehler, *Sztuczna inteligencja – szansa czy zagrożenie,* „Studia Bobolanum" 2017, nr 3, s. 71–72.

zdolne do realizacji wybranych funkcji umysłu i ludzkich zmysłów, zwłaszcza tych niepoddających się algorytmizacji, czyli zamknięciu w skończonej sekwencji określonych czynności koniecznych do wykonania zadania.

Rozwój technologii opartej na sztucznej inteligencji można podzielić na trzy etapy: wąskiej sztucznej inteligencji, ogólnej sztucznej inteligencji oraz sztucznej superinteligencji.

Wąska sztuczna inteligencja[191] (nazywana też słabą) zajmuje się jednym obszarem lub jedną czynnością, do realizacji której została stworzona. Jej maksymalnym poziomem jest odtworzenie procesów zachodzących w mózgu człowieka, stworzenie na ich podstawie modeli matematycznych dla określonego zadania i przekształcenie na programy komputerowe samodzielnie realizujące to zadanie. Pozwala to wykorzystywać ją do wykonywania jednorodnych, specyficznych zadań lub konkretnych typów problemów. Wąska AI może m.in. pokonać człowieka w grze logicznej, odpowiadać na zapytania głosowe, rozpoznawać mowę czy odpowiadać za sterowanie samochodem autonomicznym. Jest zatem inteligencją, która potrafi przewyższyć człowieka w wykonywaniu jednego, określonego zadania. O słabej AI mówi się w kontekście stosunkowo prostych, wyspecjalizowanych systemów o charakterze informacyjno-decyzyjnym, jak również złożonych systemów podejmowania decyzji w czasie rzeczywistym, ale nieodwzorowujących sposobu podejmowania decyzji przez człowieka, tylko realizujących zadania przypisane dotychczas człowiekowi i ludzkiej inteligencji[192].

Ogólna sztuczna inteligencja (nazywana też silną AI) to etap jej rozwoju związany z konstruowaniem maszyn dorównujących inteligencją człowiekowi, które mogłyby myśleć jak człowiek i wykonywać dowolne zadania intelektualne tak jak on. W tej fazie rozwoju AI naśladuje w pełni sposób i mechanizmy ludzkiego myślenia, analizowania informacji i wnioskowania, a w wyniku tych działań uzyskuje rezultaty jak człowiek.

Sztuczna superinteligencja z kolei ma się charakteryzować najwyższym stopniem zaawansowania rozwoju, co oznacza, że praktycznie w każdej dziedzinie może być bardziej inteligentna niż najbardziej rozwinięty mózg człowieka, posiadając zarówno naukową kreatywność, jak i ogólną mądrość oraz umiejętności społeczne. Pozwoli to jej na stałe i samodzielne udoskonalanie się – w ten sposób może osiągnąć poziom niekontrolowanego rozwoju,

[191] Ang. ANI – Artificial-Narrow Intelligence.

[192] Zob. A.M. Wilk, *Sztuczna inteligencja – wyzwaniem XXI wieku*, „Przegląd Telekomunikacyjny" 2018, nr 5, s. 106.

zaś motywy jej działania przekroczyć mogą zdolności poznawcze człowieka. W ujęciu generalnym superinteligencję można rozumieć jako „każdy umysł, który pod względem zdolności poznawczych znacznie przewyższa człowieka w każdej dziedzinie zainteresowań”[193], przy czym przewaga ta może dotyczyć szybkości przetwarzania informacji, zdolności do agregacji dużej liczby jednostek obliczeniowych i posiadania dodatkowych możliwości poznawczych niedostępnych współczesnemu człowiekowi. Ponadto przewiduje się, że superinteligencja będzie mieć postać inteligencji ogólnej (czyli wielozadaniowych systemów szerokiego zastosowania), posiadać autonomię (rozumianą jako możliwość podejmowania decyzji poza bieżącą kontrolą operatora) oraz zdolność samoulepszania (tj. projektowania urządzeń i wprowadzania nowszych wersji własnego oprogramowania). Należy jednak zaznaczyć, że przedstawione postulaty znaczeniowe odnoszą się do czegoś, co jeszcze (w opisywanej formie) nie istnieje, a jedynym miarodajnym punktem ich odniesienia jest inteligencja ludzka[194]. Z koncepcją superinteligencji wiąże się teoria stworzenia technologicznej osobliwości. Osobliwość tę należy rozumieć jako moment w historii ludzkości, w którym zaawansowana technologia w połączeniu z odpowiednim potencjałem informacyjnym i technicznym pozwoli na zbudowanie maszyny dysponującej superinteligencją. Wówczas mechaniczne maszyny mogą zwiększyć zdolności fizyczne człowieka, a sztuczna inteligencja przyczyni się do wzrostu możliwości intelektualnych do wręcz nieograniczonego poziomu[195]. Entuzjasta tej koncepcji, Ray Kurzweil, wyjaśnia, że „osobliwość będzie stanowić kulminację połączenia naszego biologicznego myślenia i istnienia z naszą technologią (…). Po pojawieniu się osobliwości nie będzie żadnej różnicy między człowiekiem a maszyną”[196].

Badacze problematyki AI mają świadomość, że w przyszłości komputery mogą osiągnąć zdolności powodujące, iż sztuczna inteligencja przerośnie ludzką. Niektórzy z nich, jak np. wspomniany R. Kurzweil, stoją na stanowisku, że po osiągnięciu tego poziomu AI może być kształtowana przez człowieka w taki sposób, aby wspomóc rozwiązywanie istotnych problemów ludzkości, jak np. głód, globalne ocieplenie, choroby cywilizacyjne czy bezdomność.

[193] N. Bostrom, *Superinteligencja. Scenariusze, strategie, zagrożenia*, Gliwice 2016, s. 45.
[194] Zob. P. Przybysz, *Czy należy obawiać się superinteligencji?*, „Studia Metodologiczne” 2017, nr 38, s. 196.
[195] Zob. G. Osika, *Czekając na osobliwość – o modelach interpretacji techniki*, „Filo-Sofija” 2017, nr 39/1, s. 66.
[196] R. Kurzweil, *Nadchodzi osobliwość. Kiedy człowiek przekroczy granice biologii,* Warszawa 2016, s. 25.

Z kolei inni, jak Stephen Hawking, Elon Musk[197] czy Bill Gates, wyrażają znacznie mniej entuzjastyczny stosunek, wskazując, że skoro AI będzie nieustannie i samodzielnie się udoskonalać, to nie tylko przewyższy poziom człowieka, ale osiągnie również możliwości niekontrolowanego rozwoju, co w dalszej perspektywie może sprawić, że motywy jej działania nie będą ani przewidywalne, ani zrozumiałe dla ludzi[198].

Sztuczna inteligencja jest obecnie wykorzystywana w tak wielu zróżnicowanych obszarach, że sporządzenie ich pełnego, a zarazem aktualnego spisu jest raczej niemożliwe[199]. Ze względu na zakres i cel prowadzonych rozważań dalsze odniesienia dotyczyć będą zatem tylko wykorzystania AI w sferze informacyjnej.

We wspomnianej sferze sztuczna inteligencja znajduje zastosowanie głównie w zabezpieczeniach systemów informatycznych (służy do wykrywania szkodliwego oprogramowania, przywracając optymalne parametry funkcjonowania tych systemów), zapewnianiu kryptograficznej ochrony informacji (m.in. poprzez szyfrowanie danych i dostępu do nich) oraz utrzymywaniu odpowiedniego stopnia ochrony przed atakami na infrastrukturę krytyczną. AI zapewnia także wzrost bezpieczeństwa IT, głównie z uwagi na wzmocnienie odporności punktów końcowych, czyli wszystkich urządzeń, które mają możliwość połączenia się z siecią w strukturze informatycznej organizacji. System bezpieczeństwa punktów końcowych chroni te urządzenia przed zagrożeniami związanymi z przedostawaniem się do sieci firmowej złośliwego oprogramowania oraz innymi działaniami ukierunkowanymi na wyrządzenie szkód. Wykorzystanie uczenia maszynowego oraz narzędzi sztucznej inteligencji w systemie ochrony punktów końcowych skutkuje podniesieniem poziomu ich automatyzacji. Są one w stanie samodzielnie analizować ruch w sieci organizacji, a co za tym idzie – identyfikować pojawiające się zagrożenia bez konieczności angażowania w ten proces ludzi[200]. AI jest wykorzystywana również do tworzenia filtrów antyspamowych skrzynek e-mailowych oraz

[197] Elon Musk – jeden z założycieli OpenAI, będącego konsorcjum badawczym nastawionym na prowadzenie odpowiedzialnych badań nad AI.

[198] Zob. A. Turek, *Sztuczna inteligencja – realne zagrożenie? Gates: „Nie rozumiem, czemu niektórzy się nie przejmują*", http://innpoland.pl/115221,sztuczna-inteligencja-realne-zagrozenie-gates-nie-rozumiem-czemu-niektorzy-sie-nie-przejmuja [dostęp: 12.06.2021 r.].

[199] Zob. N. Bostrom, dz. cyt., s. 35.

[200] Zob. G. Kubera, *Ochrona punktów końcowych – co trzeba o niej wiedzieć*, „Computer World" z dn. 27.12.2018, https://www.computerworld.pl/news/Ochrona-punktow-koncowych-co-trzeba-o-niej-wiedziec,411 609.html [dostęp: 23.04.2020 r.].

weryfikacji użytkowników i wymienianych treści w celu zabezpieczenia przed generowaniem przeciążeń sieci teleinformatycznych. Możliwości wykorzystania AI w sferze informacyjnej obejmują także systemy pozyskiwania i analizy informacji, rozumienia i tłumaczenia języka naturalnego, rozpoznawania optycznego oraz rozpoznawania języka mówionego i tłumaczenia mowy w czasie rzeczywistym. Sztuczna inteligencja opanowała także systemy dialogowe oraz rozpoznawanie optyczne, w tym rozpoznawanie pisma ręcznego, przyczyniając się do sprawniejszej i mniej czasochłonnej komunikacji na linii użytkownik – komputer.

Sztuczna inteligencja znalazła również zastosowanie w automatyzacji szyfrowania danych – już w 2016 r. Google ogłosił, że stworzony przez nią algorytm potrafi stworzyć i zastosować własne standardy szyfrowania danych przesyłanych pomiędzy użytkownikami w oparciu o sztuczne sieci neuronowe[201].

AI jest używana także w obszarze zwiększania bezpieczeństwa klientów podczas korzystania z internetowych usług bankowych. Jednym z największych wyzwań, z którymi mierzą się obecnie światowe instytucje finansowe, jest zapobieganie nieuprawnionemu przejmowaniu kont bankowych. Ataki phishingowe na klientów banków oraz brak efektywnego sposobu powstrzymywania wycieków z baz danych sprawiają, że nieustannie zwiększa się zapotrzebowanie na niezawodne, a jednocześnie przystępne dla użytkownika systemy zabezpieczeń bankowych. Specjaliści od systemów IT w bankowości dążą zatem do ulepszania i optymalizacji rozwiązań, które zapewnią bezpieczeństwo przetwarzania zgromadzonych zbiorów danych, koncentrując się przede wszystkim na sposobach dostępu do konta online (procedurach autoryzacji i logowania do konta). Stosowanie tradycyjnych rozwiązań (logowanie za pomocą hasła złożonego z ciągu znaków) jest narażone na atak ze strony botów ukierunkowanych na złamanie i kradzież kodów i haseł zabezpieczających. Wśród nowych rozwiązań, które mają zapewnić bezpieczeństwo użytkownikom bankowości elektronicznej, wskazuje się najczęściej autoryzację klienta za pomocą danych biometrycznych – w pierwszej kolejności odcisku palca, w dalszej perspektywie – rozpoznawania twarzy. Są one uznawane za najlepsze i najprostsze zabezpieczenie przed włamaniem do systemu z uwagi na swoją niepowtarzalność, a jednocześnie łatwość zastosowania. Nawet rysy

[201] Zob. A. Berger, *Sztuczna inteligencja Google'a tworzy własne systemy szyfrowania*, https://trybawaryjny.pl/sztuczna-inteligencja-googlea-tworzy-wlasne-systemy-szyfrowania [dostęp: 09.07.2020 r.].

twarzy utrwalone na fotografii stanowią unikatową treść w przypadku rozwiązań umożliwiających identyfikację osoby przedstawionej na obrazie. Obecnie możliwe jest już założenie konta bankowego na podstawie przesłanego przez użytkownika zdjęcia twarzy.

W XXI w. sztuczna inteligencja zaczęła zyskiwać także coraz większe uznanie jako dobro konsumenckie. Wśród najpopularniejszych rozwiązań bezpośrednio związanych z funkcjonowaniem człowieka w infosferze wyróżnić należy Siri, osobistą asystentkę dla systemu operacyjnego iOS, która oferuje m.in. interakcję z e-mailami, kalendarzem, przypomnieniami, kontaktami, oraz Alexę, bezprzewodowe urządzenie wprowadzone na rynek przez firmę Amazon. Alexa może służyć m.in. do odtwarzania muzyki, audiobooków, przekazywania różnych informacji, potrafi również kontrolować inteligentne urządzenia domowe[202].

Kluczowy cel wdrażania rozwiązań i narzędzi sztucznej inteligencji do sfery informacyjnej można zdefiniować jako stworzenie systemu cyberzabezpieczeń, w którym narzędzia te mogą jednocześnie się uczyć i rozwijać. W ten sposób generowane są kolejne określone wzorce i schematy postępowania systemu, do których na bieżąco dodawane są informacje zwrotne pochodzące z systemów analizy zagrożeń. Dzięki temu możliwe jest ciągłe doskonalenie działania wdrożonego systemu. AI jest przeszkolona i przygotowana do przetwarzania ogromnych ilości danych, zarówno ze źródeł ustrukturyzowanych (bazy danych), jak i nieustrukturyzowanych (blogi, artykuły informacyjne, wiadomości). Poprzez techniki głębokiego uczenia i uczenia maszynowego system poszerza swoją wiedzę, aby poznać, a nawet „zrozumieć" zagrożenia cybernetyczne i oszacować poziom cyberryzyka. Wdrożenie rozwiązań AI w analizowanym obszarze bezpieczeństwa, związanym z przetwarzaniem informacji, eliminuje czasochłonne zadania badawcze i pozwala na automatyczną analizę ryzyka na podstawie wybranych danych, znacząco skracając czas potrzebny analitykom bezpieczeństwa organizacji do podjęcia kluczowych decyzji i implementacji skoordynowanych środków zaradczych w stosunku do wykrytych zagrożeń.

Odnosząc się do korzyści wynikających ze stosowania sztucznej inteligencji w sferze informacyjnej, należy zauważyć, że systemy wykorzystujące rozwiązania AI stanowią istotne wsparcie w procesie decyzyjnym, niezależnie

[202] Zob. B. Mróz, *Konsument a wyzwania technologiczne XXI w.*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2017, nr 330, s. 142.

od tego, w jakiej branży znajdą zastosowanie. Wykorzystanie AI w procesie decyzyjnym może przyczynić się do zwiększenia jego skuteczności, pozwalając symulować i testować określone scenariusze, a następnie na podstawie analizy danych przewidywać potencjalne skutki planowanych działań. Zalety wynikające z zastosowania sztucznej inteligencji obejmują przede wszystkim możliwość przetwarzania i analizowania bardzo dużych ilości danych, zdolność do wyszukiwania między nimi powiązań i generowania na tej podstawie wzorców, co pozwala na grupowanie danych i tworzenie powiązań w skali rosnącej, przy jednoczesnym wykazywaniu pojawiających się anomalii i odstępstw od dostrzeżonych zależności. Dodatkowo działania te podejmowane są w czasie przekraczającym możliwości percepcji i rozumowania człowieka. To z kolei skutkuje przyspieszeniem procesu decyzyjnego, stając się elementem budowy przewagi nad konkurencją i pozwala wdrożyć skuteczne rozwiązania. Sytuacja, w której AI stanowi element tego procesu, a nie jest jego ostatecznym ogniwem, pozwala na zachowanie kontroli nad jej dalszym rozwojem w kierunku i stopniu pożądanym przez człowieka. Jeżeli chodzi o bezpieczeństwo informacji, to istotnym argumentem za wdrożeniem rozwiązań AI w kontekście zapewniania ochrony danych, wykrywania i blokowania ataków ukierunkowanych na zbiory tych danych oraz szeroko rozumiane inne zasoby informacyjne jest zminimalizowanie czasu potrzebnego na wykrycie zagrożenia. Im dłużej atakujący pozostaje w infrastrukturze sieciowej organizacji, tym więcej może pozyskać danych, zaszyfrować lub uszkodzić systemów informatycznych lub baz danych, a co za tym idzie – tym większe straty ponosi zaatakowany podmiot.

Obok szans związanych z obserwowanym rozwojem upowszechnianie rozwiązań AI generuje także nowe, nieznane wcześniej zagrożenia, wyzwania i ryzyka dla poszczególnych sfer bezpieczeństwa. Podobnie jak korzyści, tak i negatywne efekty wynikające z rozwoju AI mogą się zmaterializować w różnych jego wymiarach. Należy pamiętać, że w każdym systemie istnieje ryzyko błędnego zarządzania. Podatności i niebezpieczeństwa mogą pojawić się również w wyniku wypadków i nieprzewidywalnych zdarzeń, będących następstwami błędów konstrukcyjnych. Tego typu sytuacje stanowią wyzwanie zarówno dla decydentów najwyższego szczebla, jak i przedsiębiorców czy pojedynczych osób.

Jeżeli myślimy o zagrożeniach dla sfery bezpieczeństwa informacyjnego, to coraz większym zagrożeniem staje się dezinformacja[203], która może skutkować manipulowaniem zarówno jednostkami, jak i społeczeństwami z wykorzystaniem masowego generowania przy pomocy rozwiązań z zakresu AI dużej ilości zmanipulowanych czy fałszywych informacji. W szerszej perspektywie szkodliwe wykorzystanie AI może przyczynić się do powstania nowych cyberzagrożeń dla demokracji i pokoju, głównie w postaci socjomanipulacji. Technologia ta może bowiem zostać użyta w celach politycznych i inwigilacyjnych, do wprowadzania odbiorców w błąd i wywierania na nich zaplanowanego politycznie wpływu.

W dyskursie dotyczącym sztucznej inteligencji pojawiają się również przewidywania trendów negatywnych, związanych przede wszystkim z zagrożeniami dla cyberbezpieczeństwa. Jednym z najbardziej prawdopodobnych niebezpieczeństw jest możliwość wykorzystania nowoczesnych technologii do omijania kontroli bezpieczeństwa i dokonywania włamań przez cyberprzestępców. Technologia może się bowiem przyczynić nie tylko do efektywnej analizy mechanizmów ochronnych systemu, ukierunkowanej na wyszukanie jego najsłabszych i najbardziej podatnych na atak obszarów, ale również umożliwić podłączenie się niezweryfikowanych klientów pod spływające strumienie danych oraz wykorzystanie ich do dalszych ataków na infrastrukturę sieciową ofiary[204].

Duże zagrożenia wiążą się również z możliwością wykorzystania AI przez hakerów. Systemy AI są w stanie zarówno łatwo wykryć, jak i wykorzystać pojawiające się luki w zabezpieczeniach danych. Prognozuje się, że wraz z upływem czasu ich zdolności w tym zakresie będą coraz większe oraz mniej czasochłonne. Dostęp do oprogramowania pozwalającego na uczenie maszynowe jest łatwy, nie wymaga zaawansowanych nakładów finansowych, zwłaszcza, że „samouczki" są dostępne w Internecie. Testowanie różnorodnych rodzajów oprogramowania za pomocą licznych programów antywirusowych pozwala odkryć algorytmy, na których opiera się praca tych programów, oraz luki w ich działaniu. Atak technologiczny i złamanie zabezpieczeń pozwala uzyskać dostęp do chronionych danych i umożliwia ich przejęcie, modyfikację lub usunięcie. Wykorzystanie w tym procesie inteligentnych maszyn

[203] Szerzej na ten temat w podrozdziale 3.3.
[204] Zob. S. Gliwa, *AI vs AI. Jakie trendy bezpieczeństwa i zagrożeń czekają nas w 2020 roku*?, [online], https://www.cyberdefence24.pl/ai-vs-ai-jakie-trendy-bezpieczenstwa-i-zagrozen-czekaja-nas-w-2020-roku [dostęp: 24.04.2020 r.].

pozwala znacząco skrócić czas przeprowadzenia ataku. Kolejną formą wykorzystania sztucznej inteligencji w ramach środowiska „blackhat"[205] jest jej zastosowanie do przestępstw internetowych z użyciem oprogramowania ransomware (które blokuje dostęp do danych zawartych na dysku lub całkowicie szyfruje te dane do momentu dokonania płatności przez ofiarę ataku) oraz ataków BEC[206]. Wykorzystanie AI w tego typu atakach polega na zautomatyzowanym wyszukiwaniu najbardziej podatnych (zwłaszcza technologicznie i socjologicznie) ofiar oraz dopasowywania treści wiadomości do konkretnego odbiorcy przy użyciu danych znajdujących się przede wszystkim w ogólnodostępnych (ale także niejawnych) zasobach informacyjnych[207]. Szereg potencjalnych wyzwań i zagrożeń wiąże się z robotyzacją pracy służb policyjnych. Jako szczególnie ważna jest tu podnoszona kwestia ochrony prywatności. Pojawiają się uzasadnione obawy, że szerokie używanie AI doprowadzi do nadmiernej skali inwigilacji i utraty prywatności ludzi. Sztuczna inteligencja otwiera bowiem możliwości korzystania z ogromnych ilości danych, w tym danych osobowych, a co za tym idzie – ich nadużywania i naruszania w ten sposób bezpieczeństwa informacyjnego jednostki oraz praw obywatelskich. W omawianym kontekście prawdopodobne stają się również nadużycia w zakresie inwigilacji ze strony służb wywiadowczych i kontrwywiadowczych. AI może być również wykorzystywana do tworzenia zaawansowanej, szkodliwej inżynierii społecznej. Wsparcie sztucznej inteligencji umożliwi bowiem prowadzenie zautomatyzowanej, zaawansowanej i spersonalizowanej propagandy społecznej, w szczególności za pośrednictwem mediów społecznościowych. Treść przesyłanych informacji może być dostosowywana do poszczególnych użytkowników na podstawie śladu cyfrowego, ujawniającego aktywność w cyberprzestrzeni, preferencje, przekonania polityczne i światopoglądowe, a nawet określony nastrój, jak również przekazywana różnymi kanałami komunikacji wykorzystywanymi przez użytkownika. Złośliwe boty mogą również zostać wykorzystane do prowadzenia innych działań naruszających

[205] Black hat (czarne kapelusze) – hakerzy działający na granicy lub poza granicami prawa. Termin „blackhat" zapożyczono z westernów, w których dobrzy bohaterowie noszą białe kapelusze, natomiast złoczyńcy – czarne.

[206] Business Email Compromise – podszywanie się hakerów pod członków kadry zarządzającej przedsiębiorstwa i wysyłanie w ich imieniu personalnych próśb o przelew wysokich sum do dyrektorów finansowych.

[207] Zob. M. Korolov, *AI isn't just for the good guys anymore*, http://www.csoonline.com/article/3163022/advanced-persistent-threats/ai-isnt-just-for-the-good-guys-anymore.html [dostęp: 12.06.2021 r.].

bezpieczeństwo IT, których celem jest dezinformacja użytkowników. Możliwe jest np. użycie ich do automatycznego generowania fałszywych wyświetleń reklam, co wprowadza w błąd reklamodawców i powoduje marnotrawstwo ich budżetu.

W kontekście opisanych wcześniej zagrożeń dla bezpieczeństwa informacyjnego i bezpieczeństwa informacji konieczne jest zatem zachowanie zdolności krytycznego myślenia i weryfikacji pozyskiwanych informacji oraz ich źródeł. Jest to o tyle istotne, że treści przygotowywanych, udostępnianych i powielanych przy użyciu narzędzi opartych na sztucznej inteligencji stale przybywa. Według raportu *Bot Traffic Report 2016* mniej niż połowa całego ruchu w Internecie (48%) jest generowana przez ludzi – pozostałe 52% to działalność botów, wyręczających człowieka w konkretnych czynnościach, w tym przypadku – w aktywności internetowej. Około 30% z nich to złe boty, wykorzystywane do przestępczości internetowej. Mogą one zostać nielegalnie wynajęte i użyte do szybkiego rozprzestrzeniania zarówno złośliwego oprogramowania i wirusów, jak również do fałszywych komunikatów (zwłaszcza w mediach społecznościowych) czy generowania spamu lub innych oszustw internetowych. Ataki te mogą być przeprowadzone na platformach stacjonarnych (komputery domowe), mobilnych (telefony, tablety, smartfony), ale również na różnego rodzaju inteligentnych sprzętach domowych funkcjonujących w środowisku internetu rzeczy. Złe boty mogą również atakować systemy bankowe, doprowadzając w ten sposób do zawirowań na rynkach finansowych.

Za istotne zagrożenie natury ogólnej należy uznać to, że systemy nie są w stanie wyjaśnić, jak działają ich algorytmy, co narusza kluczową zasadę etyczną w zakresie robotyki, jaką jest przejrzystość. Zapisy rezolucji Parlamentu Europejskiego z dnia 16 lutego 2017 r. wskazują, że „w każdym przypadku powinno być możliwe uzasadnienie wszelkich decyzji podjętych za pomocą sztucznej inteligencji, które mogą mieć istotny wpływ na życie przynajmniej jednej osoby”[208]. Poszanowanie tej zasady warunkuje możliwość przedstawienia obliczeń dokonanych za pomocą systemu AI w formie zrozumiałej dla człowieka, dlatego też niezbędna jest zdolność do odtworzenia wszystkich operacji wykonanych przez system, a zwłaszcza kroków logicznych, które doprowadziły do podjęcia przez niego określonej decyzji.

[208] *Rezolucja Parlamentu Europejskiego z dnia 16 lutego 2017 zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki* (2015/2103(INL)).

Należy mieć również świadomość, że AI może stać się narzędziem działań, których celem będzie zmiana porządku ustrojowego państwa (transformacja funkcjonowania systemu politycznego) na drodze zaplanowanego zmasowanego informacyjnego oddziaływania na społeczeństwo przy użyciu rozwiązań z zakresu AI. Wraz z rozwojem nowych technologii bazujących na AI mogą w przestrzeni publicznej pojawić się nowe podmioty, niezależne od państwa i niepoddające się jego kontroli, stwarzające ryzyko podejmowania działań ingerujących w informacyjne prawa i wolności obywateli. Michael Miller bezpieczeństwo informacyjne człowieka w czasach *big data* łączy z bezpieczeństwem osobistych danych pozyskiwanych przez internet rzeczy i algorytmy służące do inwigilacji społeczeństwa oraz z bezpieczeństwem internetu rzeczy jako całości[209]. Szczególnie ta druga sfera wymaga lepszych zabezpieczeń, aby każdy punkt sieci był godny zaufania. Najsłabiej chronione inteligentne urządzenia mogą stać się potencjalnym celem ataków i spowodować niewyobrażalne szkody. A takich słabych punktów wraz z rozwojem internetu rzeczy będzie przybywać[210]. Bezpieczeństwo człowieka w środowisku ekstrakcji wielkich danych można sprowadzić za Katarzyną Jasińską do problemów związanych z:

– nieuprawnionym wykorzystywaniem informacji, które związane jest ze zbieraniem i przetwarzaniem na masową skalę danych o osobach indywidualnych;
– nadmierną komercjalizacją, która polega na intensyfikacji przekazu marketingowego we wszystkich dostępnych kanałach informacyjnych;
– cyberzagrożeniami dla infrastruktury krytycznej, które obecnie utożsamiane są głównie z atakami hakerów;
– kreowaniem fikcji, która sprowadza się do sterowania przekazem medialnym przez wszechobecne algorytmy decydujące, które informacje wyświetlić w sieci dla określonego użytkownika, i do przekazywania nieprawdziwych, szokujących informacji w celu wygenerowania fałszywego ruchu w sieci;

[209] M. Miller, *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat,* Warszawa 2016, s. 349.
[210] Zob. H. Batorowska, *Przegląd wizji badaczy na temat bezpieczeństwa i przetrwania człowieka w dobie big data i sztucznej inteligencji*, „Annales Universitatis Paedagogicae Cracoviensis. Studia ad Bibliothecarum Pertinentia" 2020, nr 18, s. 370.

– dyktaturą danych, czyli zjawiskiem, które pozwala korzystać z potencjału ukrytego w olbrzymich bazach danych do realizacji celów związanych z ugruntowaniem pozycji monopolistycznej lub władzy;
– naruszaniem zasady sprawiedliwości i wolnej woli polegającym na możliwości stosowania zasady karania za określone skłonności;
– przekazywaniem danych przez nieświadomych użytkowników, co jest konsekwencją małej wiedzy na temat wartości tych danych;
– naruszaniem neutralności sieci, czyli traktowaniem użytkowników w różny sposób;
– naruszaniem neutralności technologicznej polegającym na możliwości wykupienia priorytetowego trybu udostępnienia infrastruktury;
– informacyjnym blackoutem, w wyniku przeciążenia urządzeń i łączy nadmierną ilością danych i informacji;
– pauperyzacją intelektualną, która polega na obniżeniu możliwości intelektualnych ludzi i w konsekwencji zastąpieniu pewnych czynności przez technologie, co prowadzić może do zaniku zdolności analitycznych, skłonności do podejmowania ryzyka i zdominowania jednostki przez dyktat danych[211].

Obserwując obecny poziom zaawansowania AI i związany z nim dyskurs publiczny, można stwierdzić, iż korzyści płynące z dotychczasowych osiągnięć i perspektywy wdrożenia kolejnych rozwiązań zagłuszają sygnały o możliwych zagrożeniach. Dyskusja dotycząca nie korzyści, ale wyzwań i zagrożeń związanych ze stworzeniem mechanicznej superinteligencji przebiega – jak na razie – bez większego rozgłosu. Dominuje postawa optymistyczna, której jednym z najbardziej rozpoznawalnych orędowników jest R. Kurzweil, przepowiadający rychłe nastanie osobliwości, czyli takiego momentu w rozwoju cywilizacji, w którym postęp technologiczny gwałtownie przyspieszy. Chwilą tą ma być pojawienie się sztucznej inteligencji, zdolnej do samodzielnego udoskonalania samej siebie. Zdaniem wspomnianego autora ten cyfrowy superumysł rozwiąże problemy, z którymi naturalny mózg człowieka nie potrafi sobie poradzić[212]. Jednak trzeba, bez wątpienia dostrzegając duże korzyści ze stworzenia superinteligentnych maszyn, brać pod uwagę także możliwość, że

[211] K. Jasińska, *Big data – wielkie perspektywy i wielkie problemy*, [w:] *Megatrendy i ich wpływ na rozwój sektorów infrastrukturalnych*, J. Gajewski, W. Paprocki, J. Pieriegud (red.), Gdańsk 2015, s. 73–78.
[212] Całościowo swoje poglądy wspomniany autor zebrał w książce pt. *Nadchodzi osobliwość. Kiedy człowiek przekroczy granice biologii*.

potężniejsza od ludzkiej sztuczna inteligencja zacznie wymykać się spod ludzkiej kontroli i pracować w związku z tym nad jej utrzymaniem. Warto w tym miejscu dodać, że przekonanie, jakoby formuły algorytmiczne były w pełni neutralne, jest mylne. Każdy algorytm charakteryzuje się bowiem uprzedzeniami i błędami myślowymi jego twórców. Oznacza to, że te algorytmy mogą rządzić naszym życiem zgodnie z zamierzeniami ich autorów.

Podsumowując ustalenia dotyczące sztucznej inteligencji i jej miejsca w infosferze, ze szczególnym uwzględnieniem obszaru bezpieczeństwa informacyjnego, musimy mieć świadomość, że niemożliwe jest wyrwanie się spod jej narastającego oddziaływania. Tak długo bowiem, jak będziemy chcieli być aktywnymi uczestnikami życia społecznego (publicznego), będziemy mieli do czynienia z tym, co ona niesie. Rzecz jasna nie można w pewny sposób prognozować kolejnych efektów rozwoju sztucznej inteligencji. Jednak można stwierdzić, że będzie ona zyskiwała ciągle nowe możliwości i rozwijała się. Będzie tak dlatego, że na obecnym poziomie informatyzacji i cyfryzacji przytłaczająca większość instytucji, organizacji, jednostek, grup społecznych oraz państw nie może już funkcjonować poza mechanizmami społeczeństwa informacyjnego. Należy jednak podkreślić, że nadzieja, że sztuczna inteligencja rozwiąże wszystkie problemy, jest myśleniem na wyrost. Co więcej, w niesprzyjających okolicznościach może ona przyczynić się do głębokiego kryzysu, grożącego dezintegracją rozrastających się systemów informatyczno-informacyjnych, na których opiera się współczesny świat. Źródłem problemów może stać się m.in. zachwianie równowagi między zdobyczami technik informacyjnych a dotychczas przyjętymi i uznawanymi za fundamentalne aksjologicznymi i emocjonalnymi fundamentami życia ludzkiego gatunku. Ponieważ jednak jesteśmy ciągle w fazie rozwojowej AI, należy działać tak, aby w przyszłości nie okazała się ona tworem nieludzkim. Jest to zadanie ciągłe, w realizacji którego głównej roli nie powinny odgrywać jedynie technika i korzyści, lecz także postawy ludzkie budowane na wartościach, trosce o przyszłe pokolenia oraz świadomości rozlicznych i nie w pełni rozpoznawalnych uwarunkowań funkcjonowania sztucznej inteligencji.

3. Zagrożenia i bariery informacyjne

3.1. Rozumienie i podział zagrożeń bezpieczeństwa informacyjnego i bezpieczeństwa informacji

W logicznym następstwie uznania za konieczne wyodrębniania pojęć „bezpieczeństwo informacyjne" i „bezpieczeństwo informacji"[213] należy dążyć także do określenia zakresu znaczeniowego terminów „zagrożenia bezpieczeństwa informacyjnego" i „zagrożenia bezpieczeństwa informacji". Rzecz jasna nie da się – ze względu na ich wzajemne przenikanie i posiadanie wspólnego mianownika, jakim jest bezpieczeństwo i informacja – dokonać jednoznacznych rozgraniczeń tych pojęć. Jednak zarówno utylitarna, jak i naukowa potrzeba ogólnej systematyzacji i precyzowania aparatu pojęciowego w tak ważnej sferze, jaką jest bezpieczeństwo informacyjne, nakazuje przeprowadzenie stosownych analiz i dokonanie na ich bazie niezbędnych uogólnień.

Posiadający bogaty dorobek badawczy w dziedzinie bezpieczeństwa informacyjnego T.R. Aleksandrowicz lapidarnie stwierdza, że „zagrożeniem dla bezpieczeństwa informacyjnego podmiotu jest każde naruszenie atrybutów informacji w taki sposób, iż nie może on wypełniać swoich funkcji"[214]. Z kolei w niezbyt czytelnym ujęciu autorów projektu polskiej doktryny cyberbezpieczeństwa zagrożenia bezpieczeństwa informacyjnego to „pośrednie lub

[213] Szerzej na ten temat w rozdziale 4.
[214] T.R. Aleksandrowicz, *Bezpieczeństwo informacyjne państwa*, „Studia Politologiczne" 2018, nr 49, s. 45.

bezpośrednie, zakłócające lub destrukcyjne oddziaływania na podmiot”[215]. Dążąc do bardziej precyzyjnego ukazania istoty tej ważnej kategorii pojęciowej, można przyjąć, że zagrożenia bezpieczeństwa informacyjnego to mające różnorodny charakter procesy, zjawiska, zdarzenia i sytuacje, w wyniku których mamy do czynienia z uświadamianymi lub nieuświadamianymi ograniczeniami, błędami, zaniechaniami, nadużyciami lub przestępczymi (wrogimi) działaniami godzącymi w swobodny (zgodny z potrzebami i prawem) dostęp do aktualnych, rzetelnych, integralnych zasobów informacyjnych.

Złożoność i rozległość informacyjnych zagrożeń bezpieczeństwa rodzi konieczność ich bardziej szczegółowej charakterystyki, której dokonuje się poprzez przedstawianie różnych ujęć klasyfikacyjnych.

Piotr Bączek, autor monografii poświęconej związkom zagrożeń informacyjnych ze stanem bezpieczeństwa państwa polskiego, dzieli zagrożenia bezpieczeństwa informacyjnego na:

– losowe (klęski żywiołowe, katastrofy, wypadki, które wpływają na stan bezpieczeństwa informacyjnego podmiotu);
– tradycyjne (szpiegostwo, działalność dywersyjna lub sabotażowa ukierunkowana na zdobycie informacji lub ofensywna dezinformacja prowadzona przez osoby i organizacje);
– technologiczne (związane z gromadzeniem, przechowywaniem i przetwarzaniem informacji w sieciach teleinformatycznych, np. przestępstwa komputerowe, cyberterroryzm, walka informacyjna);
– odnoszące się do praw obywatelskich osób lub grup społecznych (nielegalna sprzedaż informacji, przekazywanie informacji podmiotom nieuprawnionym, naruszanie przez władze prywatności, bezprawne ingerencje służb specjalnych w sferę wolności i prywatności informacyjnej, ograniczanie jawności życia publicznego);
– powstające na gruncie wadliwych rozwiązań organizacyjno-strukturalnych[216].

Opierając się na ustaleniach zawartych w przywoływanym już projekcie polskiej doktryny cyberbezpieczeństwa, można w sposób ogólny wskazać

[215] Zob. *Doktryna bezpieczeństwa informacyjnego. Projekt*, BBN, Warszawa 2015, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf s. 3 [dostęp: 17.05.2021 r.].
[216] Zob. P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2005, s. 72–73.

na istnienie następujących wewnętrznych i zewnętrznych zagrożeń dla bezpieczeństwa informacyjnego. W aspekcie wewnętrznym są to zagrożenia:

- związane z niedoskonałościami społeczeństwa obywatelskiego, m.in.:
  - występowanie deficytów informacyjnych obniżających odporność na wrogą perswazję;
  - dezinformacja;
  - dywersja ideologiczna (propagowanie idei niezgodnych z interesem państwa);
  - uaktywnianie i nasilanie w społeczeństwie postaw agresywnych, radykalnych, defetystycznych;
  - wzbudzanie konfliktów społecznych w wyniku agresywnych oddziaływań informacyjnych;
  - tworzenie i oddziaływanie agentury wpływu;
  - wpływanie na morale społeczeństwa w sposób, rzutujący negatywnie na polityczno-militarne procesy decyzyjne;
- związane z funkcjonowaniem w cyberprzestrzeni, obejmujące m.in.:
  - dezinformację, trolling, wrogą propagandę;
  - ataki na sieci teleinformatyczne sektorów i instytucji o dużym stopniu wrażliwości (w tym wchodzących w skład infrastruktury krytycznej państwa);
  - istnienie niezabezpieczonych luk, dających możliwości ingerencji (także utajonej) w treści zamieszczane na portalach internetowych oraz wpływania na zdolności do działania w cyberprzestrzeni;
- związane z przestrzenią medialną, takie jak:
  - monopolizacja rynku informacyjnego i jego poszczególnych segmentów;
  - niekontrolowany rozwój rynku informacyjnego, w tym przejmowanie lub finansowanie mediów przez podmioty nieprzychylne lub wrogie danemu państwu;
  - pojawianie się w przestrzeni informacyjnej mediów propagujących idee sprzeczne z racją stanu;
  - działalność nieprzyjaznych (wrogich) podmiotów w mediach społecznościowych ukierunkowana na propagowanie treści sprzecznych z interesem narodowym;
  - nieświadome (niezamierzone) rozpowszechnianie celowo podsuwanych przekazów informacyjnych sprzecznych z interesem narodowym przez użytkowników mediów społecznościowych lub media masowe.

W aspekcie zewnętrznym zagrożenia bezpieczeństwa informacyjnego można podzielić na:

- zagrożenia o charakterze podstawowym, obejmujące:
  - deformowanie treści oraz wprowadzanie do systemów informacyjnych za pomocą oficjalnych kanałów nieprawdziwych treści logicznych;
  - destruktywną działalność służb specjalnych i podmiotów informacyjnych innych państw oraz aktorów niepaństwowych;
  - różne formy wrogiej aktywności struktur informacyjno-propagandowych aktorów państwowych i pozapaństwowych (w tym działalność propagandowa i dezinformacyjna);
  - utrata możliwości wpływania na środowisko informacyjne oraz dystrybucji informacji w tym środowisku;
- zagrożenia o charakterze poważnym, obejmujące:
  - niepożądane, zewnętrzne oddziaływania informacyjne wpływające na procedury sterowania procesami decyzyjnymi państwa;
- zagrożenia związane z niedoskonałościami funkcjonowania społeczeństwa obywatelskiego:
  - inspirowane z zewnętrz działania informacyjne podmiotów wewnętrznych mające na celu wywoływanie i pogłębianie podziałów społecznych i politycznych;
  - wsparcie zewnętrzne dla podmiotów wewnętrznych realizujących politykę przeciwnika (przeciwników);
- zagrożenia związane z funkcjonowaniem państwa w stosunkach międzynarodowych:
  - dezinformowanie obywateli innych państw (w tym zwłaszcza tych ze wspólnot organizacyjnych) w kwestiach dotyczących polityki zagranicznej danego państwa;
  - wywoływanie eskalacji napięć w stosunkach bilateralnych i multilateralnych;
  - kształtowanie negatywnego wizerunku danego państwa na arenie międzynarodowej;
  - wzbudzanie w społeczeństwach i elitach politycznych innych państw negatywnych nastrojów wobec danego państwa;
  - dyskredytowanie polityki zagranicznej państwa na arenie międzynarodowej;
  - działanie zagranicznych struktur informacyjnych przeciwko interesom państwa;

– szerzenie treści antypaństwowych za pośrednictwem mediów o zasięgu międzynarodowym i tworzenie w obiegu informacyjnym negatywnego obrazu danego państwa;

- zagrożenia związane z funkcjonowaniem w globalnej cyberprzestrzeni:
  – ataki cybernetyczne na instytucje rządowe i pozarządowe kształtujące świadomość narodową;
  – blokowanie rządowych przekazów informacyjnych na drodze ataków cybernetycznych[217].

Wspomniany wcześniej T.R. Aleksandrowicz podkreśla, że obszerna lista zagrożeń dla informacyjnego wymiaru bezpieczeństwa systematycznie się powiększa m.in. z uwagi na nieustanny rozwój technologii informacyjnych. Autor ten, wyrażając sceptyczne stanowisko wobec możliwości stworzenia zamkniętego katalogu zagrożeń dla bezpieczeństwa informacyjnego, jako podstawowe ich kategorie wymienia:

– brak dostępu do informacji;
– nadmiar informacji;
– opieranie się na informacji fałszywej i dezinformacji;
– nieskuteczną ochronę własnych zasobów informacyjnych;
– niekontrolowanie własnych kanałów informacyjnych[218].

Zdaniem Andrzeja Żebrowskiego i Wojciecha Kwiatkowskiego uzasadniony jest podział zagrożeń bezpieczeństwa informacyjnego na:

– wewnętrzne – powstające wewnątrz danego podmiotu (organizacji), obejmujące utratę, uszkodzenie, modyfikację informacji i danych z powodu niezamierzonego (błędnego, przypadkowego) lub celowego działania ich użytkowników;
– zewnętrzne – powstające poza danym podmiotem (organizacją), obejmujące utratę, uszkodzenie danych i informacji lub pozbawienie możliwości posługiwania się nimi w wyniku przypadkowego bądź celowego działania ze strony podmiotów (osób) trzecich;
– fizyczne, w których utrata, uszkodzenie danych lub brak możliwości obsługi powstaje w rezultacie wypadku, awarii, katastrofy lub innego nieprzewidzianego zdarzenia[219].

---

[217] Zob. *Doktryna bezpieczeństwa informacyjnego*…, s. 6–8.
[218] Zob. T.R. Aleksandrowicz, *Bezpieczeństwo informacyjne*…., s. 45–46.
[219] Zob. A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Kraków 2000, s. 65.

Dla uzupełnienia takiego zestawienia wspomniani powyżej autorzy dodają, że największe zagrożenie dla bezpieczeństwa informacyjnego stanowią różnorodne formy działalności ludzkiej będące często wynikiem kumulacji motywu, środka realizacji oraz okazji[220]. W ramach podsumowania powyżej przedstawionego przeglądu różnorodnych kategoryzacji zagrożeń dla bezpieczeństwa informacyjnego można przyjąć, że podstawowymi ogólnymi rodzajami zagrożeń dla bezpieczeństwa informacyjnego są: deficyt informacji, nadmiar (niekontrolowany zalew) informacji, nieuprawnione ujawnianie informacji chronionych, naruszanie praw obywatelskich w sferze informacyjnej, manipulowanie przekazem informacji, dezinformacja, przestępstwa informacyjne, walka informacyjna oraz wojna informacyjna.

Jeżeli rozpatrywać zagrożenia bezpieczeństwa informacji, to Piotr Zaskórski i Krzysztof Szwarc, prowadząc rozważania dotyczące bezpieczeństwa zasobów informacyjnych w kontekście wykorzystania informatycznych systemów wspomagających zarządzanie, formułują pogląd, że przez to pojęcie należy rozumieć „wszystkie możliwe działania skierowane na elementy systemu informacyjnego (SI), które mogą spowodować szkody – w przypadku istnienia określonej podatności”[221]. W świetle definicji, którą posługuje się Najwyższa Izba Kontroli, zagrożenie bezpieczeństwa informacji to „potencjalna przyczyna zdarzenia, incydentu naruszenia bezpieczeństwa informacji, którego skutkiem może być szkoda (strata) dla organizacji”[222]. W kontekście tych bardzo ogólnikowych ujęć istoty zagrożeń bezpieczeństwa informacji celowym jest zaproponowanie, aby zagrożenia te traktować jako występujące w wielopostaciowych (prostych i złożonych) formach działania, zjawiska i procesy (tak intencjonalne, jak i nieintencjonalne), które wywierają destruktywny, zniekształcający, niezgodny z prawem czy w jakikolwiek inny niekorzystny dla posiadacza lub odbiorcy informacji wpływ na ich jakość i dostępność.

Według Doroty Fleszer silnie umocowaną w literaturze przedmiotu klasyfikacją zagrożeń bezpieczeństwa informacji jest ta oparta na kryterium położenia ich źródeł. Obejmuje ona zagrożenia:

---

[220] Zob. tamże, s. 63–64.

[221] P. Zaskórski, K. Szwarc, *Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki” 2013, nr 9, s. 42.

[222] *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego. Informacja o wynikach kontroli*, Najwyższa Izba Kontroli, Departament Administracji Publicznej, KAP.430.020.2018, Nr ewid. 187/2018/P/18/006/KAP, Warszawa 2018, s. 5.

– wewnętrzne, powstające wewnątrz danego podmiotu i obejmujące przypadki utraty, uszkodzenia lub braku dostępu do danych zaistniałe wskutek błędów, zdarzeń przypadkowych albo celowych działań użytkowników;
– zewnętrzne, powstające poza danym podmiotem i obejmujące utratę, uszkodzenie danych lub pozbawienie możliwości korzystania z nich na skutek celowego lub przypadkowego oddziaływania ze strony osób trzecich w stosunku do sieci lub systemu, w którym są przechowywane;
– fizyczne, w przypadku których utrata, uszkodzenie danych lub brak możliwości posługiwania się nimi następuje w wyniku wypadku, awarii, katastrofy lub innych nagłych zdarzeń zakłócających funkcjonowanie systemów informacyjnych bądź urządzeń sieciowych[223].

W przedstawionej powyżej koncepcji należy dostrzec dość istotną wadę, polegającą na próbie opisu zagrożeń bezpieczeństwa informacji poprzez przedstawianie zagrożeń dla danych, które w swej czystej postaci nie stanowią informacji.

W zbliżony sposób (chociaż bez powyżej zasygnalizowanej ułomności) kwestię podziału zagrożeń dla bezpieczeństwa informacji traktują Michał Pałęga, Marcin Knapiński i Dariusz Rydz. Wymienieni autorzy rozróżniają:

– zagrożenia wewnętrzne (m.in. działanie pracownika, awarię systemu komputerowego);
– zagrożenia zewnętrzne (m.in. ataki typu DDoS [*Distributed Denial of Service* – rozproszona odmowa usług])[224].

Posługując się miarą przyczyn powstawania, przywoływani wyżej badacze dzielą zagrożenia na te będące następstwem działania ludzi i te stanowiące skutek oddziaływania środowiska naturalnego. Wśród zagrożeń związanych z czynnikiem ludzkim wymieniają zagrożenia przypadkowe, wynikające z błędu, pomyłki, braku świadomości oraz celowe (umyślne). Z kolei do zagrożeń środowiskowych zaliczają m.in. powodzie, pożary, wyładowania atmosferyczne, trzęsienia ziemi[225].

---

[223] Zob. D. Fleszer, *Wokół problematyki bezpieczeństwa informacji*, „Roczniki Administracji i Prawa" 2018, nr 1, s. 190.
[224] Są to jedne z najczęściej występujących ataków hakerskich kierowanych na systemy komputerowe lub usługi sieciowe, mające na celu zajęcie wszystkich dostępnych i wolnych zasobów w celu uniemożliwienia funkcjonowania całej usługi w sieci Internet.
[225] Zob. M. Pałęga, M. Knapiński, D. Rydz, *Identyfikacja i ocena zagrożeń bezpieczeństwa informacji za pomocą wybranych instrumentów zarządzania jakością,* [w:] *Innowacje w zarządzaniu i inżynierii produkcji*, R. Knosala (red.), t. II, Opole 2018, s. 286.

Inne spojrzenie na klasyfikację zagrożeń bezpieczeństwa informacji prezentują Jakub Kowalewski i Marian Kowalewski. Wymienieni badacze sformułowali listę zagrożeń, na której umieścili:

– siły wyższe,
– uchybienia organizacyjne,
– błędy ludzkie,
– błędy techniczne,
– działania rozmyślne.

W opisie przedstawionej listy zagrożeń dla bezpieczeństwa informacji przywoływani autorzy zaznaczyli, że terminu „siły wyższe" używają na określenie zbioru zagrożeń bezpieczeństwa informacji i systemów teleinformatycznych o charakterze obiektywnym, na które ich użytkownik nie ma większego i bezpośredniego wpływu. Z kolei uchybienia organizacyjne stanowią grupę zagrożeń bezpieczeństwa informacji powstających w wyniku złego zorganizowania i funkcjonowania instytucji (dotyczy to zwłaszcza procesu przetwarzania informacji). Błędy ludzkie rozumiane są jako zagrożenia powstałe w efekcie niecelowej działalności człowieka, natomiast błędy techniczne to zagrożenia związane z urządzeniami technicznymi i niewłaściwym ich wykorzystywaniem. Ostatnie na liście działania rozmyślne w optyce przywoływanych autorów oznaczają celową działalność ludzką zmierzającą do przechwytywania i modyfikowania informacji oraz danych, a także do zakłócania lub uniemożliwiania ich transferu[226]. Warto w ramach prowadzonego przeglądu podziałów zagrożeń dla bezpieczeństwa informacji przedstawić także ogólną ich klasyfikację występującą w dokumentach Najwyższej Izby Kontroli, według której główne zagrożenia dla bezpieczeństwa informacji to:

– brak podejścia systemowego do kwestii zapewnienia bezpieczeństwa informacji,
– nieprowadzenie audytów bezpieczeństwa informacji,
– brak analiz ryzyka w zakresie bezpieczeństwa informacji
– nieprzestrzeganie ustanowionych wymogów w zakresie bezpieczeństwa informacji[227].

[226] Zob. J. Kowalewski, M. Kowalewski, *Polityka bezpieczeństwa informacji w praktyce*, Wrocław 2014, s. 27–30.
[227] Zob. *Zarządzanie bezpieczeństwem informacji…*, s. 7.

P. Zaskórski oraz K. Szwarc zagrożenia dla bezpieczeństwa informacji dzielą na będące:

– wytworem celowych działań ludzkich o charakterze terrorystycznym, przestępczym, dywersyjnym lub sabotażowym;
– rezultatem nieświadomego, błędnego wykorzystywanie elementów systemu informacyjnego, w tym m.in. posługiwanie się niewłaściwie sformułowanymi procedurami;
– wynikiem szkodliwego oddziaływania sił natury, zwłaszcza klęsk żywiołowych;
– skutkiem awarii sprzętu komputerowego i błędów (wad) oprogramowania[228].

Rozbudowaną, ale interesującą specyfikację zagrożeń dla bezpieczeństwa informacji przedstawiła Estera Pietras[229]. Klasyfikacja ta mimo szeregu istotnych błędów formalnych (np. zamienne stosowanie terminu „dane" i „informacja"), nieczytelności i braku precyzji stosowanego języka (np. użyte w p. 12 tabeli 7 sformułowanie „Niedobór informacji w świadomości opracowania planu bezpieczeństwa informacji") jest inspirująca[230]. W spojrzeniu cytowanej autorki uwzględnione są (co należy uznać za jak najbardziej uzasadnione) nie tylko zagrożenia wynikające z przetwarzania informacji w systemach informatycznych, ale również te związane z niewłaściwym działaniem ludzi.

W rezultacie przeprowadzonych analiz i dokonanych na ich bazie uogólnień można przyjąć istnienie dwóch podstawowych wymiarów zagrożeń dla bezpieczeństwa informacji – o charakterze antropogenicznym oraz środowiskowo-technicznym. W grupie zagrożeń antropogenicznych wskazać trzeba przede wszystkim na:

– wytwarzanie i rozpowszechnianie informacji niskiej jakości (niepewnej, niepełnej);
– błędy i braki w percepcji i dystrybucji dobrej jakościowo i ważnej informacji;
– fałszowanie informacji;
– kradzież informacji;

[228] Zob. P. Zaskórski, K. Szwarc, *Bezpieczeństwo zasobów informacyjnych…*, s. 42.
[229] Zob. tabela 7.
[230] Przywołana tabela 7 została zgodnie z zasadami poprawnego cytowania przedstawiona w wersji oryginalnej, ze wszystkimi niedoskonałościami, w tym także interpunkcyjnymi i językowymi.

– niszczenie informacji;
– manipulowanie informacją;
– ukrywanie informacji;
– utratę informacji;
– wykorzystywanie informacji nieaktualnej.

W grupie zagrożeń środowiskowo-technicznych dominują:

– utrata lub dekompletacja informacji jako efekt destrukcyjnych działań sił przyrody (powodzie, trzęsienia ziemi, huragany itp.);
– utrata lub fragmentaryzacja informacji w wyniku awarii sprzętu komputerowego;
– generowanie informacji złej jakości w wyniku błędów w oprogramowaniu.

Tabela 7. Identyfikacja zagrożeń bezpieczeństwa informacji

Nazwa zagrożenia		Przyczyna	Skutek
1	Kradzież danych	Brak zabezpieczeń	Wydostanie się danych do konkurencji. Utrata konkurencyjności.
2	Włamania do systemu komputerowego	Ignorowanie zasady korzystania z poczty elektronicznej. Instalowanie nielegalnego oprogramowania.	Brak zaufania kontrahentów. Kradzież danych.
3	Nieprzestrzeganie regulaminu obowiązującego w firmie	Brak zrozumienia przepisów. Nieprzestrzeganie regulaminów.	Narażenie danych na utratę, zmodyfikowanie.
4	Przekroczenie uprawnień	Pochopne wydawanie uprawnień w systemach informatycznych. Brak wyciągania konsekwencji za przekroczenie uprawnień.	Nieuprawniony dostęp do informacji w wyniku tego straty finansowe firmy.
5	Awaria sprzętu	Kupno uszkodzonego sprzętu. Nieumiejętne użytkowanie.	Ograniczony dostęp do danych organizacji. Zakłócenia w procesie realizacji procesów.
6	Złamanie haseł	Nieprzestrzeganie zasad czystego biurka i pulpitu. Niewłaściwe tworzenie zasad.	Upowszechnianie haseł. Kradzież danych.

7	Kradzież nośników danych, dokumentów	Wynoszenie danych, nośników poza siedzibę firmy. Kontrahenci pozostawieni bez opieki.	Wyciek informacji do firm konkurencyjnych, w wyniku tego straty finansowe.
8	Awaria łączności systemu komputerowego	Nieodpowiednie użytkowanie systemu. Brak legalnego oprogramowania. Uszkodzenie podzespołów.	Zakłócenia związane z komunikacją. Brak możliwości poprawnej realizacji procesów.
9	Nieprawidłowe działania oprogramowania	Brak odpowiedniego nadzoru nad oprogramowaniem. Nieumiejętne korzystanie z oprogramowania.	Przekłamanie w działaniu, zapisywaniu i przetwarzaniu informacji.
10	Odtworzenie danych z odnalezionych nośników danych	Zagubienie, zniszczenie, nośników informacji.	Modyfikacja, niekontrolowane rozpowszechnianie danych.
11	Nieodpowiednie przygotowanie umowy z personelem i kontrahentami firmy i dostawcami	Brak świadomości zarządu.	Wykorzystanie informacji w wyniku tego strata pozycji na rynku.
12	Brak zapewnienia bezpieczeństwa informacji w przedsiębiorstwie	Niedobór informacji w świadomości opracowania planu bezpieczeństwa informacji.	Wyciek i kradzież informacji. Narażenie aktywów informatycznych na ich utratę.
13	Brak szkoleń dla kadry pracowników z zakresu bezpieczeństwa informacji	Brak świadomości kierownictwa. Brak finansów.	Nieświadome narażenie danych na ich stratę.
14	Wykorzystanie informacji udostępnionych firmie	Brak świadomości kierownictwa. Brak finansów.	Utrata pozycji na rynku, w wyniku strata części klientów.

Źródło: E. Pietras, *Szacowanie ryzyka utraty bezpieczeństwa informacji na przykładzie wybranej jednostki gospodarczej*, www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2017/T1/t1_088.pdf [dostęp: 6.06.2020 r.].

W konsekwencji zaistnienia zagrożeń dla bezpieczeństwa informacji powstających na gruncie różnie skonfigurowanych sytuacji, zdarzeń i działań, o których wspominano wcześniej, podmiot korzystający, wytwarzający czy przetwarzający informację może mieć do czynienia z:

– informacją niepełną;
– informacją niewiarygodną (niepewną);

– informacją zmanipulowaną;
– informacją sfałszowaną;
– informacją nieczytelną;
– informacją pozyskaną nielegalnie.

Konkludując, należy podkreślić, że swobodny dostęp i obrót informacją jako podstawa bezpieczeństwa informacyjnego wiąże się z szeregiem niebezpieczeństw, na jakie narażeni są wytwórcy użytkownicy i posiadacze informacji. Zagrożenia te mają różną skalę i wywołują różne skutki. Żeby efektywnie je rozpoznawać, przeciwdziałać i minimalizować powodowane przez nie ograniczenia i straty, niezbędne są coraz bardziej zaawansowane działania oparte nie tylko na rozwiązaniach technicznych i organizacyjnych, ale w coraz większej mierze na budowaniu odpowiedniego poziomu świadomości jej wytwórców i użytkowników. Trzeba pamiętać jednocześnie, że żadna z istniejących list zagrożeń bezpieczeństwa informacyjnego oraz bezpieczeństwa informacji (w tym również przedstawione powyżej) nie jest listą zamkniętą. Wykaz wspomnianych zagrożeń z pewnością ulegał będzie systematycznej modyfikacji. W związku z tym ważnym zadaniem każdego dbającego o swoje bezpieczeństwo podmiotu jest ciągłe monitorowanie zagrożeń związanych z jego środowiskiem informacyjnym, tak wewnętrznym, jak i zewnętrznym, nie tylko pod kątem ilościowym, ale także jakościowym. Jest to szczególnie ważne w społeczeństwie bazującym na danych i informacjach, które tworzą podstawy jego rozwoju i sukcesów, ale mogą zostać wykorzystane także w celu zachwiania jego bezpieczeństwem. Trzeba przy tym uwzględniać fakt, że ciągle powstają nowe programy oraz narzędzia informatyczne, znajdujące się w masowym użytkowaniu, z których część może być wykorzystywana do działań zagrażających bezpieczeństwu. Analizując kwestię zagrożeń bezpieczeństwa informacyjnego, należy podkreślić, że we współczesnych realiach, przy ciągle wzrastającym tempie i ilości wytwarzanej i wprowadzanej do obiegu informacji, nie tylko jednostki, ale i duże organizacyjnie podmioty nie poradzą sobie z nimi bez udziału państwa (a w wielu kwestiach także bez zaangażowania wspólnot międzynarodowych). Bardzo ważny jest tu czynnik czasu, który przy lawinowym przyroście informacji nie daje większych możliwości działania na rzecz bezpieczeństwa bez odpowiedniego zaplecza analitycznego, technicznego czy legislacyjnego, a takim dysponuje tylko państwo.

Warto zauważyć również, że większość publikacji i wypowiedzi ekspertów, zawierających sensowne pomysły na przeciwdziałanie i ograniczanie skutków zagrożeń informacyjnych, pokłada zbyt duże nadzieje w aktywności

jednostek, pomniejszając znaczenie działań organów i instytucji państwa. Nie lekceważąc roli świadomości i odpowiednich (sprzyjających zachowaniu bezpieczeństwa informacyjnego) zachowań indywidualnych, należy podkreślić, że współczesna specyfika zagrożeń informacyjnych powoduje, że skutecznie nie da się ich ograniczać bez dużego zaangażowania służb i instytucji państwowych. Tylko bowiem one są w stanie uruchomić odpowiednie zasoby, aby adekwatnie do rzeczywistej skali zagrożeń, monitorować je, dokonywać analiz ryzyk z nimi związanych, prowadzić strategiczne analizy ich rozwoju wraz z mapowaniem rozmieszczenia, dokonywać planowania scenariuszowego oraz opracowywać i wdrażać odpowiednie algorytmy postępowania w celu ich zwalczania. Także szybka identyfikacja potencjalnych zagrożeń na gruncie teoretycznym pozwoli na modyfikację oraz ulepszenie istniejących rozwiązań tak, aby skuteczniej eliminować bądź zmniejszać prawdopodobieństwo wystąpienia któregoś z nich, a tym samym tworzyć właściwe podstawy do osiągania odpowiedniego poziomu (tak jednostkowego, jak i systemowego) bezpieczeństwa informacji i bezpieczeństwa informacyjnego. Co istotne, mając dobrze rozpoznany, sklasyfikowany i opisany katalog zagrożeń, można także precyzyjniej, w ujęciu tak bieżącym, jak i perspektywicznym, planować realizację działań dotyczących ochrony i obrony przed nimi.

3.2. Przestępstwa i przestępczość informacyjna

Bezpieczeństwo informacyjne oparte na takich filarach, jak szeroki dostęp do wysokiej jakości informacji, nieskrępowany jej obieg oraz skuteczna ochrona informacji ważnych z punktu widzenia bezpieczeństwa państwa, a także bezpieczeństwa jednostek to jeden z podstawowych atrybutów współczesnych państw liberalno-demokratycznych. W świetle dotychczas zgromadzonych doświadczeń praktycznych oraz ocen i ustaleń naukowych można zauważyć, że im więcej wysokiej jakości informacji krąży w dostępnym dla wszystkich zainteresowanych obiegu, tym bardziej wzrastają możliwości podnoszenia efektywności procesów decyzyjnych i rozwojowych. Szczególnie ważne jest w tym kontekście zapewnienie przejrzystości życia publicznego oraz odpowiedniego poziomu kontroli działalności władz państwowych. Bardzo istotne jest również to, że obywatele posiadający odpowiedni do potrzeb dostęp do informacji mają szanse na optymalizację swoich decyzji tak w zakresie sfery życia osobistego, jak i publicznego (politycznego,

gospodarczego, kulturalnego itp.). Ponieważ bezpieczeństwo informacyjne i wiążące się z nim bezpieczeństwo informacji systematycznie zyskuje na znaczeniu, we współczesnym społeczeństwie stale wzrasta potrzeba zwiększania wysiłków na rzecz jego zapewnienia.

Naszkicowana powyżej ocena istniejącej sytuacji oraz trendów przyszłościowych czyni szczególnie ważnymi działania związane ze zwalczaniem i zapobieganiem przestępczości wymierzonej w sektor bezpieczeństwa informacyjnego. Dla zwiększenia ich efektywności niewątpliwie strategiczne znaczenie posiada wypracowywanie i podejmowanie odpowiednich inicjatyw legislacyjnych. Jest to znacznie utrudnione ze względu na istnienie niejednorodnej i nie zawsze odpowiadającej potrzebom współczesności siatki pojęciowej z obszaru bezpieczeństwa informacyjnego. W związku z tym konieczne jest, na drodze badań naukowych, ciągłe identyfikowanie, opisywanie, analizowanie, objaśnianie oraz porządkowanie i modyfikowanie terminów związanych z tym obszarem bezpieczeństwa Aby jednak dokonać tego w sposób racjonalny i efektywny, trzeba w pierwszej kolejności w miarę precyzyjnie zdefiniować pojęcia ogólne, które będą stanowić bazę do poprawnej identyfikacji pojęć szczegółowych. Za szczególnie ważne w świetle powyższych uwag należy uznać zdefiniowanie i wprowadzenie do obiegu naukowego terminów „przestępstwo informacyjne" oraz „przestępczość informacyjna". Niewątpliwie waga czynów karalnych dotyczących infosfery[231] znajduje już swoje odzwierciedlenie w ustawodawstwie, które obejmuje rozległy katalog przestępstw w różnym zakresie skierowanych przeciwko informacji lub dokonanych z niewłaściwym jej wykorzystaniem. Są one jednak rozproszone w dużej ilości aktów prawnych. Należy w tym miejscu podkreślić, że wzrost znaczenia informacji nie tylko zaowocował nadaniem jej statusu autonomicznego dobra prawnego, ale spowodował także inne reakcje ze strony przedstawicieli nauk prawnych. Część z nich zaczęła wyróżniać nową gałąź prawa – „prawo informacyjne". Stanowisko takie uznać należy za uzasadnione, mimo że materia zainteresowań tej będącej *in statu nascendi* dziedziny prawa egzystuje na pograniczu innych gałęzi prawa lub zawiera się w kilku

[231] Infosfera – dla przypomnienia – to według poglądu Luciano Floridi środowisko informacyjne, na które składają się wszystkie podmioty informacyjne, a także czynniki informacyjne, ich własności, interakcje, procesy i wzajemne relacje. Środowisko to bywa często niesłusznie utożsamiane z cyberprzestrzenią (jest ona tylko jednym z jej składników), ponieważ obejmuje także przestrzenie informacji dostępne analogowo i offline. Zob. L. Floridi, *A look in to the future impact of ICT on our lives,* „The Information Society" 2007, no. 23, p. 59.

z nich jednocześnie. Jak wskazuje Krystyna Celarek, w ramach wyodrębniania prawa informacyjnego uporządkowanie przypisywanej mu materii to zadanie niełatwe. Szczególne trudności wiążą się z uchwyceniem specyfiki informacji i uwzględnieniem jej wielowymiarowości[232]. Jednak, jak zauważa Friedrich Schoch, pokonanie tej przeszkody jest „nieodzowne, aby idea wyraźnego wyodrębnienia prawa informacyjnego mogła zostać zrealizowana"[233]. Jednocześnie F. Schoch wskazuje, że współcześnie możliwość wyróżnienia „prawa informacyjnego" jako dziedziny prawa jest już bezsprzeczna. Dowodem na to są regulacje ustawowe dotykające różnych zagadnień w istotnych obszarach cząstkowych dotyczących informacji. Również w doktrynie wykrystalizował się pogląd, że „informacja" może stanowić przedmiot regulacji prawnej. Nie bez znaczenia, jak stwierdza przywoływany badacz, jest także fakt istnienia szeregu solidnych i innowacyjnych prac naukowych stanowiących dobrą podbudową do kodyfikacji prawa informacyjnego. W jednoznacznie pozytywnej opinii F. Schocha dotyczącej niezbędności wyodrębnienia prawa informacyjnego zaletą takiego rozwiązania jest zapewnienie przejrzystości, zrozumiałości, racjonalizacji i ujednolicenia informacyjnej materii prawnej i nadanie jej systemowej spójności[234]. W podobnym tonie wypowiada się Irena Lipowicz, która w kontekście rozwoju zagrożeń generowanych przez nieodpowiednie zastosowania nowoczesnych technologii informacyjnych stwierdza, że jest to podstawa do zmian regulacji prawnych oraz że „prawo informacyjne nabiera w ten sposób konturów i zmienia swą rolę: z dość wyspecjalizowanej, niemal peryferyjnej części prawa publicznego do dyscypliny doniosłej dla przyszłości demokratycznego państwa prawnego. Uznanie jego roli zbiega się z diagnozą szczególnej trudności regulacji ze względu na płynność materii, szybkie zmiany"[235]. Potwierdza takie stanowisko i je rozwija cytowana już wcześniej K. Celarek, która wskazuje na to, że wyodrębnienie prawa informacyjnego, a także w dalszej perspektywie czasowej jego kodyfikacja, stworzy szereg pozytywnych szans dla regulowanej materii. Wspomniane szanse wiążą się przede wszystkim z:

---

[232] Zob. K. Celarek, *Prawo informacyjne. Problem badawczy teorii prawa administracyjnego*, Warszawa 2013, s. 104.

[233] F. Schoch, *Zagadnienie równowagi między wolnością informacyjną a ochroną danych w niemieckim profesorskim projekcie Kodeksu Informacyjnego*, [w:] *Internet. Ochrona wolności, własności i bezpieczeństwa*, G. Szpor (red.), Warszawa 2011, s. 20.

[234] Tamże, s. 25–27.

[235] I. Lipowicz, *Nowe wyzwania w zakresie ochrony danych osobowych,* [w:] *Internet. Ochrona wolności…,* s. 8.

– przeniesieniem istniejących już regulacji cząstkowych do kodeksu informacyjnego, czemu może towarzyszyć innowacja treściowa[236];
– osiągnięciem, dzięki stworzeniu ogólnych przepisów regulujących kompleksowo różne dziedziny, treściowego zazębienia charakteryzującej się dużym rozproszeniem materii prawa informacyjnego[237];
– tym, że treści informacyjne dotychczas nieuregulowane lub uregulowane jedynie cząstkowo uzyskają odpowiedni fundament normatywny[238].

Jak wskazuje Grażyna Szpor (powołująca się na ustalenia holenderskich badaczy Willema F. Korthalsa Altesa, Egberta J. Dommeringa, Petera B. Hugenholtza oraz Jana Jakuba C. Kabla), w Europie Zachodniej prawo informacyjne zaczęto wyodrębniać z systemu prawa już w latach 90. XX w. Jego zakres, charakteryzowany głównie przez fazy procesów informacyjnych, takich jak konwersja, przekaz i odtwarzanie, nie był jednak wyczerpujący[239]. Według F. Schocha „prawo informacyjne (w wąskim sensie) obejmuje całość norm prawnych, które zajmują się w szczególny sposób pozyskiwaniem (generowaniem, wytwarzaniem), udostępnianiem i izolowaniem, przetwarzaniem i rozpowszechnianiem informacji jako takich"[240]. Celem tak wyodrębnionego prawa informacyjnego jest zapewnienie sprawiedliwości informacyjnej[241] oraz uporządkowanie informacyjnej sfery życia[242]. Wymieniana już wcześniej K. Celarek w pogłębionej analizie, w której przekonywująco dowodzi konieczności wyodrębniania prawa informacyjnego, wskazuje na „rozumienie go jako pojęcia zbiorczego obejmującego i prawo do informacji, i informacje o obowiązującym prawie,

[236] Jako przykład takich szans autorka podaje prawo ochrony danych: stworzenie jednakowych standardów dla organów publicznych i podmiotów niebędących organami publicznymi, systematyczne przetwarzanie wymagań prawa europejskiego, wzmocnienie mechanizmów samoregulacji itd.
[237] Tu jako przykład autorka wskazuje prawo ochrony tajemnic, prawo ewidencji i rejestracji oraz prawo dostępu do informacji.
[238] Zob. K. Celarek, dz. cyt., s. 106.
[239] Zob. G. Szpor, *Prawo informacyjne*, http://wikiprawna.com.pl/index.php?title=prawo_informacyjne [dostęp: 28.12.2020 r.].
[240] F. Schoch, dz. cyt., s. 25.
[241] Sprawiedliwość informacyjna to ogólna, merytoryczna linia wiodąca prawa informacyjnego. Oparta jest przede wszystkim na zapewnieniu dostępu do informacji urzędowych, oszczędnym i ostrożnym formułowaniu katalogu okoliczności uzasadniających odmowę dostępu do informacji oraz starannym balansowaniu interesów informacyjnych i ochronnych. Zob. F. Schoch, dz. cyt., s.19.
[242] Zob. tamże.

i obowiązki informacyjne administracji publicznej, i ochronę informacji"[243]. Jedną z możliwości, jakie daje wyodrębnienie prawa informacyjnego, jest możliwość wypracowania i określenia zakresu pojęć „przestępstwo informacyjne" oraz „przestępczość informacyjna".

W praktyce zbiorczego terminu „przestępstwa informacyjne", zdaniem autora, można zacząć używać w odniesieniu do następujących rodzajów przestępstw:

– przestępstw przeciwko ochronie informacji;
– przestępstw przeciwko wiarygodności dokumentów;
– przestępstw przeciwko prawom autorskim;
– przestępstw przeciwko ochronie danych osobowych;
– przestępstw przeciwko prawom własności przemysłowej;
– przestępstw przeciw znakom towarowym;
– przestępstw przeciw informacji publicznej;
– przestępstw przeciwko tajemnicom zawodowym i innym tajemnicom prawnie chronionym;
– cyberprzestępstw[244].

Jeżeli rozpatrywać przestępczość wymierzoną w ochronę informacji, to każde racjonalnie i demokratycznie rządzone państwo, szanując swobody informacyjne określone w ustawie zasadniczej oraz wynikające z prawa międzynarodowego, dba równocześnie (przyjmując stosowne ustawodawstwo) o ochronę informacji, których nieuprawnione ujawnienie mogłoby spowodować szkody dla państwa albo byłoby z punktu widzenia jego interesów niekorzystne. Informacje takie określa się mianem niejawnych. Stopień zabezpieczenia informacji niejawnych jest uzależniony głównie od dokonanej ich klasyfikacji. Jej konsekwencją jest zaopatrzenie informacji niejawnych w odpowiednie klauzule poufności. Informacja, której nadano taką klauzulę, ma charakter niejawny, co pociąga za sobą skutki w zakresie odpowiedniego z nią postępowania w okresie ochronnym. W szczególności może być ona dostępna wyłącznie dla osób posiadających stosowne uprawnienia[245]. Ogólne regulacje dotyczące zasad ochrony informacji niejawnych reguluje w Polsce ustawa

[243] K. Celarek, dz. cyt., s.11.
[244] Należy zauważyć, że brak uzgodnionej definicji „cyberprzestępczości" powoduje, że zamiennie często stosowane są również pojęcia: „przestępczość komputerowa „ „przestępczość związana z komputerami" czy „przestępczość przy użyciu zaawansowanych technologii".
[245] Zob. D. Kamuda, *Wybrane aspekty przestępczości skierowanej przeciwko informacjom niejawnym – art. 265 i 266 k.k.*, „Modern Management Review" 2018, nr 1, s. 85.

z dnia 5 sierpnia 2010 r.[246], natomiast penalizacja czynów naruszających zasady wspomnianej ochrony dokonana została w ramach Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny. Opierając się na przepisach rozdziału XXXIII[247] oraz art. 133[248] Kodeksu karnego wyspecyfikować można następujące przestępstwa przeciwko ochronie informacji:

– ujawnienie lub wykorzystanie tajemnicy państwowej;
– bezprawne uzyskanie informacji;
– udaremnianie lub utrudnianie zapoznania się z informacją;
– wytwarzanie programów komputerowych wykorzystywanych do popełnienia przestępstwa;
– usuwanie, uszkadzanie, niszczenie lub utrudnianie dostępu do danych informatycznych bez stosownych uprawnień;
– szpiegostwo[249].

Kolejna kategoria tworząca grupę przestępstw informacyjnych to przestępstwa przeciw wiarygodności dokumentów ujęte w przepisach rozdziału XXXIV Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny. Należy w tym miejscu podkreślić wyjątkowość prawnego i społecznego znaczenia dokumentów. Jak wskazuje Joanna Piórkowska-Flieger, w obrębie każdej dziedziny prawa prowadzone są różne czynności prawne. Ze względu na ich wagę dla porządku prawnego oraz interes zaangażowanych w te czynności podmiotów są one utrwalane w przewidzianych przepisami prawa formach[250]. Dokumenty, co podkreśla Grzegorz Pieszko, zawierają stwierdzenie określonych faktów (lub faktu) niosących za sobą skutki prawne. Chodzi w związku z tym o to, żeby informacje dokumentujące te fakty odpowiadały rzeczywistości. Jest to bardzo istotne, bowiem w ten sposób następuje utrwalenie

[246] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010, nr 182, poz. 1228 z późn. zm.).
[247] Zob. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. 1997, nr 88, poz. 553 z późn. zm.).
[248] Artykuł ten dotyczy szpiegostwa jako szczególnego przestępstwa tak przeciwko Rzeczypospolitej Polskiej, jak i ochronie informacji.
[249] Przestępstwo szpiegostwa to: udział w działalności obcego wywiadu przeciwko Rzeczypospolitej Polskiej, udział w obcym wywiadzie albo działanie na jego rzecz i udzielanie temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, gromadzenie lub przechowywanie w celu udzielenia obcemu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej oraz wchodzenie do systemu informatycznego w celu ich uzyskania, zgłaszanie gotowości działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej, organizowanie lub kierowanie działalnością obcego wywiadu.
[250] Zob. J. Piórkowska-Flieger, *Prawne i społeczne uzasadnienie karalności fałszu dokumentu,* „Studia Iuridica Lublinensia" 2003, nr 1, s. 145.

oświadczeń woli lub wiedzy człowieka albo jakichkolwiek innych faktów bądź okoliczności mających znaczenie prawne[251]. Dokumentowanie czynności prawnych zapewnia ich przejrzystość i gwarantuje pewność oraz sprawność w obrocie prawnym. Natomiast fałszowanie dokumentów, z którymi łączą się określone zobowiązania i uprawnienia dotyczące różnych sfer stosunków społecznych, gospodarczych, politycznych i innych często skutecznie destabilizuje te sfery tak w ujęciu jednostkowym, jak i zbiorowym. Ukazanie katalogu przestępstw przeciwko wiarygodności dokumentów należy poprzedzić określeniem tego, czym jest dokument. Zgodnie z definicją ustawową „dokumentem jest każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne"[252]. Należy podkreślić, że przedmiotem ochrony jest w tym kontekście publiczne zaufanie do prawdziwości dokumentu oraz zgodności z prawdą treści w nim zapisanych. Jednak, jak słusznie zauważa Piotr Ochman, dla objęcia skuteczną ochroną ze strony prawa karnego dokumentów zarówno w postaci tradycyjnej, jak i tych w formie elektronicznej w każdej fazie ich życia, oraz w celu zapewnienia logicznej poprawności definicji, należy dokonać zmiany jej ustawowej treści. Zgodzić się można w tym miejscu z P. Ochmanem, że jej bardziej przystający do współczesnych potrzeb kształt mógłby być następujący: „Dokument jest to zapis na nośniku danych, z którym jest związane określone prawo albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne"[253]. Jeżeli rozpatrujemy przestępstwa przeciwko wiarygodności dokumentów, to obejmują one;

– podrabianie albo przerabianie dokumentów;
– używanie dokumentów poświadczających nieprawdę;
– niszczenie lub ukrywanie dokumentów;
– zbywanie dokumentów tożsamości;
– niszczenie, usuwanie lub fałszywe wystawianie znaków granicznych;

[251] Zob. G. Pieszko, *Społeczno-prawne aspekty penalizacji fałszowania dokumentów*, „Studia Prawnoustrojowe" 2015, nr 29, s. 174.
[252] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, art. 115.
[253] P. Ochman, *Spór o pojęcie dokumentu w prawie karnym*, „Prokuratura i Prawo" 2009, nr 1, s. 35–36.

– kradzież, posługiwanie się albo przywłaszczenie dokumentów potwierdzających tożsamość lub prawa majątkowe innej osoby;
– poświadczenie lub wyłudzenie poświadczenia nieprawdy.

Istotną kategorię przestępstw, które należałoby włączyć do grupy przestępstw informacyjnych, stanowią przestępstwa przeciwko prawom autorskim. W opinii Janusza Barty i Ryszarda Markiewicza naruszenie praw autorskich to „takie działanie, które można kwalifikować jako wkroczenie w zakres cudzego prawa majątkowego (monopolu eksploatacyjnego na konkretny utwór)”[254]. Najbardziej znanym przejawem łamania praw autorskich jest plagiat (łac. *plagiatus*, skradziony). Najogólniej rzecz ujmując, za plagiat uznaje się przywłaszczenie cudzego utworu w całości bądź w części. Internetowy słownik języka polskiego definiuje plagiat jako ”przywłaszczenie cudzego pomysłu twórczego, wydanie cudzego utworu pod własnym nazwiskiem lub dosłowne zapożyczenie z cudzego dzieła opublikowane jako własne; też: taki przywłaszczony pomysł, wydany utwór lub zapożyczenie”[255]. W ujęciu encyklopedycznym plagiatem jest „przywłaszczenie cudzego utworu, pracy naukowej, dzieła artystycznego itp., także zapożyczenie z cudzych dzieł podane jako własne i opublikowane pod własnym nazwiskiem”[256]. Uogólniając, plagiat to świadome przywłaszczenie cudzego utworu w całości lub w znaczących (istotnych) fragmentach. Za plagiat uznaje się także powtórzenie w mniej lub bardziej zmienionej formie istoty cudzego utworu (przy zatajeniu źródła i twórcy) oraz przedstawienie go jako swojego.

Wyróżnić można plagiat jawny oraz plagiat ukryty. Jawny plagiat to podpisanie się swoim imieniem i nazwiskiem (ewentualnie pseudonimem) pod cudzym, w żaden sposób nie zmienionym dziełem, bez żadnego wkładu własnego do tego dzieła. Plagiat ukryty polega na tym, że przejęte elementy cudzego utworu są mniej lub bardziej przekształcane tak, by wyłapanie podobieństw było utrudnione[257]. Oprócz działań uznawanych za plagiat, o naruszeniu praw autorskich można mówić również w przypadkach obejmujących:

---

[254] J. Barta, R. Markiewicz, *Komentarz do ustawy o prawie autorskim i prawach pokrewnych*, Warszawa 2003, s. 548.
[255] *Słownik język polskiego PWN*, https://sjp.pwn.pl/slowniki/plagiat.html [dostęp: 3.01.2021 r.].
[256] *Encyklopedia PWN*, https://encyklopedia.pwn.pl/haslo/;3957879 [dostęp: 3.01.2021 r.].
[257] Zob. A. Sewerynik, *Plagiat ukryty a wzorowanie się na cudzej twórczości*, https://www.rp. pl/Prawo-autorskie/302289997-Plagiat-ukryty-a-wzorowanie-sie-na-cudzej-tworczosci.html [dostęp: 1.01.2021 r.].

– *ghostwriting* – właściwy autor utworu nie zostaje ujawniony, opublikowanie utworu następuje pod nazwiskiem osoby, która zleciła jego przygotowanie;
– *ghost authorship* – dochodzi do pominięcia na liście autorów osób, które włożyły wkład w opracowanie utworu;
– *honorary authorship* (*guest authorship*) – umieszcza się na liście autorów osoby, które nie wniosły żadnego wkładu w przygotowanie utworu[258].

W odniesieniu do praw autorskich można w świetle aktualnie obowiązujących regulacji[259] wymienić takie rodzaje czynów zabronionych, jak:
– przywłaszczanie autorstwa albo wprowadzanie w błąd co do autorstwa całości lub części utworu albo artystycznego wykonania;
– bezprawne rozpowszechnianie cudzego utworu, artystycznego wykonania, fonogramu, wideogramu lub nadania;
– bezprawne utrwalanie lub zwielokrotnianie (w celu rozpowszechniania) cudzego utworu, artystycznego wykonania, fonogramu, wideogramu lub nadania;
– bezprawne nabywanie, pomoc w zbywaniu, przyjmowanie lub pomaganie w ukryciu, w celu osiągnięcia korzyści majątkowej, przedmiotu (przedmiotów) będących nośnikiem utworu, artystycznego wykonania, fonogramu, wideogramu rozpowszechnianego lub zwielokrotnionego;
– produkcję, obrót, reklamę, posiadanie, przechowywanie lub wykorzystywanie urządzeń lub ich komponentów przeznaczonych do nielegalnego usuwania lub obchodzenia zabezpieczeń przed nielegalnym odtwarzaniem, przegrywaniem lub zwielokrotnianiem;
– uniemożliwianie lub utrudnianie wykonywania prawa do kontroli korzystania z utworu, artystycznego wykonania, fonogramu lub wideogramu albo odmawianie udzielenia informacji mającej istotne znaczenie dla określenia wysokości wynagrodzenia twórcy.

W skład przestępstw informacyjnych włączyć należy również przestępstwa przeciw ochronie danych osobowych. Dane te definiuje się jako informacje, dzięki którym możliwe jest zidentyfikowanie osoby fizycznej. Konieczność ochrony danych osobowych wynika zarówno z respektowania

[258] Zob. *Oszustwa publikacyjne i naruszenia praw autorskich,* https://www.biblos.pk.edu.pl/nauka/publikowanie-wybrane-aspekty/oszustwa-publikacyjne-i-naruszenia-praw-autorskich [dostęp: 1.01.2021 r.].
[259] Zob. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994, nr 24, poz. 83 z późn. zm.).

obywatelskiego prawa do prywatności, jak i ograniczania ryzyka ich utraty na rzecz osób dokonujących różnorakich przestępstw przy użyciu kradzionych danych osobowych. W przypadku przestępstw przeciwko ochronie danych osobowych to, zgodnie z ustawą z 10 maja 2018 r. o ochronie tych danych, są to czyny polegające na przetwarzaniu:

– danych osobowych, których przetwarzanie jest niedopuszczalne;
– danych osobowych bez prawa przetwarzania tych danych.

Ponadto przestępstwem jest:

– udaremnianie lub utrudnianie kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych;
– niedostarczenie danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej lub dostarczenie danych, które uniemożliwiają ustalenie podstawy wymiaru administracyjnej kary pieniężnej w związku z toczącym się postępowaniem w sprawie nałożenia administracyjnej kary pieniężnej[260].

Sygnalizując konieczność wyodrębnienia przestępstw informacyjnych, należy dostrzec także niezbędność umieszczenia wśród nich przestępstw przeciwko prawom własności przemysłowej. Skala tej przestępczości i generowane w jej wyniku straty systematycznie rosną. Jak wskazuje Urząd Unii Europejskiej do Spraw Własności Intelektualnej (EUIPO)[261] na podstawie badań przeprowadzonych w 2019 r. wspólnie z Europejskim Urzędem Patentowym (EPO), wkład do gospodarki UE wnoszony przez sektory intensywnie korzystające z praw własności intelektualnej sięga ok. 42% PKB (5,7 biliona euro) i 28% zatrudnienia (do tych 28% doliczyć należy kolejne 10% zatrudnienia pośredniego w sektorach niekorzystających intensywnie z praw własności intelektualnej). Według szacunkowych danych opublikowanych w 2019 r. naruszenia praw własności intelektualnej w handlu międzynarodowym mogły dotyczyć aż 3,3% światowego handlu. Podrabiane towary stanowią nawet 6,8% przywozu do UE, czyli mają wartość 121 mld EUR rocznie. Obydwa zestawienia liczbowe są znacznie wyższe niż występujące, w badaniu

[260] Zob. Ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000), art. 107.
[261] EUIPO to agencja UE z siedzibą w Alicante w Hiszpanii. Zarządza rejestracją znaku towarowego UE (ZTUE) i zarejestrowanego wzoru wspólnotowego (ZWW); oba zapewniają ochronę własności intelektualnej we wszystkich państwach członkowskich UE. EUIPO współpracuje z narodowymi i regionalnymi urzędami ds. własności intelektualnej.

przeprowadzonym w 2016 r.[262] Jeżeli chodzi o szkody gospodarcze powstałe w związku z podrabianiem produktów w 11 sektorach gospodarki, to według EUIPO jest to blisko 60 mld euro rocznie. Straty te wiążą się z 7,4% całości wolumenu sprzedaży w państwach UE i utratą 468 tys. miejsc pracy[263]. Jak wyliczono, najczęściej podrabiane są odzież, obuwie i akcesoria. Rocznie ten segment produkcji traci 28,5 mld euro potencjalnych zysków. W innym ujęciu jest to 9,7% wartości całkowitej sprzedaży tych produktów w skali roku[264]. Należy podkreślić, że stosunkowo łagodne kary oraz wysoki zwrot z przestępczych inwestycji powodują, że podrabianie znaków towarowych stało się niezmiernie intratne dla organizacji przestępczych. Przestępstwa przeciw prawom własności przemysłowej można podzielić na przestępstwa przeciwko wzornictwu użytkowemu i przemysłowemu[265] oraz przestępstwa przeciwko znakom towarowym. Katalog przestępstw przeciwko wzornictwu użytkowemu i przemysłowemu został zawarty w Ustawie z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej[266]. Zgodnie z systematyką dokonaną przez Andrzeja Szewca można wskazane tam przestępstwa podzielić na[267]:

- przestępstwa przeciwko prawom twórcy projektu wynalazczego, obejmujące:
  – przypisywanie sobie autorstwa cudzego projektu wynalazczego;
  – wprowadzenie w błąd innej osoby co do autorstwa projektu wynalazczego;
  – naruszenie praw twórcy projektu w inny sposób;

[262] Zob. *Streszczenie – Raport z 2019 r. na temat statusu ochrony praw własności intelektualnej. Dlaczego prawa własności intelektualnej są ważne, naruszenia praw własności intelektualnej oraz walka z podrabianiem i piractwem,* https://euipo.europa.eu/tunnelweb/secure/webdav/guest/document_library/observatory/documents/reports/2019_Status_Report_on_ IPR_infringement/2019_Status_Report_on_IPR_infringement_exec_pl.pdf [dostęp: 2.01.2021 r.].

[263] *Kosztowne podróbki – raport EUIPO*, https://europarlament.pap.pl/kosztowne-podrobki-raport-euipo [dostęp: 2.01.2021 r.].

[264] Wzrasta systematycznie również handel podróbkami produktów mogących rodzić bezpośrednie zagrożenie dla życia czy zdrowia (farmaceutyków, żywności, napojów [także alkoholowych] oraz półprzewodników stosowanych w transporcie i branży medycznej).

[265] W użyciu do tej grupy przestępstw stosuje się także często umowną nazwę „przestępstwa patentowe".

[266] Ustawa z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej (Tytuł X „Przepisy karne „ obejmujący art. 303–310) (Dz.U. 2001, nr 49, poz. 508 z późn. zm.).

[267] Zob. A. Szewc, *Przestępstwa i wykroczenia przeciwko prawom własności przemysłowej*, s. 235–238, https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/3824/1/BSP%2019_A_Szewc.pdf [dostęp: 2.01.2021 r.].

- przestępstwa przeciwko prawu do uzyskania tytułu ochronnego, obejmujące:
  – zgłoszenie cudzego wynalazku, wzoru użytkowego, wzoru przemysłowego lub cudzej topografii układu scalonego w celu uzyskania patentu, prawa ochronnego lub prawa z rejestracji;
  – ujawnienie uzyskanej informacji o cudzym wynalazku, wzorze użytkowym, wzorze przemysłowym albo cudzej topografii układu scalonego;
  – uniemożliwienie uzyskania patentu, prawa ochronnego lub prawa z rejestracji w inny sposób;
- przestępstwa w zakresie używania podrobionych lub cudzych zarejestrowanych znaków towarowych[268], obejmujące:
  – oznaczanie towarów podrobionym znakiem towarowym[269];
  – oznaczanie towarów zarejestrowanym znakiem towarowym, którego sprawca nie ma prawa używać;
  – dokonywanie obrotu towarami oznaczonymi takimi znakami[270].

Ze względu na istotę ich charakteru, do przestępstw informacyjnych włączyć należy również przestępstwa przeciw informacji publicznej. Uregulowania prawne w zakresie dostępu do tego rodzaju informacji odgrywają ogromną rolę w mechanizmie funkcjonowania demokratycznych państw prawnych. Można wręcz stwierdzić, że są elementem koniecznym praktyki ustrojowej tego rodzaju państw. Umożliwiają bowiem uzyskiwanie informacji o ważnych sprawach państwowych, działalności organów władzy publicznej, zadaniach publicznych. Tak uregulowany dostęp do informacji publicznej

[268] Zgodnie z artykułem 305 Ustawy z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej: „Kto, w celu wprowadzenia do obrotu, oznacza towary podrobionym znakiem towarowym, w tym podrobionym znakiem towarowym Unii Europejskiej, zarejestrowanym znakiem towarowym lub znakiem towarowym Unii Europejskiej, którego nie ma prawa używać, lub dokonuje obrotu towarami oznaczonymi takimi znakami, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". Należy nadmienić, że znaki towarowe mogą być chronione także w oparciu o przepisy karne innych ustaw, w tym ustawy o prawie autorskim i prawach pokrewnych lub ustawy o zwalczaniu nieuczciwej konkurencji.

[269] Przez podrobiony znak towarowym należy rozumieć użyte bezprawnie znaki identyczne ze znakami zarejestrowanymi dla towarów objętych prawem ochronnym lub takie, które nie mogą być od nich odróżnione w zwykłych warunkach obrotu. Oznacza to, że przedmiotem przestępstwa mogą być wyłącznie znaki podrobione, które są przeznaczone dla tożsamych towarów (lub usług), dla których używany jest oryginalny znak.

[270] Występek ten może przyjmować postać: oznaczania towarów podrobionym znakiem towarowym, oznaczania towarów znakami towarowymi, które są zarejestrowane, lecz których oznaczający nie ma prawa używać, oraz dokonywanie obrotu takimi towarami.

wzmacnia transparentność działania organów władzy publicznej oraz jest jednym z elementów gwarantujących jawność tych działań. Dysponowanie przez społeczeństwo rzetelną i pełną informacją pozwala mu także nie tylko na aktywne uczestnictwo w życiu publicznym, ale przyczynia się również do zwiększania efektywności działań organów władzy publicznej i wzmacnia poczucie ich odpowiedzialności za te działania. Z kolei ograniczenie lub utrudnianie dostępu do informacji o pracy organów władzy publicznej w systemie demokratycznym słusznie postrzegane jest jako ograniczanie suwerena (społeczeństwa) w wykonywaniu przypisanej mu władzy i sprawowania kontroli. Jednym ze sposobów zapobiegania takim sytuacjom jest penalizacja czynów godzących w charakteryzowane prawo. Ustawa z 6 września 2001 r. o dostępie do informacji publicznej dokonuje kryminalizacji takich czynów w art. 23 stanowiącym, że „kto, wbrew ciążącemu na nim obowiązkowi, nie udostępnia informacji publicznej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku”[271]. Jak wskazuje Tomasz Bojar-Fijałkowski, ilość spraw prowadzonych z oskarżenia publicznego, czyli przez prokuratorów, oraz ilość wyroków skazujących w związku z naruszeniem przywołanego wyżej artykułu jest niewielka. Większość spraw związanych z naruszaniem prawa dostępu do informacji publicznej rozstrzygana jest bowiem przez sądownictwo administracyjne. Określony wpływ na dotychczasowy stan rzeczy ma także stosunkowo słaby stopień znajomości tej tematyki przez organy ścigania oraz dość rozpowszechnione przekonanie o małej szkodliwości społecznej czynów bezprawnych naruszających prawo do informacji publicznej[272]. Pomimo że dotychczas przypadków zastosowania art. 23 było niewiele, to ze względu na rozwijającą się aktywność organizacji pozarządowych, zajmujących się m.in. kontrolą realizacji zadań w sferze publicznej, oraz wzrastającą świadomością prawną osób fizycznych należy domniemywać, że inicjowanie i prowadzenie postępowań karnych w związku z nieudostępnieniem informacji publicznej stanie się częstsze.

Warunki zaliczenia do segmentu przestępstw informacyjnych spełniają także przestępstwa przeciwko tajemnicom zawodowym oraz innym tajemnicom prawnie chronionym.

---

[271] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej.

[272] Zob. T. Bojar-Fijałkowski, *Dostęp do informacji publicznej – wybrane zagadnienia materialnoprawne i proceduralne z uwzględnieniem informacji o środowisku i jego ochronie jako szczególnego rodzaju informacji publicznej*, [w:] *Dostęp do informacji publicznej. Wybrane aspekty teorii i praktyki*, A. Lusińska, A. Kalinowska-Żeleźnik (red.), Gdańsk 2014, s. 19.

Jak podkreśla Michał Rusinek, jeszcze nie tak dawno problematyka tajemnicy zawodowej ograniczała się do kilku zawodów tradycyjnie uznawanych za oparte na zaufaniu i dyskrecji, takich jak np. lekarz czy prawnik[273]. Jednak szereg przeobrażeń związanych z rozwojem społeczeństwa informacyjnego, gospodarki wolnorynkowej i liberalno-demokratycznych systemów politycznych pociągnął za sobą wzrost zapotrzebowania na gwarancje bezpieczeństwa informacyjnego w coraz bardziej rozległych aspektach działalności ludzkiej. Spowodowało to m.in. zwiększenie liczby tajemnic zawodowych i innych tajemnic prawnie chronionych. Generalnie stosowane i akceptowane jest rozumienie tajemnicy zawodowej jako tajemnicy związanej z wykonywaniem określonego zawodu lub czynności zawodowych[274]. Katalog tajemnic objętych ochroną prawną nie ogranicza się jednak jedynie do tych związanych z wykonywaniem konkretnych zawodów. W polskim porządku prawnym określa się także szereg innych tajemnic prawnie chronionych, odnoszących się do instytucji państwowych, samorządowych, organizacji społecznych czy też podmiotów gospodarczych. W oparciu o szeroko zakrojoną analizę aktów prawnych Krzysztof Domagała i Tomasz Domagała wyróżnili 48 rodzajów tajemnic zawodowych i 22 rodzaje tajemnic prawnie chronionych, dodając, że katalog ten nie jest zamknięty[275]. Jeżeli chodzi o przestępstwa przeciwko tajemnicom zawodowym oraz innym tajemnicom prawnie chronionym, to w świetle artykułu 266 Kodeksu karnego są nimi czyny związane z:

– ujawnianiem lub wykorzystywaniem wbrew przepisom ustawy lub przyjętego na siebie zobowiązania informacji, z którą sprawca zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową;
– ujawnieniem przez funkcjonariusza publicznego osobie nieuprawnionej informacji niejawnej o klauzuli „zastrzeżone" lub „poufne" lub informacji uzyskanej w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes[276].

Ostatnią z kategorii przestępstw wpisywanych w zakres przestępstw informacyjnych są cyberprzestępstwa. Jeżeli rozważyć tę kategorię, to na jej

[273] Zob. M. Rusinek, *Tajemnica zawodowa i jej ochrona w polskim procesie karnym*, Warszawa 2007, s. 11.
[274] Tamże, s. 17.
[275] Zob. K Domagała, T. Domagała*, Tajemnice prawnie chronione po wejściu w życie ustawy z dnia 05.08.2010 r. o ochronie informacji niejawnych*, http://www.zielona-gora.po.gov.pl/magazyn/upload/lektury_ elektroniczne/tajemnice1.pdf [dostęp: 3.01.2021 r.].
[276] Zob. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny.

wyodrębnienie wpłynął przede wszystkim rozwój wykorzystywania technologii i sprzętu komputerowego do czynów naruszających prawo karne. W związku z tym początkowo do ich nazywania zaczęto stosować takie pojęcia jak „przestępstwa związane z wykorzystaniem komputera" czy po prostu „przestępstwa komputerowe". Szybko jednak, wobec dynamicznego rozwoju form i zakresu tego typu przestępstw, terminologię taką zaczęto uznawać za mało adekwatną[277]. Jednocześnie badacze zajmujący się omawianą problematyką, próbujący określić istotę przestępstw popełnianych przy użyciu technologii informacyjnych oraz telekomunikacyjnych, coraz częściej zaczęli odwoływać się do pojęcia cyberprzestrzeni[278], co w rezultacie przełożyło się również na pojawienie się terminów „cyberprzestępstwo" oraz „cyberprzestępczość".

Mimo że nadal trudno jest ustalić precyzyjnie i w miarę jednoznacznie zakres znaczeniowy pojęcia „cyberprzestępstwo" (m.in. ze względu na to, że tego typu czyny przestępcze dynamicznie wraz z postępem technologicznym ewoluują), to konstruowanie takich definicji jest niezmiernie istotne. Decydują o tym tak potrzeby naukowe, jak i utylitarne (w szczególności zaś właściwa organizacja ścigania karnego, budowa systemów cyberbezpieczeństwa itp.), których zaspokojenie przyczyniać się będzie do skutecznego przeciwdziałania i zwalczania cyberprzestępczości, a tym samym poprawy poziomu bezpieczeństwa informacyjnego. Spośród wielu prób zdefiniowania tego, czym jest cyberprzestępstwo, należy w pierwszym rzędzie wymienić ujęcie, które powstało podczas X Kongresu ONZ w Sprawie Zapobiegania Przestępczości i Traktowania Przestępców w 2000 r. w Wiedniu, gdzie wypracowano definicję zawierającą podział na:

[277] Zob. I. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 8.

[278] Termin „cyberprzestrzeń" (ang. *cyberspace*) stworzył i upowszechnił w 1984 r. William Gibson. Za jedną z bardziej udanych wersji tego określenia można uznać tę stworzoną przez Marka Madeja, mówiącą, że jest to ogół powiązań o charakterze wirtualnym („nieprzestrzennym" w sensie fizycznym, niematerialnym) powstałych i istniejących dzięki ich fizycznym manifestacjom (komputery, infrastruktura telekomunikacyjna). Zob. M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009, s. 28. Z kolei w ujęciu *Strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024,* „cyberprzestrzeń to przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne". Zob. Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M.P. 2019, poz. 1037).

a) cyberprzestępstwo *sensu stricto* (przestępstwo komputerowe), obejmujące nielegalne działania przeciwko bezpieczeństwu systemów komputerowych i elektronicznie przetwarzanych przez te systemy danych, wykonywane z wykorzystaniem operacji elektronicznych;
b) cyberprzestępstwo *sensu largo* (przestępstwo dotyczące komputerów), obejmujące nielegalne działania popełniane przy użyciu lub skierowane przeciwko systemom czy sieciom komputerowym (także nielegalne posiadanie oraz udostępnianie lub rozpowszechnianie informacji za pomocą komputera lub sieci)[279].

Stosunkowo lapidarna, ale przydatna do prowadzenia dalszych analiz definicja cyberprzestępstwa zawarta została w dokumencie zatytułowanym *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* przyjętym przez Radę Ministrów 25 czerwca 2013 r. Zgodnie z treścią tego dokumentu „cyberprzestępstwo to czyn zabroniony popełniony w obszarze cyberprzestrzeni"[280].

Stojąc na gruncie powyższych ujęć, opierając się na rozważaniach Janusza Wasilewskiego, można wskazać, że „cyberprzestępstwem jest każdy czyn spełniający łącznie dwie następujące przesłanki:
– jest czynem zabronionym w rozumieniu dowolnego przepisu prawnego;
– szczególnym miejscem popełnienia czynu musi być cyberprzestrzeń rozumiana nie jako kategoria geograficzna, ale nowa, logiczna domena ludzkiej działalności, podbudowywana przez szeroko rozumianą infrastrukturę teleinformatyczną, lecz z nią nieutożsamiana (cyberprzestrzeń jako środowisko wirtualne, oderwane od substratu fizycznego)"[281].

Dążąc do w miarę przejrzystego ukazania zasadniczego katalogu cyberprzestępstw, można je – za Mariuszem Stefanowiczem – ująć w ramach

[279] Zob. I. Jaroszewska, dz. cyt., s.10.
[280] *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013, s. 5, https://jakubow.pl/wp-content/uploads/2015/06/Polityka-Ochrony-Cyberprzestrzeni-RP_148x210_wersja-pl.768174_715482.pdf [dostęp: 23.10.2020 r.]. Dokument opracowało Ministerstwo Administracji i Cyfryzacji przy współpracy z Agencją Bezpieczeństwa Wewnętrznego. Polityka została przyjęta uchwałą Rady Ministrów 25 czerwca 2013 roku i obowiązywała tylko administrację rządową. Nie obejmowała również niejawnych systemów teleinformatycznych. W 2017 roku została zastąpiona przez Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017––2022 przyjęte Uchwałą nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r., które z kolei zostały zastąpione przez Strategię cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019––2024 przyjęte Uchwałą nr 125 Rady Ministrów z dnia 22 października 2019 r.
[281] J. Wasilewski, *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 8, s. 167.

dwu kategorii. Pierwsza z nich to przestępstwa, w których przedmiotem ataku jest komputer oraz przetwarzanie danych w systemach informatycznych, obejmujące takie czyny, jak:

– podawanie się za inną osobę;
– nieuprawnione uzyskiwanie informacji;
– stosowanie podsłuchu komputerowego;
– udaremnienie uzyskania informacji lub dostępu do danych informatycznych;
– sabotaż komputerowy;
– rozpowszechnianie złośliwych programów oraz *cracking*;
– stosowanie tzw. narzędzi hackerskich;
– oszustwa komputerowe.

Druga z kategorii cyberprzestępstw to te, w których komputer stanowi narzędzie do ich popełnienia. Obejmuje ona:

– obrazę uczuć religijnych (przestępstwa przeciwko wolności sumienia i wyznania);
– składanie propozycji obcowania płciowego małoletnim;
– publiczne propagowanie lub pochwalanie zachowań o charakterze pedofilskim;
– publiczne propagowanie faszystowskich lub innych totalitarnych ustrojów politycznych;
– nawoływanie do nienawiści na tle różnic narodowościowych, etnicznych, rasowych czy wyznaniowych albo ze względu na bezwyznaniowość (mowa nienawiści);
– obrót fikcyjnymi kosztami;
– zbywanie własnego lub cudzego dokumentu stwierdzającego tożsamość (przestępstwa przeciwko wiarygodności dokumentów)[282].

Jeżeli chodzi o cyberprzestępczość, to w komunikacie Komisji Europejskiej z 7 lutego 2013 roku stwierdzono, że pojęcie to „odnosi się do szerokiego wachlarza różnych rodzajów działalności przestępczej, w przypadku której komputery i systemy informatyczne stanowią podstawowe narzędzie przestępcze lub są głównym celem działania przestępczego”[283].

[282] Zob. M. Stefanowicz, *Cyberprzestępczość – próba diagnozy zjawiska*, „Kwartalnik Policyjny” 2017, nr 4, s. 21.
[283] *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*, Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, s. 3, https://eur-lex.

Zamykając powyższe rozważania, w oparciu o ustalenia M. Siwickiego można przyjąć do dalszego zastosowania, że do szerokiego kręgu cyberprzestępczości należą przestępstwa:

– przeciwko bezpieczeństwu przetwarzanej informacji;
– związane z użyciem środków masowego przekazu do rozpowszechniania lub prezentowania informacji zakazanych przez prawo;
– instrumentalnego wykorzystania (użycia) elektronicznych sieci informatycznych i systemów informatycznych do naruszania dóbr chronionych przez prawo[284].

Uogólniając przedstawione rozważania, należy wskazać, że chociaż termin „przestępstwo informacyjne" nie należy w aktualnie istniejącym stanie prawnym do pojęć zdefiniowanych ustawowo, to nie sposób nie zauważyć, że istnieje konieczność jego wprowadzenia chociażby ze względu na systematyczny rozwój ilościowy i jakościowy czynów bezprawnych dokonywanych w infosferze i z nią związanych. Łączy się z tym również niezbędność przyjęcia terminu „przestępczość informacyjna" i określenia jego zakresu znaczeniowego. Koronnym argumentem przemawiającym za takim rozwiązaniem jest potrzeba wypracowania zbiorczej formuły, obejmującej ogół czynów karalnych wymierzonych w prawo do informacji, obowiązki informacyjne i ochronę informacji w różnych formach. Biorąc pod uwagę powyżej przedstawiony zestaw przestępstw związanych z informacją i ich cechy charakterystyczne, można roboczo przyjąć, że przestępstwo informacyjne to czyn bezprawny, zawiniony i posiadający znaczną szkodliwość społeczną, wymierzony w chronione prawem karnym indywidualne i zbiorowe dobra informacyjne. Natomiast przestępczość informacyjna to grupa czynów polegających na naruszaniu indywidualnych i zbiorowych dóbr informacyjnych chronionych przez prawo karne.

Kontynuując uwagi podsumowujące, wskazać trzeba również, że współczesny zglobalizowany, coraz bardziej zinformatyzowany i nasycany nowoczesnymi technologiami informacyjnymi świat oprócz pożytków płynących z takiego stanu rzeczy doświadcza także szeregu zagrożeń i wyzwań dla bezpieczeństwa informacyjnego. Dlatego też za tym wszystkim nadążyć muszą regulacje prawne jako ważny instrument kreowania i realizacji polityki

europa.eu/legalcontent/PL/TXT/PDF/?uri=CELEX:52013JC0001&from=en [dostęp: 4.01.2021 r.].

[284] Zob. M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8, s. 250.

bezpieczeństwa informacyjnego. Należy pamiętać, że przestępstwa informacyjne oraz przestępczość informacyjna (chociaż nigdy tak nie nazywane) nie są zjawiskami nowymi. Towarzyszą one bowiem ludzkiej cywilizacji od zarania dziejów i wraz ze zmianami w niej zachodzącymi rozwijają swe formy i zasięg. Co prawda na najwcześniejszych etapach rozwoju ludzkości trudno jest mówić o istnieniu przestępczości informacyjnej jako takiej, ale z całą pewnością można wskazać wiele zachowań (np. różnych form naruszania tajemnic, fałszowania dokumentów czy też przywłaszczania sobie cudzego dorobku intelektualnego) stanowiących naruszenia zasad obowiązujących w zakresie wytwarzania, przechowywania i przekazywania informacji. Podobnie jak wiele innych zjawisk patologicznych, przestępstwa informacyjne oraz przestępczość informacyjna są w określonym stopniu produktem postaw ludzkich kształtowanych w ciągu wieków i utrwalanych pod wpływem panujących stosunków społecznych oraz możliwości technicznych. Wiele form przestępczości informacyjnej albo wręcz poszczególne zachowania (np. kradzieże wynalazków, plagiaty czy wykradanie tajemnic) stanowiące naruszenia porządku informacyjnego, a dzisiaj definiowane jako czyny zabronione o znamionach przestępstwa, przetrwało wieki, chociaż ewoluowały techniki ich popełniania. Nie można także, uwzględniając doświadczenia historyczne, pominąć faktu, że wchodzące w skład tego zjawiska zachowania zawsze działały destrukcyjnie na podstawy porządku ekonomicznego i społecznego, niszcząc więzi społeczne, podważając zaufanie do norm prawnych i uznawanych wartości, a współcześnie czynią to z o wiele większą mocą i na globalna skalę. Wskazuje to niewątpliwie, jak trwałym i nieodłącznym elementem życia społecznego jest zjawisko przestępczości informacyjnej.

3.3. Dezinformacja

Dezinformacja (chociaż nie zawsze tak nazywana) jako jedno z zagrożeń informacyjnych w ciągle ewoluujących formach towarzyszy ludzkości od tysiącleci. Należy pamiętać, że już ok. 400 lat p.n.e. chiński strateg Sun Tzu w swoim fundamentalnym dziele dotyczącym zasad prowadzenia wojen wskazywał, że „wojna jest sztuką wprowadzania wroga w błąd”[285]. Na podstawie dostępnych źródeł można stwierdzić, że instrumenty i mechanizmy dezinformacyjne

[285] Sun Tzu, *Sztuka wojny,* Warszawa 1994, s. 80.

w odległych czasach wykorzystywano przede wszystkim w działaniach militarnych. Były one na tyle skuteczne, że nawet po długich okresach walk, w których stosowanie klasycznych środków walki nie dawało zwycięstwa, potrafiły zapewnić oczekiwany sukces. Wystarczy przypomnieć chociażby fortel Greków, który pomógł im zająć obleganą przez dziewięć lat Troję. W stosowaniu podstępów biegłe były także plemiona azjatyckie. W ocenie współczesnych teoretyków wojen informacyjnych szczególnie wyróżniał się na tym polu władca imperium mongolskiego Czyngis-chan, prowadzący zaawansowane kampanie dezinformacyjne przy użyciu emisariuszy i agentów wpływu wobec państw, które planował podbić[286]. Warto przywołać także to, co Niccolo Machiavelli, jeden z najwybitniejszych przedstawicieli renesansowej myśli politycznej, napisał w traktacie o sprawowaniu władzy zatytułowanym *Książę*. Sławny florentyńczyk wspomina tam m.in. o metodzie zwalczania przeciwników politycznych za pomocą rozpowszechniania o nich fałszywych wiadomości: „O jednym mówiono, że ukradł państwowe pieniądze; o innym, że nie wykonał powierzonego mu zadania, bo został przekupiony; o innym jeszcze, że kierowany ambicją popełnił taką a taką pomyłkę”[287]. W XIX wieku pruski generał Carl Phillip Gottlieb von Clausewitz w rozważaniach dotyczących znaczenia wiadomości podczas wojny podkreślał wagę umiejętności rozróżniania wiarygodnych informacji, ponieważ, jak wskazywał, wśród wiadomości otrzymywanych na wojnie wiele „jest sprzecznych, jeszcze więcej jest fałszywych, a najwięcej niepewnych”[288]. Jednocześnie wspomniany teoretyk wojny uwypuklał fakt, że w określonych okolicznościach (słabość sił własnych, trudne położenie) podstęp połączony z odwagą może zapewnić powodzenie w działaniach wojennych[289]. Jednak dopiero w carskiej Rosji uczyniono z maskowania, oszustwa i prowokacji fundament strategii politycznej. Można powiedzieć, że jednym z symboli tych rosyjskich osiągnięć stało się określenie „wioski potiomkinowskie”[290], używane od dawna jako synonim mistyfikacji tworzonej

[286] Zob. A. Lelonek, *Wojna informacyjna, operacje informacyjne i psychologiczne: pojęcia, metody i zastosowanie*, [w:] *Potencjał słowa. Międzynarodowe stosunki i komunikacja: stan i perspektywy*, A. Lelonek (red.), Warszawa-Lwów 2016, s. 84.
[287] N. Machiavelli, *Książę. Rozważania nad pierwszym dziesięcioksięgiem historii Rzymu Liwiusza*, Warszawa 1984, s. 127.
[288] C. von Clausewitz, *O wojnie,* Warszawa 1958, s. 74.
[289] Tamże, s. 181.
[290] Określenie pochodzi od nazwiska gubernatora Nowej Rosji, księcia Grigorija Potiomkina, który w 1787 r. zorganizował dla carycy Katarzyny II i jej dworu oraz kilku przedstawicieli obcych państw rejs w dół Dniepru, aby pokazać, jak pod jego rządami rozkwita podległa mu gubernia. Ponieważ była ona w rzeczywistości słabo zaludniona i biedna, w celu wywołania

dla ukrycia prawdziwego obrazu rzeczywistości. Po upadku caratu nowe bolszewickie władze zaczęły stosować dezinformację na szeroką skalę, wykorzystując ją zarówno do zwalczania przeciwników wewnętrznych, jak i oddziaływania na otoczenie międzynarodowe. Egzemplifikację takiego podejścia możemy odnaleźć w stanowisku Włodzimierza Lenina, który twierdził, że należy prowadzić „wojnę psychologiczną, w której nie trzeba wytaczać dział na pole bitwy, lecz naród (…) siłą swojej woli doprowadza do rozkładu tkanki moralnej i duchowej innego narodu”[291].

Oddziaływanie psychologiczne, prowokacje, maskowanie i pozoracja były stosowane także przez państwa zachodnie. Jednak tego typu operacje podejmowano głównie przeciwko nieprzyjacielskim państwom w sferze militarnej. Przykładem mogą być tu Niemcy, które podczas I wojny światowej stworzyły specjalną jednostkę, nazwaną służbą dezinformacyjną, która zajmowała się koordynacją pozorowanych połączeń radiowych w taki sposób, aby zawarte w nich wprowadzające w błąd treści mogły być odczytywane przez służby wywiadowcze państw Ententy.

Również w Polsce międzywojennej stosunkowo wcześnie zaczęto doceniać walory operacji dezinformacyjnych, chociaż na ich określenie używano terminu „inspiracja”. Już w latach 20. XX w. kadra Oddziału II Sztabu Głównego (SG)[292] objęta była szkoleniami dotyczącymi zarówno prowadzenia działań inspiracyjnych, jak i przeciwdziałania im. Zgodnie z poglądami wypracowanymi i przyjętymi w tej komórce organizacyjnej SG przez inspirację rozumiano „działalność polegającą na podaniu wywiadowi przeciwnika wiadomości, ukrywających własne zamierzenia, czyli ochronę istotnej własnej tajemnicy, oraz zmuszeniu go do traktowania informacji, podanej przez wywiad własny, jako prawdziwej, względnie na zmuszeniu wywiadu obcego do analizy

zaplanowanego wrażenia książę G. Potiomkin nakazał na trasie przejazdu stworzyć makiety prawdziwych wiosek, a w tych istniejących odnowić i przystroić fasady. Istotnym elementem tych działań było także przebieranie ludności w nowe stroje i organizowanie robót na pokaz. Należy zauważyć, że wersja ta jest podważana przez rosyjskiego historyka Aleksandra Panchenkę, który uważa, że jest to przykład antypotiomkinowskiej propagandy, bowiem książę, chociaż ozdabiał i upiększał miasta i wsie, to nie czynił z tego tajemnicy.

[291] S. Newcourt-Nowodworski, *Czarna propaganda. Polska, Niemcy, Wielka Brytania. Tajemnice największych oszustw II wojny światowej*, Kraków 2008, s. 27.

[292] Oddział II – jednostka organizacyjna polskiego Sztabu Głównego (do 1928 r. Sztabu Generalnego) odpowiedzialna za wywiad, kontrwywiad, radiokontrwywiad i kryptologię. Funkcjonowała w latach 1918–1945.

inspirowanych wiadomości przez czas dłuższy”[293]. Teoretycznymi aspektami związanej z dezinformacją propagandy[294] zajmował się m.in. pułkownik Stefan Rowecki, który szczególną uwagę zwrócił na jej stosowanie w czasie wojny. S. Rowecki dobitnie podkreślał znaczenie oddziaływania propagandowego na opinię publiczną, zaznaczając, że bez „solidnie zorganizowanej potężnej propagandy nie sposób wyobrazić sobie prowadzenia jakichkolwiek działań wojennych”[295]. Istotny impuls rozwojowy dla dezinformacji stanowiła II wojna światowa. Szeroko wykorzystywały ją wtedy wszystkie strony konfliktu. Brytyjczycy np. sformowali w tym celu kilka jednostek zajmujących się dywersją propagandową oraz maskowaniem operacyjnym. Również brytyjska agentura działająca przeciwko III Rzeszy oprócz uzyskiwania informacji wprowadzała do obiegu na jej terytorium materiały propagandowe[296].

Po II wojnie światowej dezinformację szczególnie intensywnie zaczęto wykorzystywać w Związku Socjalistycznych Republik Radzieckich (ZSRR). Towarzyszył temu rozwój specjalistycznych komórek organizacyjnych w służbach specjalnych tego państwa[297]. ZSRR oddziaływał również na stosowanie dezinformacji przez tajne służby państw bloku wschodniego. W latach 60. XX w. pod wpływem Moskwy stworzono w nich wyspecjalizowane struktury zajmujące się rozpowszechnianiem fałszywych wiadomości i plotek[298].

Dezinformacja była także jednym z instrumentów pracy operacyjnej cywilnych i wojskowych służb specjalnych Polskiej Rzeczpospolitej Ludowej (PRL), a tematyka z nią związana znalazła się w programach szkolenia tych służb.

Współcześnie dezinformacja nie tylko zwiększa swój zakres i siłę oddziaływania, ale wykazuje również bardzo duży potencjał rozwojowy. Jednocześnie pozostaje zagrożeniem stosunkowo słabo rozpoznanym i uświadamianym zarówno w środowiskach decydentów państwowych, jak i szeroko rozumianych kręgach społecznych. Specyfika dezinformacji jako zagrożenia

[293] *Inspiracja i aktywność jako metody nowoczesnego wywiadu*, Ministerstwo Spraw Wojskowych – Sztab Generalny, Warszawa 1926, s. 23.
[294] W okresie walki z niemieckim okupantem gen. Stefan Rowecki (ps. Grot) jako Komendant Armii Krajowej użył tej wiedzy w praktyce jako jeden z inicjatorów prowadzenia propagandy dywersyjnej przeciwko Niemcom w ramach tzw. akcji „N”. Za całokształt działań propagandowych ZWZ, a następnie AK, odpowiadało Biuro Informacji i Propagandy (BIP).
[295] S. Rowecki, *Propaganda w przygotowaniu kraju*, Warszawa 1933, s. 24.
[296] S. Newcourt-Nowodworski, dz. cyt., s. 98.
[297] Zob. V. Volkoff, *Dezinformacja – oręż wojny*, Warszawa 1991, s. 12.
[298] I.M. Pacepa, R.J. Rychlak, *Dezinformacja. Były szef wywiadu ujawnia metody dławienia wolności, zwalczania religii i wspierania terroryzmu,* Gliwice 2015, s. 118.

informacyjnego polega na łączeniu przez nią składników innych typów zagrożeń informacyjnych oraz podatności ludzkich umysłów na zabiegi manipulacyjne. Istnienie wspomnianej podatności powoduje, że ludzie nie tylko w kategoriach jednostkowych, ale także jako większe zbiorowości społeczne stanowią stosunkowo często obiekty zabiegów dezinformacyjnych, przy pomocy których uzyskuje się zaplanowany wpływ na ich decyzje i postępowanie. W języku potocznym dezinformacja często mylnie bywa utożsamiana z pojęciami takimi jak: dyskredytacja, mistyfikacja, manipulacja, prowokacja, blef, intryga czy kamuflaż. Ten pogląd wypływa z faktu, że przy zastosowaniu tych socjotechnicznych metod również można doprowadzić do zaplanowanych zmian w postawach określonych osób czy grup społecznych, jednak bez tak szerokich skutków, jak w przypadku dezinformacji. Istotne jest zatem ustalenie definicyjnego obrazu dezinformacji. W słowniku wyrazów obcych termin „dezinformacja" jest objaśniany jako „informacja fałszywa, myląca"[299]. W *Słowniku języka polskiego* dezinformacja to „wprowadzanie w błąd przez podanie fałszywych informacji; nieprawdziwa, myląca informacja"[300]. *Leksykon wiedzy wojskowej* ujmuje dezinformację w wąskim, *stricte* militarnym kontekście jako „rozpowszechnianie nieprawdziwych wiadomości i dokumentów dla wprowadzenia w błąd nieprzyjaciela co do faktycznego zamiaru, organizacji prowadzenia operacji (walki, bitwy), a także składu wojsk własnych i charakteru ich działania"[301]. Dla autorów wielotomowej encyklopedii powszechnej wydanej w ZSRR w latach 50. XX w. dezinformacja to „rozprowadzanie przez prasę i radio fałszywych danych w celu wprowadzania w błąd opinii publicznej"[302]. Z kolei polski leksykon poświęcony tajnym służbom autorstwa Jana H. Lareckiego zawiera następujące ujęcia dezinformacji:

- „metodologiczny sposób oddziaływania na przeciwnika, podejmowany z zamiarem wykreowania celowego, ukierunkowanego wpływu na kształtowanie opinii i bieg możliwych do przewidzenia zdarzeń[303]";
- „zaplanowane wg jednolitej koncepcji tajne działanie polegające na przygotowaniu, opracowaniu i w konsekwencji podsunięciu/przekazaniu przeciwnikowi (jego służbie specjalnej) lub jawnym rozpowszechnianiu,

[299] Zob. *Słownik wyrazów obcych PWN*, J. Tokarski (red.), Warszawa 1980, s. 149.
[300] *Słownik języka polskiego PWN*, M. Szymczak (red.), Warszawa 1978, t.. I, s. 390.
[301] *Leksykon wiedzy wojskowej*, Warszawa 1979, s. 87.
[302] *Wielka encyklopedia radziecka*, t. XII, Moskwa 1952, s. 566, cyt. za: A. Golicyn, *Nowe kłamstwa w miejsce starych. Komunistyczna strategia podstępu i dezinformacji,* Warszawa 2007, s. 5.
[303] T.H. Larecki, *Wielki leksykon tajnych służb świata,* Warszawa 2017, s. 211.

ale z ukrytymi celami, w społeczeństwie kraju przeciwnika częściowo lub całkowicie fałszywych informacji, dokumentów (pism, listów, publikacji, rękopisów itp.), zdjęć lub w innej formie spreparowanych danych, mających wytworzyć pozornie prawdziwy obraz lub pogląd i kształtować opinię o osobie, zdarzeniu czy zjawisku zgodnie z operacyjnymi interesami służby specjalnej podejmującej działania dezinformacyjne lub/i politycznymi państwa, w interesie którego dana służba je realizuje, na ogół dla spowodowania bezpośredniej lub pośredniej szkody dla bieżących lub przyszłych interesów przeciwnika. Efektem takich działań jest wpływanie na procesy decyzyjne rozważane przez gremia innego państwa (rząd, parlament, organy gospodarcze), które mogą wykorzystać takie informacje dla podejmowania decyzji szkodzących żywotnym interesom tego kraju"[304].

W opinii brytyjskiego znawcy problematyki, Richarda Deacona[305], dezinformacja to „sfabrykowane świadectwa, taktyka oczerniania oraz sfabrykowane dokumenty wykorzystane do zdyskredytowania przeciwnika"[306]. Pochodzący z Rosji, ale tworzący i publikujący na Zachodzie Vladimir Volkoff[307] twierdził, że dezinformacja stanowi „syntezę służby wywiadowczej (zdobywanie wiadomości dotyczących nieprzyjaciela) i kontrwywiadowczych (infiltrowanie jego służb wywiadowczych), dlatego że umożliwia »zdalne sterowanie« celem za pomocą wcześniej przygotowanych materiałów i to nie przez tajne, pełne niewiadomych wpływanie na specjalistyczne organy, lecz przez jawne oddziaływanie na człowieka na ulicy, a poprzez niego na władzę i ekspertów"[308]. Cytowany autor wyspecyfikował również listę metod oddziaływania psychologiczno-manipulacyjnego na przeciwnika, obejmującą podstęp,

[304] Tamże.
[305] Richard Deacon (właściwe nazwisko George Donald King McCormick, 1911–1998), podczas II wojny światowej oficer wywiadu brytyjskiej marynarki wojennej, potem dziennikarz, autor wielu prac na temat służb specjalnych i operacji szpiegowskich.
[306] R. Deacon, *Spyclopaedia*, London 1989, p. 400; cyt. za: P. Kocoń, *Militarne operacje dezinformacyjne w perspektywie interakcjonizmu symbolicznego*, „Zeszyty Naukowe WSOWL" 2012, nr 4, s. 25.
[307] Vladimir Volkoff, Władimir Nikołajewicz Wołkow (1932–2005), osiadły we Francji rosyjski emigrant i pisarz. W latach 1966–77 przebywał i pracował w USA jako wykładowca literatury francuskiej i rosyjskiej. Laureat wielu nagród literackich. Popularyzator teorii Anatolija Golicyna dotyczących dezinformacyjnej strategii ZSRR.
[308] V. Volkoff, dz. cyt., s. 10.

wprowadzanie w błąd (intoksykację)[309], białą i czarną propagandę, wpływanie, logomachię[310] oraz dezinformację[311]. Szczególnie duży nacisk V. Volkoff kładł na niezbędność rozróżniania dezinformacji oraz intoksykacji. To drugie pojęcie według niego dotyczy wprowadzania przeciwnika w błąd. Jest to działanie jednorazowe, krótkotrwałe, obliczone na osiągniecie dość precyzyjnie określonego celu, którym może być np. zmylenie przeciwnika co do miejsca i czasu ataku[312]. Z kolei dezinformacja to działanie złożone, ukierunkowane na osiągnięcie więcej niż jednego celu, realizowane w dłuższych perspektywach czasowych (nawet kilkunastoletnich). Dezinformacją oddziałuje się na wiele podmiotów (instytucje, państwa, społeczeństwa). Przywoływany teoretyk dezinformacji wskazuje w kontekście wspomnianych różnic, że „wprowadzanie w błąd jest techniką, a dezinformacja doktryną"[313]. Koresponduje z tym poglądem opinia Stanisława Hoca, który dezinformację postrzega jako strategię zawierającą dwa składniki: wprowadzanie w błąd oraz wywieranie wpływu[314]. Na gruncie prawnym dezinformacja „jest szczególnym rodzajem oszustwa"[315]. W środowisku specjalistów od zarządzania kryzysowego operuje się lapidarnym określeniem traktującym dezinformację jako „umyślne przekazywanie nieprawdziwych informacji w celu wprowadzenia odbiorcy w błąd"[316].

Według Komisji Europejskiej (KE) dezinformacja to „fałszywa lub myląca informacja tworzona, prezentowana i rozpowszechniana dla osiągnięcia korzyści ekonomicznych lub spowodowania szkód publicznych poprzez celowe oszukiwanie opinii publicznej"[317]. W projekcie doktryny bezpieczeństwa

[309] Intoksykacja (w mikrobiologii oznacza zatrucie organizmu toksyną zawartą w żywności przed jej spożyciem) w omawianym przypadku to umieszczanie wśród informacji prawdziwych także częściowo prawdziwych lub nieprawdziwych.
[310] Logomachia – jałowy spór o słowa, w rzeczywistości dotyczący spraw drugorzędnych.
[311] Zob. V. Volkoff, dz. cyt., s. 6–10.
[312] Zob. tamże, s. 6–8.
[313] Tamże, s. 11.
[314] Zob. S. Hoc, *Przestępstwo dezinformacji wywiadowczej w kodeksie karnym*, „Przegląd Sądowy" 2000, nr 5, s. 50.
[315] P. Chlebowicz, *Interpretacja pojęcia dezinformacji w świetle art. 132 k.k.,* „Studia Prawnoustrojowe" 2012, nr 15, s. 42.
[316] *Księga komunikacji kryzysowej 2017. Podstawy zarządzania informacją w kryzysie*, Rządowe Centrum Bezpieczeństwa, Warszawa 2017, s. 5, https://rcb.gov.pl/wp-content/uploads/KKK_2017_sklad_pk2-1.pdf [dostęp: 10.09.2020 r.].
[317] Brussels, 5.12.2018 join (2018) 36 Final Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Action Plan against Disinformation Communication on Tackling On-line Disinformation, com (2018) 236, s. 2.

informacyjnego RP z 2015 dezinformacja[318] określona została jako „rozpowszechnianie zmanipulowanych lub sfabrykowanych informacji (albo kombinacji jednych i drugich) w celu skłonienia ich odbiorców do określonych zachowań korzystnych dla dezinformującego lub też w celu odwrócenia ich uwagi od faktycznie zaistniałych wydarzeń"[319]. W bardziej opisowym ujęciu można, w świetle raportu opracowanego przez Naukową i Akademicką Sieć Komputerową (NASK) Państwowy Instytut Badawczy, mówić o dezinformacji wówczas, kiedy rozpowszechniane informacje:

– mają całkowicie lub częściowo fałszywy charakter;
– są zmanipulowane lub wprowadzają odbiorców w błąd;
– odnoszą się do ważnych z punktu widzenia interesu publicznego zagadnień;
– są ukierunkowane na wywoływanie niepewności lub wrogości;
– mają prowadzić do polaryzacji albo zakłócania procesów demokratycznych;
– są przekazywane lub wzmacniane z użyciem zautomatyzowanych i agresywnych technik, (np. boty społeczne, sztuczna inteligencja, mikrotargeting czy trollowanie)[320].

Jolanta Darczewska w ramach analizy współczesnego rosyjskiego podejścia do dezinformacji opisuje ją jako pewien ciągły zgodny z celami i zasadami planowania strategicznego proces, polegający na systemowej i zintegrowanej działalności państwa, prowadzonej na wielu płaszczyznach przy wykorzystaniu różnorodnych kanałów (dyplomatycznych, politycznych, ekonomicznych, militarnych, społecznych, medialnych). Działalność taka realizowana jest w sposób niestandardowy (nie stosuje się modeli uniwersalnych) i przy użyciu pośrednich, trudnych do uchwycenia technik przekazu i oddziaływania. Jest ona nakierowana na realizację celów strategicznych i wzmocnienie pozycji państwa dezinformującego oraz doprowadzenie do sytuacji, w której aktorzy wewnętrzni państwa (państw) poddawanego oddziaływaniom dezinformacyjnym będą realizować te cele[321]. W ciekawych rozważaniach autorstwa

[318] Walory tego interesującego ujęcia osłabia fakt, że autorzy projektu doktryny nie rozróżniają terminów „dezinformacja" i „propaganda „ traktując je w sposób nieuzasadniony jako tożsame.
[319] *Doktryna bezpieczeństwa informacyjnego…*, s. 4.
[320] *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, M. Wrzosek (red.), Warszawa 2019, s. 7.
[321] Zob. J. Darczewska, *Dezinformacja – rosyjska broń strategiczna*, https://rcb.gov.pl/dezinformacja-rosyjska-bron-strategiczna/ [dostęp: 15.09.2020 r.].

Mikołaja Juliusza Wachowicza dezinformacja jest przedstawiona m.in. jako „świadome, umyślne i podstępne wprowadzanie w błąd przeciwnika przez ukrywający rzeczywiste zamierzenia dowolny podmiot państwowy lub pozapaństwowy, w przestrzeni fizycznej lub informacyjnej, za pomocą odpowiednio zniekształconych (dosłownie bądź kontekstowo) danych, informacji i dokumentów, w celu doprowadzenia dezinformowanego do podjęcia korzystnych dla dezinformatora decyzji (działań lub zaniechań), zmylenia dezinformowanego, odwrócenia jego uwagi, uzyskania efektu zaskoczenia, zniekształcenia realnego obrazu rzeczy i świata, jak również w celu ochrony godziwych i niegodziwych interesów dezinformatora”[322]. Analizując dezinformację jako zagrożenie dla biznesu, Jacek Borecki wskazuje, że o jej istocie decyduje przekazywanie celowo przygotowywanych i preparowanych informacji, aby wytworzyć u odbiorców mylne wyobrażenia o rzeczywistości, na podstawie których podejmują oni decyzje[323]. Warto w tym miejscu przywołać także pogląd Marka Świerczka, który w rozważaniach poświęconych rosyjskiemu systemowi działań dezinformacyjnych przyjął, że „dezinformacja to proces wpływania na zachowanie podmiotu dezinformowanego przez zniekształcanie postrzegania przez niego rzeczywistości, prowadzące ofiarę dezinformacji do podejmowania działań zgodnych z obrazem zdeformowanym, a zarazem odpowiadających interesom podmiotu dezinformującego. Jest to proces planowany i przeprowadzany przez wyspecjalizowane instytucje państwowe, które dysponują odpowiednimi do tego zasobami i starają się zapanować nad różnymi kanałami uzyskiwania informacji przez podmiot dezinformowany”[324]. Biorąc pod uwagę zróżnicowanie przedstawionych propozycji definicyjnych, przy uwzględnieniu ich walorów i krytycznym potraktowaniu niedostatków należy przyjąć, że współcześnie dezinformacji nie można rozpatrywać w wąskim znaczeniu tylko jako celowego przekazywania sfabrykowanych informacji z intencją wprowadzania w błąd i uzyskiwania tą drogą zaplanowanych rezultatów. Należy zauważyć, że przytaczane ujęcia, w większości koncentrując się tylko na przekazywaniu przez podmiot (podmioty) dezinformujące spreparowanych celowo informacji, pomijają lub traktują pobieżnie takie

[322] M.J. Wachowicz, *Ujęcie teoretyczne pojęcia dezinformacji*, „Wiedza Obronna” 2019, nr 1–2, s. 250.
[323] Zob. J. Borecki, *Dezinformacja jako zagrożenie dla prywatnych i publicznych przedsiębiorstw*, „The Warsaw Institute Review” – edycja specjalna, 2017, s. 8.
[324] M. Świerczek, *„System matrioszek, czyli dezinformacja doskonała. Wstęp do zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego” 2018, nr 10, s. 213–214.

elementy, jak inscenizowanie określonych wydarzeń, podstępne gesty czy deklaracje, eksponowanie i wyolbrzymianie sukcesów oraz ukrywanie i minimalizowanie niepowodzeń. W rzeczywistości współczesna dezinformacja stanowi skomplikowany system przedsięwzięć (politycznych, gospodarczych, dyplomatycznych, militarnych, społecznych, cybernetycznych) realizowanych zarówno w sferze informacyjnej, jak i pozainformacyjnej po to, by wywierać wpływ, indoktrynować, destabilizować, powodować konflikty czy kierować aktywność organizacyjną i decyzyjną tych, którzy są dezinformowani, w takie obszary, które będą sprzyjać (służyć) realizacji krótkoterminowych i dalekosiężnych planów podmiotu dezinformującego. Dezinformacja w swym rdzeniu opiera się na specyficznych rodzajach informacji: fałszywych, tendencyjnych (gloryfikujących lub oczerniających), wycinkowych, które mają nie tylko wprowadzać w błąd odbiorców, ale w połączeniu z działaniami pozainformacyjnymi tworzyć wiedzę pozorną, bezużyteczną czy wręcz szkodliwą, na bazie której powstawać będą błędne decyzje i sposoby reagowania korzystne z punktu widzenia podmiotu dezinformującego.

Podsumowując ten fragment analiz, można zatem stwierdzić, że istota dezinformacji sprowadza się do zaplanowanych, świadomych, podstępnych, wzajemnie sprzężonych wielowątkowych działań w sferze informacyjnej i pozainformacyjnej realizowanych przez ukrywający swoje rzeczywiste zamierzenia podmiot dezinformujący, którym może być zarówno jednostka ludzka, jak i państwo (koalicja państw, grupa państw połączonych sojuszem), ale także grupy interesu, ugrupowania polityczne czy duże korporacje biznesowe. Celem tych działań jest wywoływanie reakcji, kształtowanie opinii, budowanie relacji, odwracanie uwagi, zniekształcanie obrazu rzeczywistości, tworzenie klimatu politycznego, inspirowanie do podejmowania decyzji lub ich zaniechiwania w sposób zgodny z celami podmiotu dezinformującego i zabezpieczających jego interesy. Różnorodność stosowanych zabiegów, form działania oraz koncentracja dezinformacji na określonych sferach spowodowała, że badacze oraz praktycy zainteresowani tą działalnością zaczęli sporządzać różnorodne jej klasyfikacje. A. Golicyn, opierając się na wewnętrznych opracowaniach radzieckich służb specjalnych z lat 50. XX w., wyróżnił dezinformację strategiczną, polityczną, wojskową, techniczną, ekonomiczną oraz dyplomatyczną[325]. Rafał Brzeski, bazujący na przeglądzie publikacji amerykańskich i radzieckich, wskazuje na występowanie dwóch podstawowych typów dezinformacji:

[325] A. Golicyn, dz. cyt., s. 53.

strategicznej i taktycznej. Dezinformacja taktyczna w świetle ustaleń R. Brzeskiego może mieć charakter:

– polityczny (np. opublikowanie sfabrykowanej notatki wewnętrznej polityka wybranego do skompromitowania);
– wojskowy (np. podsuwanie nieprawdziwych danych technicznych jakichś rodzajów uzbrojenia);
– ekonomiczny (np. wprowadzanie do obiegu zmanipulowanych danych dotyczących stanu gospodarki danego państwa).

Dezinformacja taktyczna to działanie o charakterze raczej krótkotrwałym. Jest ona zbliżona do wprowadzania w błąd w jednej lub kilku przenikających się kwestiach (chociaż nie tożsama z nim). Zachowując atrybut celowej działalności o charakterze planowym, ma jednak zdecydowania krótszą perspektywę czasową, liczoną raczej w wymiarze miesięcy niż lat.

Dezinformacja strategiczna z kolei polega na systematycznym przekazywaniu (podmiotowi lub podmiotom będącym celem oddziaływań dezinformacyjnych) przez długi czas (liczony nawet w dziesiątkach lat) fałszywych sygnałów i informacji oraz sfabrykowanych przekazów w celu wytworzenia nieprawdziwego obrazu różnych sytuacji, skutkującego ich mylną oceną przekładającą się na procesy decyzyjne. Dezinformacja strategiczna jest ukierunkowana na stopniowe przejmowanie inicjatywy i narzucanie sposobów postrzegania rzeczywistości odpowiadających interesom podmiotu dezinformującego[326]. Radosław Bielawski i Agata Ziółkowska, odwołując się do dorobku innych autorów (w tym zwłaszcza Marka Wrzoska[327]) oraz posługując się kryterium sfery oddziaływania, wyróżniają cztery kategorie dezinformacji: polityczną, ekonomiczną, naukowo-techniczną oraz wojskową. Dezinformacja polityczna według przywołanych autorów może być prowadzona w odniesieniu do wewnętrznej i zewnętrznej sfery aktywności państwa. W sferze wewnętrznej obiektem oddziaływania tego rodzaju dezinformacji prowadzonej przez dane państwo jest jego społeczeństwo. W takim ujęciu ma ona za zadanie kształtowanie pożądanych opinii, zachowań i postaw osób tworzących to społeczeństwo. Dezinformacja w sferze zewnętrznej ma na celu stworzenie

[326] Zob. R. Brzeski, *Dezinformacja. Skrypt,* Warszawa 2011, s. 3, https://forumemjot.wordpress.com/2012/06/04/dezinformacja-skrypt-warszawa-2011-rafal-brzeski/ [dostęp: 1.10.2020 r.].
[327] Zob. M. Wrzosek, *Dezinformacja – skuteczny element walki informacyjnej*, „Zeszyty Naukowe AON" 2012, nr 2, s. 22.

pozytywnego wizerunku państwa na arenie międzynarodowej[328]. W sytuacjach, gdy działania danego państwa rodzą (lub mogą rodzić) krytykę i sprzeciw społeczności międzynarodowej, zadaniem dezinformacji staje się zamaskowanie rzeczywistych celów i intencji takich działań oraz uzyskanie dla nich akceptacji i poparcia. Dezinformacja ekonomiczna jest ukierunkowana na wprowadzanie w błąd w zakresie stanu osiągnięć ekonomiczno-gospodarczych (w tym także dotyczących gospodarki obronnej).

Dezinformacja naukowo-techniczna jest realizowana w celu ukrycia przed potencjalnymi przeciwnikami rzeczywistego stanu osiągnięć i odkryć naukowych, posiadanego doświadczenia, zmian w teorii sztuki wojennej, nowych rodzajów wyposażenia wojskowego oraz perspektyw i możliwości wdrożenia innowacji technicznych. Dezinformacja wojskowa może być według przywoływanych autorów realizowana w stosunku do przeciwnika, wojsk własnych oraz otoczenia. Oddziaływanie na przeciwnika dotyczy spowodowania przekazywania przez jego systemy rozpoznania błędnych informacji. Celem dezinformacji adresowanej do własnych sił zbrojnych jest powodowanie ich działań, utwierdzających przeciwnika co do prawdziwości wniosków wyciągniętych z rozpoznania[329]. Uwzględniając istniejące ustalenia, można, zdaniem autora, wyróżnić współcześnie następujące rodzaje wzajemnie przenikających się i komplementarnych gałęzi (nurtów) dezinformacji: polityczną, ekonomiczną, militarną, społeczną, ekologiczną, kulturową i ideologiczną.

Jeżeli bierzemy pod uwagę dezinformację polityczną, to obejmuje ona przedsięwzięcia oddziaływające na kształt i funkcjonowanie systemów politycznych poszczególnych państw (np. wpływanie na wyniki wyborów, zmiany w ustawodawstwie [także na poziomie konstytucyjnym], nominacje na wysokie stanowiska państwowe, kreowanie i podtrzymywanie wewnętrznych konfliktów politycznych itp.). Dezinformacja polityczna prowadzona jest w celu wywierania wpływu na funkcjonowanie systemów politycznych z zewnątrz (prowadzić ją mogą inne państwa), może być też działaniem o charakterze wewnętrznym. Dezinformacja polityczna to także przedsięwzięcia podejmowane

[328] Należy zauważyć, że jest to zbyt zawężone rozumienie dezinformacji zewnętrznej, która służyć może również podważaniu autorytetu i pozycji międzynarodowej innego państwa lub państw.

[329] Zob. R. Bielawski, A. Ziółkowska, *Media społecznościowe a kształtowanie bezpieczeństwa państwa,* [w:] *Człowiek a technologia cyfrowa – przegląd aktualnych doniesień*, P. Szymczyk, K. Maciąg (red.), Lublin 2018, s. 90–91.

w ramach oddziaływania na stosunki międzynarodowe i funkcjonowanie systemu międzynarodowego.

W przypadku dezinformacji militarnej chodzi o wywoływanie pożądanych nastrojów, poglądów, ocen i zachowań związanych z planami i działaniami wojskowymi strony dezinformującej, m.in. może to być błędne ocenianie potencjału i zamierzeń militarnych, wywoływanie odpowiednich wrażeń w ramach procesu poszukiwania koalicjantów i zjednywania sojuszników, ukrywanie realnych osiągnięć w zakresie techniki wojskowej lub też przedstawianie ich w przeszacowanej wielkości, maskowanie prawdziwych celów interwencji i konfliktów zbrojnych.

Dezinformacja ekonomiczna to działania ukierunkowane na wywoływanie zaplanowanych reakcji rynków w zakresie cen, zawierania kontraktów, podaży surowców, promowanie określonych produktów z ukrytymi celami (np. w zakresie osłabienia gospodarek innych ich producentów czy wejścia do systemów informacyjnych poprzez masowe zakupy sprzętu teleinformatycznego), ukrywanie własnych kłopotów ekonomicznych, przedstawianie zmanipulowanych statystyk ekonomicznych.

W przypadku dezinformacji społecznej są to przekazy generalnie adresowane do szeroko rozumianej opinii publicznej w celu wywoływania reakcji dużych odłamów społeczeństwa. Mogą być one jednak także ukierunkowane na wybrane jego segmenty, np. rolników czy zatrudnionych w jakimś sektorze produkcji przemysłowej. Dezinformacja tego rodzaju realizuje programy wytwarzania w społeczeństwie poglądów i postaw, które są korzystne dla dezinformatora. Dezinformacja społeczna może służyć także do wywoływania odruchów niezadowolenia, buntów społecznych czy tworzenia ruchów poparcia dla jakichś podsuwanych przez dezinformatorów inicjatyw bądź osób aktywnie działających na dużą skalę w życiu publicznym. Dezinformacja ekologiczna to przede wszystkim przedstawianie w sposób nieprawdziwy stanu środowiska naturalnego i występujących w tym zakresie wyzwań, napięć i zagrożeń. Dezinformacja taka często służy wybielaniu własnych działań lub zaniedbań szkodzących temu środowisku. Istotny element dezinformacji ekologicznej stanowi podważanie wiarygodności jego obrońców z jednoczesnym propagowaniem swego rzekomego proekologicznego nastawienia. Istota dezinformacji kulturowej sprowadza się do dezawuowania dorobku tych kultur, które podmiot dezinformujący uznał za gorsze, mniejszościowe, wsteczne czy destrukcyjnie wpływające na kulturę narodową czy inne interesujące dezinformatora sfery, np. demografię. Dezinformacja ideologiczna polega na

propagowaniu zalet i atrakcyjności ideologii popieranej (reprezentowanej) przez dezinformatora przy pomijaniu jej wad i zagrożeń, które może wytworzyć lub – jak w przypadku ideologii totalitarnych – które już stworzyła. Towarzyszą temu dezinformujące przekazy dotyczące ideologii konkurencyjnych lub tych wprost zwalczanych.

Dążąc do ukazania istoty dezinformacji, nie sposób pominąć kwestii podstawowych reguł związanych z jej stosowaniem. W tym kontekście można, modyfikując ustalenia Tomasza Grabowskiego, wskazać, że prowadzenie działalności dezinformacyjnej w taki sposób, aby była ona wieńczona sukcesami, powinno być oparte na następujących zasadach:

– celowości (muszą zostać jasno sprecyzowane cele, określające pożądane rezultaty działań);
– przygotowania (należy zapewnić dostępność odpowiednich środków i instrumentów niezbędnych do realizacji działań dezinformacyjnych oraz dysponować planami ich użycia w przypadkach zaistnieniu określonych skutków pośrednich);
– kompleksowości (należy stosować różnorodne formy oraz metody oddziaływania dezinformacyjnego, połączone z pełnym wykorzystaniem dostępnych środków oraz instrumentów i kanałów dezinformacji);
– scentralizowanego kierowania (musi być zapewniony czytelny i precyzyjny rozdział zadań, koordynacja i współpraca między podmiotami realizującymi działania dezinformacyjne, ważne jest również ograniczenie inicjatyw podmiotów wykonujących zadania na niższych szczeblach operacji dezinformacyjnych);
– wiarygodności (działania dezinformacyjne należy prowadzić w taki sposób, aby zawarty w nich przekaz miał znamiona prawdziwości; nie może to być również działalność nieadekwatna do sytuacji czy nielogiczna);
– multiplikacji (nieprawdziwe informacje muszą pochodzić z możliwie dużej ilości źródeł, tak aby z jednej strony wzajemnie mogły się uwiarygodniać, a z drugiej utrudniać dogłębną analizę);
– elastycznej manewrowości (w razie wywołania niepożądanych efektów lub tylko częściowego powodzenia należy zachować zdolności do przerwania działań dezinformujących bez ujawniania ich celu oraz sprawnego określenia nowych zadań, a także zmiany i przetasowań w gronie wykonawców);
– reżimu czasowego (należy dać podmiotowi dezinformowanemu wystarczającą ilość czasu na odebranie informacji, jej zrozumienie oraz reakcję,

ale ograniczyć możliwości czasowe w zakresie jej gruntownej analizy mogącej doprowadzić do odkrycia manipulacji i oszustw);
– zrównoważonej ciągłości (przekazywanie zmanipulowanych informacji powinno przebiegać systematycznie, intensywność dezinformacji nie powinna także narastać tuż przed rozpoczęciem zaplanowanych w związku z nią innych aktywnych działań);
– spójności (należy zapewnić zgodność celu dezinformacji z celami taktycznymi lub strategicznymi podmiotu dezinformującego w danej dziedzinie lub dziedzinach [np. polityki zagranicznej] oraz zadbać o logiczne związki między formułowanymi przekazami);
– oryginalności (poszukiwanie nowatorskich pomysłów i rozwiązań, dywersyfikacja używanych instrumentów, a także zmienność metod ich stosowania);
– tajności (dbałość o utrzymanie zamierzeń i celów prowadzonych działań dezinformacyjnych w tajemnicy przed podmiotami dezinformowanymi, otoczeniem zewnętrznym oraz szeroko traktowanym własnym środowiskiem, w tym również przed osobami wykonującymi konkretne szczegółowe zadania dezinformacyjne)[330].

Klasyczny zestaw metod działań dezinformacyjnych przedstawiany przez V. Volkoffa to:
– przekazywanie nieprawdy niemożliwej do stwierdzenia (przedstawianie, upublicznianie oczywistej nieprawdy przy założeniu, że nie ma świadków, którzy mogliby te kłamstwa zdemaskować, i nie ma także innych sposobów, aby tą prawdę ujawnić);
– łączenie informacji prawdziwych z nieprawdziwymi (mieszanie przez dezinformatora w wybranych proporcjach prawdy i nieprawdy stosowane w przypadkach, gdy odbiorcy mają pewną wiedzę o danej kwestii, lecz nie znają dokładnie wszystkich dotyczących jej szczegółów);
– zniekształcanie prawdy (opierające się na uznaniu zaistniałych faktów przy jednoczesnym zasugerowaniu takiego motywu i takich okoliczności im towarzyszących, które są w stanie wywołać przekonanie o poprawności [słuszności] sposobu działania podmiotu wspieranego przez dezinformatora);

[330] Zob. T. Grabowski, *Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014–2016)*, „Horyzonty Polityki" 2017, nr 20, s. 43–44.

– rozmycie (polegające na „przykryciu" głównej informacji niewygodnej dla dezinformatora przez dużą ilość informacji drobiazgowych i nieistotnych dla danej sytuacji);
– selekcja faktów (przedstawianie informacji prawdziwych, ale niekompletnych tak, aby przekaz był jak najbardziej korzystny dla podmiotu dezinformującego);
– tendencyjny komentarz (podmiot dezinformujący nie zaprzecza faktom, dokonuje natomiast szerokiego ich omówienia, w ramach którego przez odpowiednie zabiegi interpretacyjne dąży do wywołania korzystnych dla siebie skojarzeń);
– ilustracja (posłużenie się do zobrazowania uogólnień faktem o charakterze jednostkowym);
– uogólnienie (przedstawianie faktu jednostkowego w taki sposób, aby do odbiorców trafił przekaz, że nie jest to zachowanie [zjawisko] unikatowe, lecz że występuje często i w związku z tym nie jest odstępstwem od normy);
– nierówne proporcje (niezależnie od faktycznej ilości informacji, stanowisk czy poglądów o danej kwestii, przedstawia się dużo będących użytecznymi dla strony dezinformującej, a niekorzystne dostarcza się w wymiarze jednostkowym [marginalnym]);
– równe proporcje (przedstawianie przez podmiot dezinformujący podobnej ilości informacji i argumentów za i przeciw, przy czym informacje i argumenty na rzecz jakiejś tezy, opinii czy wniosków przedstawione zostają starannie, np. przy pomocy mających wiarygodny charakter ekspertyz, natomiast argumenty przeciwstawne podawane są co prawda w podobnej ilości, ale w sposób nieciekawy i mało wiarygodny)[331].

Reasumując przeprowadzone rozważania należy podkreślić, że dezinformacja to obecnie jedno z najbardziej destrukcyjnych zagrożeń dla informacyjnego wymiaru bezpieczeństwa. Z uwagi na swój wielowątkowy i wielopłaszczyznowy charakter oraz systematyczny rozwój dostępnych instrumentów, a także doskonalenie metod ich stosowania zagrożenia generowane przez dezinformacje są w stanie wywierać negatywny wpływ na: funkcjonowanie i kształt systemów politycznych, nastroje, relacje i preferencje społeczne, gospodarkę, podejście do problemów ekologicznych, sferę militarną i kulturową. W wymiarze strategicznym szczególnym obiektem działań dezinformacyjnych

[331] Zob. V. Volkoff, dz. cyt., s. 164–166.

jest dążenie do wpływania na kształtowanie polityki międzynarodowej i wewnętrznej państw tak w ujęciu indywidualnym, jak i zbiorowym. Dezinformacja jest w stanie zakłócić percepcję rzeczywistości i kreować zgodne z interesami dezinformujących podmiotów zachowania, postawy jednostek, grup społecznych, podmiotów państwowych czy organizacji i instytucji międzynarodowych. Rewolucja technologiczna, która wprowadziła świat w erę społeczeństwa informacyjnego, spowodowała, że nie tylko na nowo zaczęto dezinformację definiować, ale także w przypadku szeregu państw, dzięki możliwościom, jakie daje Internet, uczyniono z niej jeden z kluczowych instrumentów zabiegania o swoje interesy. Współcześnie dotykać może ona praktycznie każdej sfery funkcjonowania podmiotów będących celem oddziaływań dezinformacyjnych. Jednak w świetle dotychczasowych doświadczeń widać, że największym zainteresowaniem państwowych podmiotów dezinformujących cieszy się sfera bezpieczeństwa ze szczególnym uwzględnieniem jego politycznych, militarnych i gospodarczych aspektów, zwłaszcza zaś zagadnień roli i położenia na arenie międzynarodowej (ogólny wizerunek, wiarygodność sojusznicza, otwartość na współpracę, relacje międzysąsiedzkie, funkcjonowanie w strukturach integracyjnych). Istotnym celem jest również sfera wewnątrzpaństwowa (relacje państwo – obywatel, nastroje społeczne, poziom ich radykalizacji, poziom bezpieczeństwa wewnętrznego, przestrzeganie wartości demokratycznych, transparentność działań państwa i zaufanie do jego instytucji).

3.4. Walka informacyjna

Jeżeli przyjrzeć się kwestii walki informacyjnej, to można powiedzieć, że różne jej formy stosowane były już od czasów starożytnych. Jednak dopiero od połowy XX wieku wraz z dynamicznym rozwojem społeczeństwa informacyjnego ten rodzaj walki stał się autonomiczną formą działań, stosowaną praktycznie we wszystkich dziedzinach życia społecznego, oraz zyskał możliwości prowadzenia w nieograniczonym wymiarze przestrzennym. Dodatkowo siła rażenia środków walki informacyjnej wraz z rozwojem globalnego systemu komunikacji i przekazu informacji systematycznie ulega zwiększeniu. Biorąc pod uwagę rzeczywistą skalę prowadzonych współcześnie walk informacyjnych, poziom zaangażowanych sił i środków oraz ich widoczne i ukryte skutki, należy uznać je za szczególny rodzaj zagrożenia dla bezpieczeństwa, w tym – co zrozumiałe – również dla jego informacyjnego wymiaru. Opracowania

naukowe dotyczące problematyki walki informacyjnej wprawdzie są coraz liczniejsze, jednak w dużej części z nich pomija się kwestię jej istoty, koncentrując uwagę na instrumentach i metodach prowadzenia tej walki. Dostrzec należy także i to, że w wielu przypadkach piszący w sposób nieuprawniony traktują walkę informacyjną jako pojęcie tożsame z wojną informacyjną. Można nawet odnieść wrażenie, na co zwraca uwagę m.in. Marek Wrzosek, że mimo jednoznacznych różnic pomiędzy walką a wojną, stosujący zamiennie oba terminy sprawiają wrażenie osób niezdających sobie z tego sprawy[332]. Potwierdza to Piotr Daniluk, pisząc: „nie sposób nie zauważyć częstego mylenia pojęcia »walka informacyjna« z pojęciem »wojna informacyjna«, które przecież dotyczą różnych poziomów prowadzenia konfrontacji informacyjnej. Być może wytłumaczeniem takiego zjawiska jest to, że w polskiej literaturze dotyczącej bezpieczeństwa ukazały się nieliczne opracowania dotyczące tej problematyki"[333]. Należy zatem w tym miejscu jednoznacznie podkreślić, że w przypadku specyficznych zagrożeń bezpieczeństwa informacyjnego, jakim jest walka i wojna informacyjna, nie tylko nie można nie dostrzegać zasadniczych różnic pomiędzy nimi, ale i pomijać faktu, iż trudno współcześnie mówić o tym, że miała już miejsce jakaś wojna informacyjna[334]. Aby nie ulegać rodzącym poznawczy zamęt przekazom płynącym z opracowań zawierających poddane powyżej krytyce poglądy, warto przypomnieć, że w ujęciu słownikowym walka to m.in. starcie uzbrojonych grup, oddziałów, zorganizowane działanie sił zbrojnych w celu pokonania przeciwnika, zmaganie się pojedynczych przeciwników lub zespołów, działanie mające na celu: usunięcie czegoś, zdobycie, odzyskanie kogoś lub czegoś, ścieranie się sprzecznych interesów, poglądów[335]. W filozoficznym ujęciu, rozpropagowanym przez Tadeusza Kotarbińskiego, walka to wszelkie działania co najmniej dwupodmiotowe, gdzie przynajmniej jeden z podmiotów przeszkadza drugiemu[336]. Jak zauważa przywoływany wcześniej M. Wrzosek, walka to działanie przeciwstawne, konfrontacyjne, zmierzające do zmiany istniejącego stanu rzeczy[337]. Na ogół walka

[332] Zob. M. Wrzosek, *Wojny przyszłości. Doktryna, technika, operacje militarne*, Warszawa 2018, s. 189.
[333] P Daniluk, *Współczesne wymiary konfrontacji informacyjnej*, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, nr 2, s. 37.
[334] T.R. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016, s. 129.
[335] Zob. *Słownik języka polskiego PWN*, https://sjp.pwn.pl/sjp/walka;2534473.html [dostęp: 10.05.2021 r.].
[336] Zob. T. Kotarbiński, *Traktat o dobrej robocie*, Warszawa 1982, s. 221.
[337] Zob. M. Wrzosek, *Wojny przyszłości…*, s. 188.

charakteryzuje się tym, że uczestniczące w niej podmioty dążą do celów niezgodnych i czynią to świadomie, uwzględniając w swoich planach działania strony przeciwnej. Istotą walki jest zorganizowane bezpośrednie oddziaływanie na przeciwnika. Wojnę natomiast definiujemy jako konflikt zbrojny między państwami, blokami państw, narodami. Jest to kontynuacja polityki środkami przemocy, mająca na celu realizację określonych interesów politycznych, ekonomicznych lub ideologicznych. Inaczej rzecz ujmując, wojna to prowadzenie polityki z użyciem środków przemocy, w których dominującą metodą jest walka prowadzona przez zorganizowane siły zbrojne[338]. Należy zatem podkreślić, że wojna to zjawisko bardziej złożone i różnorodne, a walka w różnych formach może stanowić jej przejaw. Może, chociaż nie musi, ponieważ możliwe jest prowadzenie walki lub walk bez przechodzenia w stan wojny[339]. Czym zatem jest walka informacyjna? W opisowym ujęciu H. Batorowskiej walka informacyjna ukazana jest jako kategoria działań, w ramach których dochodzi do starcia co najmniej dwóch przeciwstawnych stron, które walcząc o istotne dla nich dobra, prowadzą rozpoznanie, realizują działania ofensywne, defensywne i opóźniające. W każdym z tych aspektów walki, wykorzystując różne techniki, pozyskuje się, gromadzi, przetwarza, analizuje i wykorzystuje informacje. Walka informacyjna to w istocie szereg operacji informacyjnych mających zapewnić zwycięstwo m.in. poprzez:

– osłabianie czujności i woli walki przeciwnika;
– utrwalanie postaw neutralnych w jego szeregach i otoczeniu;
– wzmacnianie postaw przyjaznych dla strony atakującej;
– skuteczne maskowanie własnych zamierzeń;
– zapewnienie bezpieczeństwa realizacji własnych planów.

Walka informacyjna może być prowadzona tak w sferze militarnej, jak i pozamilitarnej i toczy się zarówno w publicznej, jak i prywatnej całościowo traktowanej przestrzeni informacyjnej, w której funkcjonują strony walczące[340]. Punktem krytycznym, po przekroczeniu którego każda walka staje się walką informacyjną, jest uczynienie podstawą stosowanych działań dezinformacji i manipulacji. W tego rodzaju walce informacja staje się zarówno bronią ofensywną, jak i celem ataków[341]. W projekcie doktryny bezpieczeństwa

[338] Zob. F. Skibiński, *Rozważania o sztuce wojennej*, Warszawa 1978, s. 29.
[339] Zob. W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne w XXI wieku*, M. Kubiak, S. Topolewski (red.), Siedlce-Warszawa 2016, s. 37.
[340] Zob. O. Wasiuta" R. Klepka dz. cyt., t. 2, Kraków 2019, s. 503.
[341] Zob. tamże.

informacyjnego RP z 2015 r., w którym podjęto próbę przyjęcia definicji szeregu ważnych pojęć, walka informacyjna została określona jako „czynności polegające na oddziaływaniu na informacje i/lub systemy informacyjne w celu kształtowania i przejmowania procesów decyzyjnych przeciwnika (zautomatyzowanych oraz z udziałem czynnika ludzkiego), przy jednoczesnej ochronie własnych procesów decyzyjnych; w wymiarze wojskowym także działalność mająca na celu wywarcie pożądanego wpływu na wolę, rozumienie i zdolności przeciwników, potencjalnych przeciwników lub innych stron konfliktu, wspierających cele danej misji”[342]. W walce informacyjnej, według projektu doktryny, mogą być stosowane działania ofensywne i defensywne. Do pierwszej grupy jej autorzy zaliczyli: operacje psychologiczne, pozorację, destrukcję, walkę elektroniczną, ataki informatyczne, działania z zakresu komunikacji społecznej. W grupie działań defensywnych umieścili: zapewnienie bezpieczeństwa informacyjnego, osłonę, działania kontrpropagandowe, działania kontrwywiadowcze, walkę elektroniczną oraz informacyjne działania specjalne[343].

Jeżeli zanalizować ujęcia bardziej zwięzłe o charakterze definicyjnym, to na pewno należy przywołać stanowisko jednego z uznanych badaczy zagadnienia, Leopolda Ciborowskiego, które zostało zaprezentowane w *Słowniku terminów z zakresu bezpieczeństwa narodowego*. Walka informacyjna jest tam zdefiniowana jako „działania kooperacji negatywnej wzajemnej, w których cel destrukcyjnego oddziaływania skoncentrowany jest na systemach informacyjno-sterujących przeciwnych stron. Przedmiotem walki informacyjnej jest system informacyjno-sterujący”[344]. Inna definicja zamieszczona we wspomnianym słowniku mówi, że walka informacyjna to „konflikt, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią. Walka informacyjna obejmuje także fizyczną destrukcję infrastruktury, która wykorzystywana jest przez przeciwnika do działań operacyjnych”[345]. Z kolei według Józefa Kosseckiego „Walka informacyjna jest szczególnym przypadkiem procesu sterowania społecznego, którego celem jest niszczenie przeciwnika za pomocą informacji”[346]. Narzędziem tej walki, jak podkreśla cytowany autor, jest informacja niszcząca, która:

[342] *Doktryna bezpieczeństwa informacyjnego…*, s. 3.
[343] Zob. tamże.
[344] *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2002, s. 153.
[345] Tamże.
[346] J. Kossecki, *Totalna wojna informacyjna XX wieku a II RP*, Kielce 1997, s. 2.

– osłabia struktury funkcjonalne przeciwnika (przede wszystkim poprzez utrudnianie przekazu informacji między decydentami a wykonawcami);
– daje asumpt do nietrafnych decyzji i wywołuje w ten sposób błędne działania przeciwnika (odbywa się to na drodze wprowadzania do systemu przeciwnika błędnych algorytmów decyzyjnych i realizacyjnych, które nie tylko go osłabiają, ale mogą także doprowadzić do samozniszczenia)[347].

Nawiązująca do poglądów J. Kosseckiego Angelika Gronowska-Starzeńska mianem walki informacyjnej określa „proces, w którym na skutek ataku informacyjnego dochodzi do zakłócenia procesów informacyjnych (poznawczo-decyzyjnych) odbywających się w społeczeństwie niszczonym w celu przejęcia tych procesów przez niszczyciela zgodnie z jego interesem"[348].

Jak podkreśla przywoływany wcześniej M. Wrzosek, u podstaw formułowania ogólnej koncepcji pojmowania walki informacyjnej leżało jej militarne ujęcie oparte na stosowaniu systemów informacyjnych w celu obniżenia zdolności obronnych przeciwnika. Wychodząc z tego ogólnego rozumienia walki informacyjnej w wymiarze wojskowym, na potrzeby pozawojskowe przyjęto, że celem działań w ramach walki informacyjnej (a zatem jej istotą) będzie „niszczenie zasobów informacyjnych przeciwnego państwa, jego sieci komputerowych oraz dezorganizacja instytucji finansowych, a także utrudnianie pracy systemów telekomunikacji publicznej czy instytucji rządowych"[349]. Próbę określenia tego, czym jest walka informacyjna, podjęli także Agnieszka Bógdał-Brzezińska i Marcin Gawrycki. Według tych autorów jest to „zorganizowana w formę przemocy aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłanej przez nie informacji przed podobnym działaniem przeciwnika"[350]. Wyraźny brak adekwatności tego ujęcia wiąże się z ograniczeniem pojęcia walki informacyjnej

[347] Zob. tamże.
[348] A. Gronowska-Starzeńska, *Walka informacyjna – wybrane problemy w ujęciu cybernetycznym*, „Zeszyty Naukowe Akademii Sztuki Wojennej" 2017, nr 4, s. 39–40.
[349] M. Wrzosek, *Zmagania o informacje we współczesnych organizacjach*, „Zeszyty Naukowe AON" 2010, nr 4, s. 46.
[350] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 323.

tylko do działalności państwa i tylko tej skierowanej wyłącznie na zewnątrz. Podobnie zawężone podejście prezentuje Ryszard Szpyra. Według tego autora walka informacyjna to „zorganizowana w formie przemocy militarna aktywność państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłania przez nie informacji przed podobnym działaniem przeciwnika”[351]. Zacytowana definicja walki informacyjnej obejmuje wyłącznie aktywność państwa w sferze zewnętrznej i do tego jest ograniczona do sfery militarnej. Bardzo interesującą i w znacznej mierze odzwierciedlającą główne cechy walki informacyjnej propozycję definicyjną sformułował Piotr Sienkiewicz, twierdząc, że należy ją traktować jako „całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych). Istotą tak rozumianej walki informacyjnej jest:

1) zniszczenie (lub degradacja wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych;
2) zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystanych systemów informacyjnych”[352].

Koresponduje z tym stanowiskiem pogląd cytowanego przez Michała Wojnowskiego rosyjskiego teoretyka Siergieja Komowa, który rozumie walkę informacyjną jako „całokształt wsparcia informacyjnego, informacyjnego przeciwdziałania oraz informacyjnej ochrony własnych zasobów prowadzonych według jednolitego planu w celu zdobycia i utrzymania przewagi informacyjnej nad stroną przeciwną”[353]. Czytelnie kwestię istoty walki informacyjnej charakteryzuje także M. Wrzosek, który wzorując się na poglądach L. Ciborowskiego, wskazuje, że „walka informacyjna to kooperacja negatywna wzajemna, realizowana w sferze zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej, gdzie każdemu działaniu jednej

[351] R. Szpyra, *Operacje informacyjne państwa w działaniach sił powietrznych*, Warszawa 2002, s. 149.
[352] P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, s. 375, https://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf [dostęp: 10.05.2021 r.].
[353] M. Wojnowski, *Terroryzm w służbie geopolityki. Konflikt rosyjsko-ukraiński jako przykład realizacji doktryny geopolitycznej Aleksandra Dugina i koncepcji „wojny buntowniczej” Jewgienija Messnera*, „Przegląd Bezpieczeństwa Wewnętrznego” 2014, nr 11, s. 77.

strony przyporządkowane jest działanie antagonistyczne strony drugiej”[354]. W konsekwencji takiego ujęcia cytowany autor, uwzględniając czynnik kooperacji negatywnej, wyróżnia dwa podsystemy walki informacyjnej:

– zakłócania systemu informacyjnego przeciwnika poprzez wprowadzanie do niego odpowiednich wiadomości i komunikatów oraz destrukcyjnego oddziaływania wobec jego nośników informacji;
– obrony informacyjnej własnych systemów opartej na przeciwdziałaniu rozpoznaniu i zakłócaniu informacyjnemu przez przeciwnika[355].

W odniesieniu do kwestii rozumienia istoty walki informacyjnej na uwagę zasługują także bardzo dobrze udokumentowane źródłowo i interesujące poznawczo analizy przeprowadzone przez Marka Madeja. Badacz ten zwraca uwagę na przydatność zastosowania w podejściu do analizowanego terminu perspektywy inkluzywnej i ekskluzywnej. Jak zauważa, w przypadku pierwszym chodzi o różne działania mające na celu niszczenie, modyfikowanie lub zdobywanie i wykorzystywanie posiadanych przez przeciwnika zasobów informacji oraz systemów ich gromadzenia, przechowywania przetwarzania i przesyłania, jak również ochronę własnych zasobów informacyjnych i systemów przed akcjami przeciwnika. Przy takim rozumieniu walki informacyjnej zakres stanowiących jej istotę działań nie ogranicza się do operacji prowadzonych przy użyciu technologii informatycznych, lecz obejmuje też wiele innych form aktywności, zarówno realizowanych fizycznie, jak w warstwie symbolicznej bez wykorzystania infrastruktury teleinformatycznej[356]. M. Madej, optujący za szerokim inkluzyjnym definiowaniem walki informacyjnej, podkreśla, że „To, co w części definicji szerszych walki informacyjnej stanowi element szczególnie istotny, ale wciąż jeden z wielu, w definicjach ekskluzywnych jest jedynym składnikiem. W nich zakres walki informacyjnej jest bowiem ograniczony do działań przy użyciu technologii informatycznych oraz w ramach powstałych w wyniku ich rozwoju powiązań o charakterze wirtualnym”[357].

[354] M. Wrzosek, *Zmagania o informacje…*, s. 43.
[355] Zob. tamże.
[356] Zob. M. Madej, *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007, s. 324–325.
[357] Tamże, s. 325.

Tabela 8. Zachodnie ujęcia terminu „walka informacyjna"

Walka informacyjna to działania informacyjne prowadzone w czasie kryzysu lub konfliktu dla osiągnięcia pożądanych celów w relacjach z przeciwnikiem lub wsparcia działań prowadzących do tych celów. *Joint Doctrine for Information Operations, Joint PUB 3-13,* Joint Chiefs of Staff, Washington 1998
Walka informacyjna to działania informacyjne, prowadzone dla obrony własnej informacji i systemów informacyjnych lub dla atakowania i wywarcia wpływu na informację lub systemy informacyjne przeciwnika, jest prowadzona głównie w czasie kryzysu lub konfliktu, defensywny komponent tej walki, podobnie jak obrona powietrzna, realizowany jest w każdej fazie działań militarnych, od pokoju do wojny. *AFDD2-5 Information Operations,* USAF, 1998
Walka informacyjna to działania podejmowane dla osiągnięcia przewagi informacyjnej polegające na wpływaniu na informacje przeciwnika, jego procesy zależne od informacji, informacyjne systemy i sieci komputerowe, przy jednoczesnej obronie własnych informacji, procesów zależnych od informacji, zasobów informacyjnych, systemów i sieci komputerowych. *DOD & Joint Staff – CJCSI 3210.01,* in: *FM100-6 Information Operations,* Headquarters, Department of the Army, 1996
Walka informacyjna to działania podejmowane dla osiągnięcia przewagi informacyjnej, prowadzone w ramach wspierania narodowej strategii militarnej. Działania te mają na celu wpływanie na informację i systemy informacyjne przeciwnika przy równoczesnej obronie własnej informacji i systemów. E. Paige, [in:] G. Ivefors, *Information Warfare, Defeat the Enemy before Battle-a warfare Revolution in the 21 Century?,* www.kla.liu.eci-guniv/infowar, 26 January 2001
Walka informacyjna, w najogólniejszym sensie, jest użyciem informacji dla osiągnięcia własnych narodowych celów. Podobnie jak dyplomacja, ekonomiczna rywalizacja czy użycie sił zbrojnych, informacja jest kluczowym czynnikiem narodowej potęgi. Ponadto, co jeszcze ważniejsze, informacja staje się głównym narodowym zasobem, który wspiera dyplomację, ekonomiczną rywalizację oraz przemoc militarną. Walka informacyjna w tym sensie może być postrzegana jako konflikt między państwami lub narodami, prowadzony częściowo przez globalną infrastrukturę informacyjną i komunikacyjną. J. Arquila, D. Ronfeld*, Cyberwar is Coming,* "Comparative Strategy", december 1993, p. 41–65, za: G. Stein. *Information Warfare,* [in:] A.D. Campen, D.H. Deart, R.T. Gooddenn, *Cyberwar: Security, Strategy and Conflict in the Information Age,* AFCEA International Press, Fairfax 1996
Walka informacyjna jest formą konfliktu, w którym bezpośrednie atakowanie systemów informacyjnych jest środkiem atakowania wiedzy i przekonań przeciwnika. Walka informacyjna może być prowadzona jako element działań wojennych – w postaci wojny sieciowej (*net war*) lub cyberwojny (*cyberwar*) – lub może przybrać formę walki samodzielnej. R. Szafrański, *Cyberwar: A Theory of Information Warfare: Preparing for 2020*, [in:] A.D. Campen, D.H. Deart, R.T. Gooddenn, *Cyberwar: Security, Strategy and Conflict in the Information Age,* AFCEA International Press, Fairfax 1996

Źródło: P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009, s. 81–82.

Tabela 9. Walka informacyjna na przykładzie państw

Państwo	Pojęcie
Stany Zjednoczone	Walka informacyjna to działania podejmowane w celu uzyskania przewagi w tym zakresie przez kształtowanie procesów i systemów informacyjnych oraz sieci komputerowych przeciwnika, przy jednoczesnej ochronie własnych zasobów informacyjnych.
RFN	Walka informacyjna jest rozumiana jako wszechstronne wykorzystywanie informacji i technik łączności, jak również technik przeznaczonych do zakłócania i niszczenia wrogich ośrodków informacji i systemów łączności w czasie kryzysu i konfliktu celem osiągnięcia przewagi strategicznej i taktycznej.
Wielka Brytania	Walka informacyjna to dążenie do obezwładniania przeciwnika przez zniszczenie jego systemów komputerowych, finansowych, telekomunikacyjnych czy kontroli ruchu.
Federacja Rosyjska	Walka informacyjna to kompleks przedsięwzięć obejmujących wsparcie, przeciwdziałanie i obronę informacyjną, prowadzonych według jednolitej koncepcji i planu, w celu wywalczenia i utrzymania panowania nad przeciwnikiem w dziedzinie informacyjnej podczas przygotowania operacji wojskowych oraz prowadzonych działań bojowych.
Polska	Walka informacyjna to zorganizowana w formie przemocy aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania się przeciwnika lub przepływających przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłania przez nie informacji przed podobnym działaniem przeciwnika. Walka informacyjna to kooperacja negatywnie wzajemna, przynajmniej dwupodmiotowa, realizowana w sferach: zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej, gdy każdemu działaniu jednej strony przyporządkowane jest działanie antagonistyczne strony drugiej.
Sojusz Północnoatlantycki	Walka informacyjna to działania informacyjne prowadzone w okresie kryzysu i/lub konfliktu zbrojnego z zamiarem promowania określonego celu politycznego lub wojskowego w odniesieniu do wskazanego przeciwnika lub przeciwników.

Źródło: A. Żebrowski, *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Roczniki Kolegium Analiz Ekonomicznych" 2013, nr 29, s. 455.

Jeżeli przyjrzeć się poglądom teoretyków zachodnich na kwestię walki informacyjnej (zebranych w formach tabelarycznych przez P. Sienkiewicza

i H. Świebodę[358] oraz A. Żebrowskiego[359]), to można zauważyć, iż koncentrują się one na traktowaniu tej walki jako działań informacyjnych prowadzonych zwłaszcza w czasie kryzysów i konfliktów tak w celu uzyskania przewagi informacyjnej, jak i ochrony własnych zasobów informacyjnych. Opierając się na dokonanym przeglądzie stanowisk dotyczących definiowania pojęcia „walka informacyjna", można w rezultacie uznać, że jest to zbiór działań informacyjnych (o defensywnym i ofensywnym charakterze) prowadzonych w sposób zorganizowany, stosownie do możliwości i zamiarów stron (mogą nimi być podmioty: państwowe, pozapaństwowe, działające na zlecenia państw, nieformalne grupy aktywistów itp.) walczących, mających na celu przeforsowanie i realizację określonych, posiadających konkretny, chociaż ograniczony zakres interesów (politycznych, wojskowych, ekonomicznych itp.) w odniesieniu do konkretnego przeciwnika lub przeciwników[360].

Odwołując się m.in. do dorobku Dorothy E. Denning[361] oraz M. Madeja[362], można wskazać na istnienie dwóch zasadniczych odmian walki informacyjnej:

– walki defensywnej;

– walki ofensywnej.

Ofensywną walkę informacyjną można określić jako zespół działań, w ramach których strona atakująca dąży do zdobycia lub wykorzystania w zaplanowany przez siebie sposób jakiegoś zasobu lub zasobów informacyjnych strony atakowanej w celu zmniejszenia ich wartości dla posiadacza, a czasami jednocześnie zwiększenia ich wartości dla siebie. Z kolei defensywną walkę informacyjną można zdefiniować jako zespół działań prowadzonych przez stronę broniącą się, mających na celu obronę przed zwiększeniem dostępu do jej zasobów informacyjnych przez stronę atakującą oraz utrzymanie dostępności i integralności dla siebie.

Z punktu widzenia konfliktów zbrojnych znaczenie walki informacyjnej dobitnie podkreśla Bolesław Balcerowicz, który opierając się na poglądach Jeffrey'a Barnetta, wskazuje, że:

– zastosowanie walki informacyjnej będzie niezbędne do uzyskania zwycięstwa;

---

[358] Zob. tabela 8.
[359] Zob. tabela 9.
[360] Zob. W. Fehler, *O pojęciu bezpieczeństwa informacyjnego…*, s. 39.
[361] Zob. D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 32–38.
[362] Zob. M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*, s. 327.

– walka informacyjna może mieć charakter autonomiczny, może wspierać działania militarne, może też być wiodącą formą działań wspieraną operacjami militarnymi;
– walka informacyjna zawierać będzie elementy ofensywne i defensywne;
– walka informacyjna będzie prowadzona na poziomie strategicznym, operacyjnym i taktycznym;
– siły zbrojne muszą być przygotowane do działań w warunkach skutecznych oddziaływań informacyjnych przeciwnika[363].

Jeżeli chodzi o ukierunkowanie walki informacyjnej, to jak wskazuje L. Ciborowski[364], prowadzący tego rodzaju walkę starają się uwzględniać najnowsze osiągnięcia naukowe, przy pomocy których da się oddziaływać na różne elementy infosfery przeciwnika.

Tabela 10. Ukierunkowanie walki informacyjnej

Ukierunkowanie walki informacyjnej
Zdalne wprowadzanie do sieci informatycznych wirusów komputerowych, dostosowanych programowo do samopowielania i szybkiego rozprzestrzeniania.
Lokowanie w systemach informatycznych tzw. bomb logicznych, które jako odpowiednio opracowane aplikacje programowe będą dostosowane do uaktywniania się na określone wcześniej sygnały lub według zaprogramowanych wcześniej reżimów czasowych.
Blokowanie wymiany danych w torach transmisyjnych, deformowanie treści oraz wprowadzanie do systemów informacyjnych nieprawdziwych treści logicznych za pośrednictwem środków masowego przekazu, kanałów łączności rządowej i wojskowych systemów dowodzenia.
Wprowadzanie wirusów komputerowych do rządowych oraz komercyjnych sieci i systemów informatycznych, jak również układów zdalnego sterowania tymi systemami.
Wytwarzanie impulsów wielkiej mocy, zaprogramowanych na niszczenie urządzeń elektronicznych, a także środków biologicznych – specjalnych mikrobów – do niszczenia obwodów elektronicznych i materiałów izolacyjnych.
Stosowanie broni elektronicznej przeciwko wybranym elementom infrastruktury i przemysłu, powodujące np. paraliżowanie łączności, transportu, dopływu energii elektrycznej, czyli paraliżowanie życia w danym regionie.

Źródło: L. Ciborowski, *Potencjalne zagrożenia – identyfikacja i charakterystyka*, „Myśl Wojskowa" 2000, nr 4, s. 86–87.

[363] Zob. B. Balcerowicz, *O pokoju. O wojnie. Między esejem a traktatem*, Warszawa 2013, s. 196–197.
[364] Zob. tabela 10.

Analizom istoty i znaczenia walki informacyjnej jako pojęcia ważnego, ale wysoce złożonego, towarzyszą także bardzo pomocne dla właściwego zrozumienia jej istoty wysiłki na rzecz zestawienia jej cech. Wśród badaczy, którzy mają w tej materii niekwestionowany dorobek należy wymienić A. Żebrowskiego oraz M. Wrzoska. Pierwszy z nich wskazuje na następujące wyróżniające cechy walki informacyjnej:

– anonimowość przeciwnika, który funkcjonuje w strukturze wirtualnej, jest więc trudny do wskazania i zidentyfikowania:
– specyfikę terenu działań, którym jest globalna sieć informacyjna;
– brak granic geograficznych (przestrzennych) i politycznych;
– możliwość prowadzenia tego rodzaju walki w dowolnym miejscu i czasie;
– wielość obiektów mogących być celem ataku;
– stosowanie rozwiązań wykorzystujących powszechny dostęp do nowoczesnych technik teleinformatycznych i komunikacyjnych;
– brak jasnego prawa, rodzący niejasną odpowiedzialność związaną z prowadzeniem walki;
– słabość i niedookreśloność przedsięwzięć prewencyjnych;
– szybkość działań;
– wielopłaszczyznowość (walka informacyjna może być elementem operacji politycznej, gospodarczej i innej, może mieć także różny zasięg)[365].

Z kolei M. Wrzosek zwraca uwagę, iż specyfikę walki informacyjnej określa to, że:

– bezpośrednio nie powoduje ona ofiar śmiertelnych oraz istotnych zniszczeń fizycznych;
– nie wymaga fizycznej obecności w miejscu ataku;
– osoby uczestniczące w walce na ogół nie są narażone na utratę życia lub zdrowia;
– koszty psychiczne dla bezpośredniego sprawcy, towarzyszące podjęciu działań w ramach walki informacyjnej, są niskie;
– jest działaniem systemowym o szerokim zasięgu;
– wywołuje złożone (często długotrwałe i kosztowne) skutki mogące dotykać wielu różnych składników systemów informacyjnych i ich użytkowników znajdujących się w odległych od siebie regionach geograficznych;

[365] Zob. A. Żebrowski, *Determinanty walki informacyjnej*, [w:] *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania*, H. Batorowska (red.), Kraków 2017, s. 94.

– przedmiotem jej destrukcyjnego oddziaływania są nie tylko poszczególne elementy składowe systemu informacyjnego, lecz przede wszystkim istniejące między nimi powiązania[366].

W podsumowaniu należy podkreślić potrzebę konsekwentnego wskazywania, że walka informacyjna nie może być traktowana jako synonim wojny informacyjnej. Z przedstawionych powyżej analiz wynika również, że zakres podmiotowy i przedmiotowy współczesnych walk informacyjnych staje się coraz bardziej szeroki i wielowątkowy, tak że podział na militarne i pozamilitarne walki informacyjne wydaje się tracić na znaczeniu. Przy obecnych możliwościach tkwiących w społeczeństwie informacyjnym i stopniu rozwoju technicznego walki informacyjne mogą być prowadzone w dowolnym czasie i z dowolnego miejsca, a ich celem (obiektem) w wybranych obszarach działania mogą być jednostki, grupy społeczne, państwa czy grupy państw. Kierując się ogólnym kryterium celów i zasięgu takich walk oraz skalą zastosowanych środków, można wyróżnić zatem walki informacyjne o charakterze:

– taktycznym (mające związek z jakąś konkretną kwestią, prowadzone w ograniczonym podmiotowo i przestrzennie zakresie przy użyciu stosunkowo niewielkich zasobów);
– operacyjnym (mające szerszy – wieloelementowy zakres przedmiotowy i podmiotowy, prowadzone w szerokim wymiarze czasowo-przestrzennym z wykorzystaniem znacznej ilości zasobów);
– strategicznym (mogące mieć nieograniczony zasięg przestrzenny, prowadzone z wykorzystaniem globalnej sieci informacyjnej oraz angażujące w sposób długotrwały bardzo duże siły i środki).

Ponieważ we wszystkich obszarach działania państw, a także innych zorganizowanych podmiotów pozapaństwowych i jednostek, wykorzystywana jest informacja oraz systemy informacyjnego komunikowania się, tematyka walk informacyjnych oraz generowanych przez nie skutków i możliwości ich ograniczania powinna stać się przedmiotem intensywnych dyskusji oraz badań, tak na poziomie służb i instytucji odpowiedzialnych za ochronę żywotnych interesów państwa w sferze bezpieczeństwa informacyjnego, jak również instytucji akademickich.

[366] Zob. M. Wrzosek, *Zmagania o informacje…*, s. 47–48.

3.5. Wojna informacyjna

Podejmując problem ukazania istoty i sposobów postrzegania wojny informacyjnej i dążąc do tego, aby pojęcie to traktować adekwatnie do jego rzeczywistego znaczenia, nie można pominąć odniesień do tradycji definiowania wojny jako takiej. Słownik Merriam-Webster opisuje wojnę jako „stan zwykle otwartego i ogłoszonego wrogiego konfliktu zbrojnego między państwami lub narodami"[367]. *Stanford Encyclopedia of Philosophy* stwierdza, że„wojnę należy rozumieć jako rzeczywisty, zamierzony i powszechny konflikt zbrojny między wspólnotami politycznymi"[368]. Podobny sposób traktowania wojny odnajdziemy w internetowej wersji *Encyclopedia Britannica*, gdzie jest ona definiowana jako „konflikt między podmiotami politycznymi obejmujący działania wojenne o znacznym czasie trwania i skali"[369]. Zgodnie z klasycznym ujęciem Carla von Clausewitza wojna to „akt przemocy, mający na celu nagięcie woli przeciwnika do naszej woli"[370]. Głównym środkiem służącym do realizacji tak ustanowionego celu jest przemoc czy też przymus fizyczny. Julian Kaczmarek podkreśla, że „Z punktu widzenia walczących stron, można ujmować wojnę jako maksymalne nasilenie aktywności wojskowej, napięcia psychologicznego, działalności prawnej, ekonomicznej wytrzymałości i konsolidacji społecznej"[371]. Robert E. Osgood[372], znany badacz stosunków międzynarodowych, określił wojnę jako „zorganizowane starcie sił zbrojnych państw suwerennych, dążących do wzajemnego narzucenia własnej woli"[373]. Według innego znanego amerykańskiego uczonego, Quincy Wrighta, „Wojna jest stanem prawnym

[367] *Merriam-Webster Dictionary,* https://qlf3cqm6hbj4jyqwnggyhohzia-adv7ofecxzh2qqi-merriam-webster-com.translate.goog/dictionary/war?show=0&t=1347910895 [dostęp: 15.05.2021 r.].
[368] *The Stanford Encyclopedia of Philosophy*, https://quxcmx7hq3makbek7gukfbclza-adv7ofecxzh2qqi-plato-stanford-edu.translate.goog/archives/fall2008/entries/war/ [dostęp: 15.05.2021 r.].
[369] *War*, https://www.britannica.com/topic/war [dostęp: 15.05.2021 r.].
[370] C. von Clausewitz, *O naturze wojny*, Warszawa 2010, s. 24.
[371] J. Kaczmarek, C. Staciwa, S. Zapolski, *Doktryna wojenna*, Warszawa 1982, s. 26.
[372] Robert E. Osgood (1921–1986) badacz polityki zagranicznej i wojskowej, autor szeregu znaczących tekstów dotyczących stosunków międzynarodowych, wieloletni wykładowca na Uniwersytecie Johnsa Hopkinsa, doradca Ronalda Reagana podczas kampanii prezydenckiej w 1980 roku.
[373] R.E. Osgood, *Limited War: The Challenge To American Security,* University of Chicago Press, 1957, cyt. za: A. Polak, *Wojna. Definicje, teorie, klasyfikacje,* „Zeszyty Naukowe AON" 2010, nr 4, s. 380.

pozwalającym dwom lub większej liczbie wrogich grup rozwiązywać konflikt przez użycie siły zbrojnej"[374]. Z kolei zdaniem Carla Schmitta wojna „to konflikt prowadzony za pomocą uzbrojenia między jednostkami zorganizowanymi politycznie"[375]. Ryszard Wróblewski uważa zaś, że wojna jest „procesem, formą przejawiania się konfliktu społecznego, którego składową jest konflikt zbrojny"[376]. Jeżeli chodzi o wpisanie wojny informacyjnej do katalogu znanych już rodzajów wojen, to zgodzić się należy z opinią prezentowaną przez P. Daniluka, który uważa, że można tego dokonać na kanwie interpretacji poglądów C. von Clausewitza, iż wojna stanowi narzędzie polityki i jest dalszym ciągiem stosunków politycznych, ale przeprowadzonych przy pomocy innych instrumentów. Na tej podstawie można wywieść, że instrumenty te mogą mieć zarówno charakter militarny, ekonomiczny, technologiczny czy informacyjny. To z kolei umożliwia prowadzenie odpowiednich rodzajów wojen, w tym także wojny informacyjnej.

Za wyodrębnieniem wojny informacyjnej przemawia także rozwój społeczny i technologiczny dostarczający nowych możliwości w sferze konfrontacji pomiędzy państwami, pozwalający odchodzić od klasycznego pojmowania wojny. O postępującej zmianie charakteru wojen zaświadczają również przeobrażenia w strukturach organizacyjnych sił zbrojnych, w których oprócz klasycznej triady (wojska lądowe, lotnictwo, marynarka wojenna) powstały wojska specjalne, cyberwojska czy siły kosmiczne[377].

Jeżeli zbadać kwestię pojawienia się terminu „wojna informacyjna" w obiegu naukowym, to obszernie przedstawia ją Yaryna Onishechko w oparciu o szeroką kwerendę źródłową – wspomniana autorka powołuje się m.in. na ustalenia Siergieja Grinajewa oraz Igora Panarina. Pierwszy z wymienionych badaczy początki używania tego pojęcia datuje na rok 1976, a jako jego twórcę wskazuje Thomasa P. Rona, który we wspomnianym roku przedstawił raport zatytułowany *Weapon Systems and Information War* (*Systemy broni i wojna informacyjna*). Igor Panarin z kolei dowodzi, że termin „wojna informacyjna" zastosowany został pierwszy raz w opublikowanej w 1967 książce Allana Dullesa *The Secret Surrender* (*Tajna kapitulacja*), w której autor użył go dla

[374] Q. Wright, *A Study of War*, Chicago 1942, p. 50.
[375] C. Schmitt, *Teologia polityczna i inne pisma,* Kraków-Warszawa 2000, s. 204.
[376] R. Wróblewski, *O definiowaniu wojny*, [w:] *Oblicza współczesnych wojen,* M. Kubiak, R. Wróblewski (red.), Warszawa-Siedlce 2018, s. 23.
[377] P. Daniluk, *Wojna informacyjna – złożona przeszłość i niepewna przyszłość,* „Rocznik Bezpieczeństwa Międzynarodowego" 2019, nr 2, s. 150.

określenia indywidualnych, wywiadowczych działań dywersyjnych, mających na celu osłabienie zaplecza przeciwnika. Y. Onishechko przywołuje także świadectwo Jamesa Mulverona, wskazującego, że pojęcie „wojna informacyjna" pojawiło się w 1985, kiedy opublikowano książkę Shena Weiguanga *Information Warfare* (*Wojna informacyjna*). Cytowana badaczka zauważa również, że na gruncie normatywnym omawiany termin został zastosowany w pochodzącej z 1992 roku dyrektywie Departamentu Obrony dla oznaczenia operacji informacyjnych, prowadzonych w czasie kryzysu czy konfliktu dla osiągnięcia czy promowania specyficznych celów i stosowanych wobec konkretnego przeciwnika lub przeciwników[378].

Przechodząc do kwestii właściwego pojmowania istoty wojny informacyjnej, należy zgodzić się z B. Balcerowiczem, że będzie to wojna nowej ery oraz że w całej okazałości tego typu wojna nie miała jeszcze miejsca[379]. Jeżeli chodzi o definiowanie tego, czym jest (czym może być) wojna informacyjna, to John Alger uważa, iż „Na wojnę informacyjną składają się działania, których celem jest ochrona, wykorzystanie, uszkodzenie, zniszczenie informacji lub zasobów informacji albo też zaprzeczenie informacjom po to, aby osiągnąć znaczne korzyści, jakiś cel lub zwycięstwo nad przeciwnikiem"[380]. W opinii amerykańskich wojskowych są to „działania podejmowane dla osiągnięcia przewagi informacyjnej poprzez wpływanie na informacje przeciwnika, procesy oparte na przetwarzaniu informacji, systemy informacyjne"[381].

Olga Wasiuta i Sergiusz Wasiuta, opisując wojnę informacyjną, wskazują, że jest to „wpływ na ludność cywilną i/lub wojskową innego kraju poprzez rozpowszechnianie odpowiednio dobranych informacji. Obiektem wojny informacyjnej jest zarówno zbiorowa świadomość, jak i indywidualna. A wpływ informacyjny może odbywać się zarówno w tle szumu informacyjnego i w próżni informacyjnej. Wprowadzenie w życie obcych celów sprawia, że wojna informacyjna staje się wojną i odróżnia ją od zwykłej propagandy. Zasobami wojny informacyjnej są różne narzędzia komunikacji – od mediów do poczty i plotek. Informacje te obejmują przeinaczenia faktów lub narzucanie obywatelom

[378] Zob. Y. Onishechko, *Media w Rosji a wojna informacyjna. Analiza zjawiska na przykładzie programu „Wiesti o 20:00" w czasie konfliktu wojennego na wschodzie Ukrainy,* „Kultury Wschodniosłowiańskie – Oblicza i Dialog" 2016, t. VI, s. 175–176.
[379] Zob. B. Balcerowicz, dz. cyt., s. 201.
[380] W. Schwartau, *Information Warfare,* 2nd Ed., New York 1996, p. 12.
[381] The Chairman of the Joint Chiefs of Staff Instruction, CJCSI S-3210.01, 02 January 1996.

emocjonalnego postrzegania, wygodnego agresorowi”[382]. W bardziej syntetycznym, późniejszym ujęciu Wojciecha Cendrowskiego oraz O. Wasiuty wojna informacyjna to „ogół działań, które można scharakteryzować jako manipulację informacjami, dezinformację i propagandę mające na celu zdobycie lub utrzymanie przewagi w polityce globalnej lub regionalnej”[383]. Cytowana już wcześniej D.E. Denning stosuje dość lapidarne określenie wojny informacyjnej, pisząc, że na taki rodzaj wojny „składają się ofensywne i defensywne działania skierowane przeciw zasobom informacyjnym. Są to działania o charakterze »sukces-porażka«”[384]. Wspomniana autorka dodaje jednocześnie (co jest bardzo ważne dla poprawnego rozumienia pojęcia), iż „W wojnie informacyjnej biorą udział nie tylko komputery i sieci komputerowe. Obejmuje ona informacje we wszelkiej postaci i przesyłane wszystkimi środkami, począwszy od ludzi i ich fizycznego środowiska do druków, telefonów, radia i telewizji, do komputerów i sieci komputerowych. Wojna taka to operacje skierowane przeciw treści informacji i operacje przeciw związanym z nimi systemom, włącznie z oprzyrządowaniem, oprogramowaniem i pracą człowieka”[385]. Bardzo wiele cennych spostrzeżeń do rozważań na temat tego, czym jest woja informacyjna, wnosi Jacek Regina Zacharski. W opinii tego autora treść pojęcia „wojna informacyjna” w dużej mierze uzależniona jest od kultury strategicznej, w obrębie której jest ono formułowane. Autor ten przyjmuje definicję mówiącą, że „wojna informacyjna to jawne lub ukryte, celowo ukierunkowane i świadome oddziaływanie na siebie (ścieranie się/walka) systemów informacyjnych mające na celu uzyskanie określonej korzyści w sferze materialnej”[386]. Jednocześnie, rozszerzając zakres prowadzonej analizy pojęcia, J.R. Zacharski wskazuje na dwa sposoby rozumienia wojny informacyjnej. W pierwszym, szerokim ujęciu, proponuje traktowanie wojny informacyjnej jako wojny algorytmów i technologii, co powoduje, że „jest to konfrontacja, w której systemy i struktury traktowane są jako nośniki wiedzy i informacji niezbędnych z jednej strony dla działania, z drugiej utrzymywania woli działania. Oznacza to, że wojnę informacyjną stanowią działania koercyjne prowadzone przeciw podstawom wiedzy

[382] Zob. O. Wasiuta, S. Wasiuta, *Wojna informacyjna zagrożeniem dla bezpieczeństwa ludzkości*, [w:] *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania*, H. Batorowska (red.), Kraków 2017, s. 71.
[383] O. Wasiuta, R. Klepka, dz. cyt., t. 2, s. 539.
[384] D.E. Denning, dz. cyt., s. 23.
[385] Tamże, s. 14.
[386] J.R. Zacharski, *Wojna informacyjna*, [w:] *Zagrożenia i wyzwania bezpieczeństwa współczesnego świata*, I. Oleksiewicz, K. Stępień (red.), Warszawa 2016, s. 194.

przeciwnika i mechanizmom jej używania”[387]. Drugie ujęcie, nazywane przez cytowanego autora „najszerszym”, opisuje wojnę informacyjną jako „aktywność realizowaną na trzech poziomach: 1. percepcji; 2. struktury informacyjnej; 3. fizycznego rażenia infrastruktury przeciwnika”[388].

W Federacji Rosyjskiej główne kierunki badań w zakresie wojny informacyjnej wytyczają, jak zauważa Michał Wojnowski, badacze wywodzący się w większości z środowisk wojskowych oraz związanych ze służbami specjalnymi. Wspomniany autor wskazuje, że pojęcie wojny informacyjnej jest w Rosji traktowane niejednoznacznie i wyróżnia w tym kontekście trzy nurty definicyjne:

- nurt traktujący wojnę informacyjną jako pojedyncze działania lub operacje o charakterze informacyjnym oraz sposoby i środki charakterystyczne dla konkurencji między firmami, korporacjami itp.;
- nurt postulujący zastępowanie pojęcia „wojna informacyjna” określeniami „konfrontacja informacyjna” lub „walka informacyjna” i przypisanie do tych terminów działań militarnych przybierających formę tzw. operacji informacyjno-uderzeniowych, których celem będzie m.in.:
  – zniszczenie infrastruktury informacyjnej wrogiego państwa;
  – zdezorganizowanie systemu dowodzenia jego armii oraz struktur administracji państwowej;
  – zdezorientowanie przywódców politycznych;
- nurt traktujący wojnę informacyjną jako konfrontację pomiędzy państwami, koalicjami państw lub blokami polityczno-militarnymi, której celem jest destrukcja politycznej, ekonomicznej i społecznej struktury danego państwa oraz masowe psychologiczne oddziaływanie na społeczeństwo prowadzące do destabilizacji państwa.

Poznawczo interesujący jest także przywołany przez M. Wojnowskiego pogląd Władimira Cymbała, wskazującego na istnienie dwóch możliwych ujęć terminu „wojna informacyjna”, szerszego i węższego. W tej pierwszej perspektywie, zdaniem W. Cymbała, jest to zespół działań podejmowanych przez jedno z państw przeciwko ludności cywilnej innego państwa lub grupy państw w okresie pokoju w celu uzyskania wpływu na świadomość społeczną przez naukę, sztukę, kulturę, system edukacji i inne. Z kolei w ujęciu węższym wojna informacyjna jest formą militarnych działań mających na

[387] Tamże.
[388] Tamże, s. 195.

celu osiągnięcie przewagi informacyjnej nad przeciwnikiem w dziedzinie rozpowszechniania, wykorzystania i przetwarzania informacji oraz wdrażania decyzji umożliwiających osiągnięcie przewagi na polu walki[389]. Z kolei według poglądu Andrieja Manojły wojna informacyjna jest skrajną metodą konfrontacji informacyjnej pomiędzy państwami realizowaną za pomocą różnych sposobów informacyjnego wpływu, z przewagą tajnych operacji informacyjno-psychologicznych. Operacje takie stanowią kompleks przedsięwzięć obejmujących m.in. cyberataki, prowadzone w celu zniszczenia lub modyfikacji zasobów i systemów informacyjnych przeciwnika oraz wywierania destrukcyjnego wpływu na psychikę społeczeństwa oraz elit przywódczych[390]. Bohdan Pac, analizując i ujmując w syntetyczną formę rosyjskie poglądy na wojnę informacyjną, wskazuje, że ten rodzaj wojny jest traktowany przez Rosjan „jako oddziaływanie na masową świadomość w międzypaństwowej rywalizacji systemów cywilizacyjnych w przestrzeni informacyjnej, wykorzystujące szczególne sposoby kontroli nad zasobami informacyjnymi, które mogą być stosowane jako swoista broń informacyjna. Działania te skierowane są nie tylko przeciw siłom zbrojnym, ale przede wszystkim ukierunkowane są na całe społeczeństwo oraz jego świadomość, a także na aparat administracyjny, świat nauki i kultury oraz przemysł i ekonomikę danego państwa"[391].

Niezależnie od różnic w stosunku do definiowania pojęcia „wojna informacyjna", rosyjscy teoretycy są na ogół zgodni co do tego, że istota wojny informacyjnej zawiera się w prowadzeniu trzech rodzajów operacji:

- informacyjnych;
- psychologicznych;
- informacyjno-psychologicznych[392].

Do zbliżonych wniosków dochodzi Jolanta Darczewska, która uważa, że „w zdecydowanej większości rosyjscy autorzy pod pojęciem »wojna informacyjna« rozumieją oddziaływanie na masową świadomość w międzypaństwowej rywalizacji systemów cywilizacyjnych w przestrzeni informacyjnej, wykorzystujące szczególne sposoby kontroli nad zasobami informacyjnymi,

[389] Zob. M. Wojnowski, *Terroryzm w służbie geopolityki*…, s. 79.
[390] Zob. tenże, *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 27.
[391] B. Pac, *Wojna informacyjna jako skuteczne narzędzie destabilizacji państw i rządów*. Raport z 2 lutego 2016 r., https://www.defence24.pl/wojna-informacyjna-jako-skuteczne-narzedzie-destabilizacji-panstw-i-rzadow-raport [dostęp:12.04.2021 r.].
[392] Zob. M. Wojnowski, *„Zarządzanie refleksyjne" jako paradygmat*…, s. 14–15.

a używane w charakterze »broni informacyjnej«"[393]. Wspomniana autorka dodaje także istotną w kontekście prowadzonych rozważań uwagę, że rosyjską „teorię zbudowano w opozycji do teorii cyberbezpieczeństwa, rozwijanej w Stanach Zjednoczonych i w Europie Zachodniej, a związanej przede wszystkim z militarnym i wywiadowczym zastosowaniem nowych technologii informatycznych"[394].

W podobnym tonie wypowiada się J.R. Zacharski, który wskazuje na dwa wzorce wojny informacyjnej:

- pierwszy, związany z zachodnią kulturą strategiczną oraz przemyśleniami części strategów chińskich, oparty na wydzieleniu:
  – domeny działań z zakresu technologii mieszczących się w obrębie oddziaływania (rażenia) fizycznego;
  – domeny stosowania elektromagnetycznych środków walki.
- drugi, obecny w rosyjskiej myśli strategicznej, traktujący wojnę informacyjną jako działania na poziomie percepcji oraz struktury informacyjnej[395].

Warto także na potrzeby prowadzonych rozważań ukazać perspektywę, w jakiej postrzega się wojnę informacyjną w Stanach Zjednoczonych. Według formułowanych tam poglądów wojna ta „polega na defensywnym i ofensywnym wykorzystaniu informacji i systemów informacyjnych w celu odcięcia przeciwnika od dopływu informacji, jak też wykorzystania, zniekształcania lub niszczenia informacji, które posiada, przy jednoczesnym zachowaniu własnych zasobów i systemów informacyjnych w nietkniętym stanie"[396]. Generalnym celem przy takim spojrzeniu na wojnę informacyjną jest prowadzenie oddziaływania na sferę wolicjonalną i decyzyjną przeciwnika tak, aby postępował on zgodnie z zamierzeniami podmiotu, który na niego informacyjnie oddziałuje.

Za ważne i sprzyjające czytelnemu przedstawieniu istoty wojny informacyjnej należy uznać opinie wyrażone przez Adama Lelonka, który zwraca uwagę, że wojnę informacyjną można sprowadzić do trzech płaszczyzn celów[397] i związanych z nimi działań[398]. Według tego autora wojna informacyjna

[393] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, Warszawa 2014, s. 12.
[394] Tamże, s. 11.
[395] Zob. J.R. Zacharski, dz. cyt., s. 195–198.
[396] B. Pac, dz. cyt.
[397] Zob. tabela 11.
[398] Zob. A. Lelonek, dz. cyt., s. 71.

to odmiana „miękkiej wojny". Wynika to z wykorzystywania manipulacji informacyjnej oraz kierowania do przeciwnika zmodyfikowanego lub fałszywego przekazu zakłócającego obraz rzeczywistości, kształtującego postawy i wpływającego na morale społeczeństwa, a także modyfikującego percepcję liderów politycznych i ich postulatów. Wojna informacyjna może, jak zauważa A. Lelonek, przybrać także charakter wojny wewnętrznej[399].

Tabela 11. Wojna informacyjna

Cel	Działania
Zasoby fizyczne	Uszkodzenie lub zniszczenie systemów informacyjnych i komunikacji przeciwnika przy wykorzystaniu konwencjonalnych technik wojskowych.
Zasoby „miękkie"	Infiltracja, degradacja, niszczenie systemów informacyjnych; wykorzystanie zewnętrznych aktorów i skorumpowanych struktur wewnętrznych do łamania zabezpieczeń i osłabiania możliwości systemów informacyjnych przeciwnika, w tym także przy pomocy złośliwego oprogramowania.
Zasoby psychiczne	Cicha penetracja systemów informacyjnych i komunikacyjnych przeciwnika, mająca na celu zarządzanie percepcją, kształtowaniem opinii, podsycaniem dezinformacji i angażowaniem w walkę epistemologiczną.

Źródło: A. Lelonek, *Wojna informacyjna, operacje informacyjne i psychologiczne: pojęcia, metody i zastosowanie,* [w:] *Potencjał słowa. Międzynarodowe stosunki i komunikacja: stan i perspektywy*, A. Lelonek (red.), Warszawa-Lwów 2016, s. 71–72.

Cytowany autor podkreśla, że rozwój narzędzi i potencjalnych obszarów wojny informacyjnej jest szczególnie widoczny u społeczeństw posiadających dostęp do wysoko rozwiniętych technologii. Celem wojen informacyjnych mogą być w opinii A. Lelonka zwłaszcza przeciwnicy, którzy dysponują podobnym potencjałem technologicznym. Co warto podkreślić, przywoływany badacz zauważa rzecz ważną, a mianowicie to, że wojna informacyjna może być prowadzona także przez występujące przeciwko danemu państwu organizacje niejawne czy terrorystyczne[400].

[399] Zob. tamże, s. 71–73.
[400] Tamże, s. 72–73.

Jak wskazuje P. Daniluk, wojnę informacyjną można analizować w ujęciu systemowym, wyodrębniając:

- wojnę sieciową (obejmującą sieci społecznościowe, wykorzystującą Internet do blokowania dostępu do informacji lub usług realizowanych za jego pomocą);
- cyberwojnę (prowadzoną głównie przez komponenty wojskowe przeciwko siłom zbrojnym przeciwnika);
- wojnę medialną (która objawia się współcześnie wykorzystaniem dwóch zasadniczych środków przekazu. Najważniejszym, ze względu na zasięg, jest telewizja i radiofonia. Drugim rodzajem środków przekazu są tradycyjne media, czyli prasa, plakaty, ulotki, bilbordy oraz filmy);
- komunikację bezpośrednią (opartą o działania służb specjalnych)[401].

Z kolei według Martina Libickiego[402] można mówić o siedmiu formach wojny informacyjnej:

- wojnie w zakresie dowodzenia i kierowania;
- wojnie opartej na wywiadzie;
- wojnie elektronicznej;
- wojnie psychologicznej;
- wojnie hakerów;
- wojnie na informacje gospodarcze;
- cyberwojnie[403].

W odniesieniu do środków wojny informacyjnej Jacek Regina Zacharski pisze o stosowaniu:

- ataków kinetycznych;
- zakłóceń elektronicznych;
- ataków sieciowych;
- dezinformacji pola walki;
- operacji psychologicznych;
- operacji zabezpieczających[404].

[401] Zob. P. Daniluk, *Wojna informacyjna*…, s. 163.
[402] Martin C. Libicki (1952-), absolwent Massachusetts Institute of Technology, wykładał w Narodowym Uniwersytecie Obrony, służył w Sztabie Marynarki Wojennej USA, był ekspertem Rand Corporation, obecnie w ramach Akademii Marynarki Wojennej USA zajmuje się badaniami nad cyberwojną oraz wpływem technologii informacyjnych na bezpieczeństwo.
[403] Zob. M.C. Libicki, *What Is Information Warfare*, Islamabad 1995, p. 18.
[404] Zob. J.R. Zacharski, dz. cyt., s. 196.

Cytowany już wcześniej A. Lelonek przedstawia następujący zestaw instrumentów wojny informacyjnej:

- wirusy i robaki komputerowe;
- konie trojańskie i bomby logiczne;
- luki w programach służące do uzyskania nieautoryzowanego dostępu;
- chipping (czyli dodawanie chipów lub świadome powodowanie wad konstrukcyjnych);
- nanoroboty i maszyny molekularne;
- zagłuszanie elektroniczne oraz impuls elektromagnetyczny;
- broń energetyczną oraz broń elektromagnetyczną[405].

Uwzględniając treści przywołanych powyżej definicji oraz charakterystyk wojny informacyjnej, można zaproponować takie ujęcie, zgodnie z którym jest to „zaplanowana forma przemocy zastosowana przez państwo (koalicję państw), w ramach której podjęta zostaje próba rozstrzygnięcia istniejących sporów, zaspokojenia postulowanych żądań czy narzucenia zachowań na drodze prowadzonych na szeroką skalę obezwładniających działań informacyjnych w różnych sferach: politycznej, gospodarczej, wojskowej, społecznej, ekologicznej realizowanych przy użyciu różnych narzędzi (propaganda, ataki cybernetyczne, zakłócenia radioelektroniczne, agenci wpływu, manipulacja opinią publiczną itp.)”[406]. W wojnie informacyjnej, gdy dojdzie do niej w „czystej” formie, nie będzie klasycznych walk zbrojnych, ponieważ opanowanie przestrzeni informacyjnej przeciwnika pozwoli stronie atakującej na sparaliżowanie jego możliwości w zakresie stawiania oporu i reakcji oraz osiągnięcie celów bez użycia siły militarnej.

Podsumowując, należy jeszcze raz podkreślić praktyczne i teoretyczne znaczenie rozróżniania pojęć „walka informacyjna” i „wojna informacyjna”. Wiąże się to nie tylko z prowadzeniem owocnego (a nie jałowego) dyskursu naukowego w zakresie istoty bezpieczeństwa informacyjnego, lecz także z generowaniem koniecznych rozstrzygnięć np. w dziedzinie teorii i praktyki sztuki wojennej czy prawa konfliktów zbrojnych. Jednocześnie dostrzec należy trudności w badaniu i precyzowaniu istoty wojny informacyjnej wynikające z kilka niełatwych do usunięcia przyczyn. Pierwsza z nich wiąże się z tym, że wojna informacyjna to określenie o charakterze interdyscyplinarnym, używane w różnych dziedzinach nauki. Jej postrzeganie i definiowanie może

[405] Zob. A. Lelonek, dz. cyt., s. 72.
[406] W. Fehler, *O pojęciu bezpieczeństwa informacyjnego…*, s. 41.

ulegać zmianie w zależności od tego, w ramach jakiej dyscypliny jest ona badana. Druga istotna przyczyna wspomnianych trudności wiąże się z tym, że w pracach badawczych nad problematyką wojen informacyjnych, które rozpoczęły się w latach 80. XX wieku, widać nadmierną koncentrację na czynnikach technologicznych, przy pomijaniu lub ograniczaniu roli innych czynników związanych z rewolucją w przestrzeni informacyjnej, która spowodowała, że to sieć może być głównym obszarem prowadzenia wojen informacyjnych.

Na utrudnienia w procesie definiowania terminu „wojna informacyjna" wpływa również kwestia tłumaczenia. Problem polega na tym, że w języku angielskim, w którym po raz pierwszy zaczęto używać pojęcia *information warfare*, znaczenie pierwszego słowa – *information* – nie budzi wątpliwości, natomiast *warfare* może być (i bywa) tłumaczone zarówno jako „wojna", jak i „walka". To wszystko sprzyja chaosowi definicyjnemu, który dodatkowo pogłębia interpretacyjny nieład, w ramach którego część specjalistów sięga po publicystyczne wzorce i formuły, myląc i spłaszczając podstawowe pojęcia.

3.6. Bariery informacyjne

Bariery informacyjne to kategoria pojęciowa, która może budzić wątpliwości w zakresie traktowania jej jako samodzielnej, a nie przyporządkowanej do grupy zagrożeń bezpieczeństwa informacyjnego. Rodzi to konieczność podkreślenia różnic dotyczących tych dwóch pojęć, które w codziennym zwłaszcza, potocznym i pobieżnym odbiorze mogą wydawać się niezbyt wyraźne i jednoznaczne, ale są namacalne i pozwalają na traktowanie wspomnianych barier jako odrębnej kategorii pojęciowej. Przede wszystkim należy zwrócić uwagę, że zagrożenia informacyjne w większości wypływają ze źródeł antropogenicznych i technologicznych. Dostrzec należy także pewną grupę zagrożeń godzących w bezpieczeństwo informacyjne, związaną z destrukcyjnym oddziaływaniem sił natury, takich jak np. powodzie czy pożary, mogące niszczyć czy uszkadzać zasoby informacyjne. Zagrożenia dla bezpieczeństwa informacyjnego to kategoria zmienna i rozwojowa zarówno ze względu na ludzką aktywność, jak i dużą innowacyjność, np. w zakresie przestępczości informacyjnej czy działalności dezinformacyjnej. Zagrożenia te są w związku z tym trudne do ograniczenia, nie wspominając o ich eliminacji. Jeżeli chodzi o bariery informacyjne, to w dużej mierze łączą się one z zachowaniami informacyjnymi. Zachowania te, za Moniką Krakowską, można określić jako „ogół ludzkich

aktywności pozostających w relacji do źródeł i kanałów informacji, a także jako różnorodne, aktywne lub bierne, intencjonalne lub nieintencjonalne działania odnoszące się do reagowania na informacje; jej poszukiwanie, wykorzystywanie, przekazywanie, ale też unikanie lub odrzucanie”[407]. Jak wskazuje Natalya Godbold, działania aktywne to np. monitorowanie, łączenie, wyodrębnianie, weryfikowanie. Te pasywne to z kolei ignorowanie informacji czy odbiór informacji bez zainteresowania. Aktywności o zabarwieniu pozytywnym obejmują czynne pozyskiwanie, zbieranie, gromadzenie informacji, a te o charakterze negatywnym wiążą się np. z kwestionowaniem, niszczeniem czy celowym zniekształcaniem informacji[408]. W kontekście powyższych uwag za ważny należy uznać pogląd jednego z autorytetów naukowych w dziedzinie badania barier informacyjnych, Thomasa D. Wilsona, który wskazuje na istnienie trzech kategorii zmiennych wpływających na ludzkie zachowania informacyjne:

– związanych z charakterystycznymi cechami danej osoby (światopogląd, preferencje, wykształcenie, doświadczenie zawodowe, samoocena, wiek, płeć, pochodzenie społeczne);
– związanych z pozycją i rolą zawodową (wymagania dotyczące uprawianej profesji, ograniczenia i przywileje, normy grupowe);
– związanych z otoczeniem (zmienne finansowe, prawne, czasowe, geograficzne, kulturowe)[409].

Bariery informacyjne wiążą się z powstawaniem potrzeb informacyjnych i pozostają w ścisłym związku z różnymi ograniczeniami wpływającymi na poziom i jakość ich zaspokojenia. Wspomniane bariery w większości mają charakter przeszkód, które dzięki systematycznemu rozwojowi nauki, postępowi technicznemu, odpowiednim nakładom finansowym, edukacji oraz indywidualnej aktywności ludzi można niwelować lub eliminować. Tak stało się z barierą przestrzenną. Dzięki upowszechnieniu nauki języka angielskiego oraz rozwojowi translatorów elektronicznych postępuje także ograniczanie barier językowych. Szereg barier ma jednak charakter osobniczy, związany np. z motywacją do zdobywania wiedzy, poziomem możliwości percepcyjnych czy chęcią uzyskiwania nowych umiejętności. Także te bariery daje się

[407] M. Krakowska, *Zachowania informacyjne człowieka*, [w:] *Nauka o informacji*, W. Babik (red.), Warszawa 2016, s. 430.
[408] Zob. N. Godbold, *Beyond information seeking: towards a general model of information behaviour*, „Information Research” 2006, no. 4, p. 7–8, https://files.eric.ed.gov/fulltext/EJ1104640.pdf [dostęp: 21.05.2021 r.].
[409] Zob. T. Wilson, *Information behaviour an interdisciplinary perspective*, „Information Processing &Management” 1997, vol. 33, no. 4, p. 556.

przezwyciężać m.in. w drodze edukacji, szkoleń, treningów czy innych form rozwijających intelekt oraz umiejętności praktyczne. Jednak trzeba zaznaczyć, że tu o sukcesach decyduje zaangażowanie i konsekwencja osób zainteresowanych takimi działaniami. Zważywszy na ścisły związek barier informacyjnych z potrzebami i zachowaniami informacyjnymi ludzi, trzeba mieć świadomość ciągłego ich istnienia i wpływu na kształtowanie przestrzeni informacyjnej. Dostrzec należy również zjawisko pojawiania się nowych barier związanych z rozwojem technologii informacyjno-komunikacyjnych czy lawinowym przyrostem informacji. Ogólna definicja bariery umieszczona w jednym ze słowników języka polskiego wskazuje, że jest to „rzecz, która utrudnia powstanie jakiegoś zjawiska lub sytuacji”[410]. Według *Słownika terminologicznego informacji naukowej* bariera informacyjna to „przeszkoda utrudniająca lub uniemożliwiająca korzystanie z informacji bądź rozpowszechnianie informacji”[411]. Z kolei w niemieckim leksykonie informacji i dokumentacji bariera informacyjna jest opisywana jako „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; 2) ponieważ użytkownik ma utrudniony dostęp do tych źródeł, z różnych przyczyn”[412]. W encyklopedycznym ujęciu autorstwa K. Batorowskiej „Bariery informacyjne mogą dotyczyć dostępu do informacji, ale też przepływu wiedzy lub przeszkód występujących w procesie komunikacji. Bariery informacyjne jako przeszkody, które zakłócają proces przepływu informacji od jej twórców do adresatów, mogą oddziaływać na użytkownika niezależnie od jego świadomości (bariery obiektywne) lub poprzez tę świadomość (bariery subiektywne)”[413]. Według definicji Marzeny Świgoń bariery informacyjne „są to przeszkody, które utrudniają, opóźniają lub uniemożliwiają dostęp do informacji, czyli pozyskiwanie i korzystanie z informacji”[414]. Wspomniana

[410] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/slowniki/bariera.html [dostęp: 20.05.2021 r.].
[411] *Słownik terminologiczny informacji naukowej*, M. Dembowska i in. (red.), Wrocław-Warszawa 1979, s. 28.
[412] *Lexikon Information und Dokumentation*, S. Rückl, G. Schmol (red.), Leipzig 1984, s. 187.
[413] *Encyklopedia bezpieczeństwa*, O. Wasiuta, S. Wasiuta (red.), t. I, Kraków 2021, s. 210.
[414] M. Świgoń, *Bariery informacyjne: podstawy teoretyczne i próba badań w środowisku naukowym*, Warszawa 2006, s. 23.

badaczka zaznacza, że termin ten zaczął być używany w latach 70. XX wieku w piśmiennictwie rosyjskim, a nieco później również w niemieckim[415]. Uwzględniając treści przedstawionych definicji, do dalszego zastosowania autor przyjmuje stanowisko traktujące barierę informacyjną jako „względnie trwały rodzaj przeszkody, która utrudnia, ogranicza lub uniemożliwia pozyskiwanie, przekazywanie, dostarczanie i wykorzystywanie informacji"[416].

Złożoność oraz różnorodność barier informacyjnych powoduje, że w ramach prowadzonych badań tworzone są różne ich podziały. Zagadnieniami klasyfikacji barier informacyjnych jako jedni z pierwszych zaczęli zajmować się Dietrich E. Haag i Thomas D. Wilson. Pierwszy z wymienionych badaczy, który uważany jest za również za prekursora prac nad barierami informacyjnymi, w latach osiemdziesiątych XX wieku skonstruował szczegółową klasyfikację, w której zawarł listę 41 takich barier. Natomiast T.D. Wilson wprowadził do naukowego obiegu do dziś bardzo popularną i nośną poznawczo typologię zawierającą cztery ich grupy:

– bariery związane z osobą użytkownika;
– bariery interpersonalne;
– bariery środowiskowe;
– bariery związane ze źródłami informacji[417].

Także polscy badacze i znawcy problematyki barier informacyjnych stworzyli szereg ich klasyfikacji. Niektóre z nich mają charakter ogólny i syntetyczny, inne zaś są rozbudowane i szczegółowe. Do pierwszej grupy niewątpliwie zaliczyć można zestawienia sporządzone przez Elżbietę B. Zybert, Wiesława Babika, Jolantę Sobielgę, Tomasza Galewskiego oraz Marię Próchnicką. Pierwsza z wymienionych osób przyjęła, że istnieją trzy rodzaje barier informacyjnych:

– 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)[418].

[415] Zob. tamże, s. 457.
[416] W. Fehler, *Bariery informacyjne jako czynnik kształtujący współczesne bezpieczeństwo informacyjne*, [w:] *Prawne aspekty informacji chronionych*, M. Kubiak (red.), Siedlce 2020, s. 19.
[417] Zob. O. Wasiuta, R. Klepka, dz. cyt., t. 1, s. 61.
[418] Zob. E.B. Zybert, *Bariery w dostępie do książki i biblioteki w środowisku niedostosowanych społecznie*, „Poradnik Bibliotekarza" 1992, nr 7/8, s. 11.

Z kolei W. Babik jako zasadniczą barierę informacyjną wskazuje niewystarczającą ilość czasu na wyszukiwanie informacji. Oprócz tego wymienia także:

- bariery natury psychologicznej (m.in. opór psychiczny przed proszeniem o pomoc w sferze informacyjnej czy lęk przed korzystaniem z komputera);
- bariery kulturowe, społeczne i edukacyjne związane ze środowiskiem, w którym żyje i funkcjonuje użytkownik informacji;
- bariery związane z zawodnością i ograniczoną wydajnością kanałów przepływu informacji[419].

Według J. Sobielgi bariery informacyjne podzielić można na cztery kategorie:

- 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;
- procesy i stany psychiczne użytkownika informacji blokujące efektywne jej wykorzystanie[420].

W klasyfikacji zaprezentowanej przez Tomasza Galewskigo, badającego problem barier informacyjnych z perspektywy personalnych aspektów funkcjonowania przedsiębiorstwa, wymienione zostały:

- bariery informacyjne *sensu stricto*, rodzące się na gruncie niedostatku informacji, operowaniu informacją złej jakości oraz informacją mało użyteczną;
- bariery psychologiczne związane z ludzkimi ograniczeniami w procesie generowania informacji oraz jej interpretacji;
- bariery socjologiczne powstające na tle grupowych norm społecznych wpływających na indywidualne sposoby percepcji informacji;
- bariery organizacyjne powstające w związku ze złą organizacją procesów informacyjnych i niewłaściwym stanem zasobów technicznych służących do korzystania z informacji;

[419] W. Babik, *Ekologia informacji…*, s. 57–58.
[420] Zob. J. Sobielga, *Psychologiczne aspekty barier informacyjnych – badania wśród studentów,* „Praktyka i Teoria Informacji Naukowej i Technicznej" 1997, nr 4, s. 14.

– bariery ekonomiczne związane z deficytem środków finansowych ograniczających optymalizację systemów informacyjnych[421].

Najbardziej syntetyczny podział zaproponowała M. Próchnicka, która wyodrębniła bariery o charakterze:

– zewnętrznym, względnie niezależne od użytkownika informacji (np. czasowe i ekonomiczne);
– wewnętrznym, powstające na tle niedostatecznego przygotowania użytkowników do odbioru informacji oraz braku umiejętności selekcji źródeł informacji[422].

Do rozbudowanych klasyfikacji zaliczyć należy tę sporządzoną przez Wacława Przelaskowskiego, który do czynników ograniczających dostęp do informacji zaliczył:

– barierę odległości związaną z warunkami geograficznymi i transportowymi;
– bariery związane z funkcjonowaniem państw (stopień swobody przepływu i wymiany informacji ponad granicami państw, ograniczenia ze strony struktur administracyjnych);
– bariery związane z warunkami konkurencji (powstające na tym tle ograniczenia, np. dotyczące ochrony wynalazków);
– bariery ekonomiczne wynikające z niedoboru lub braku środków finansowych na zakup informacji;
– bariery językowe (wynikające z różnorodności języków, stosowanych terminów czy systemów oznaczeń);
– bariery profesjonalno-terminologiczne (powstające między różnymi dyscyplinami nauki);
– barierę wykształcenia (związaną z deficytem wiedzy niezbędnej do zrozumienia informacji)[423].

Obszerną klasyfikację barier informacyjnych przedstawiły także Magdalena Rzemieniak i Katarzyna Kamińska, które w ramach badań problematyki komunikacji społecznej wskazują na bariery związane z:

– różnicami w indywidualnej percepcji informacji;
– brakiem precyzji w przekazywaniu informacji i komunikatów;

[421] Zob. T. Galewski, *Bariery informacyjne w przedsiębiorstwie*, „Zarządzanie i Finanse" 2012, nr 1, s. 465–468.
[422] Zob. M. Próchnicka, *Informacja a umysł*, Kraków 1991, s. 169.
[423] Zob. W. Przelaskowski, *Problemy informacji naukowej*, Warszawa 1979, s. 43.

– wybiórczym odbieraniem przekazów informacyjnych (brak zainteresowania, niesłuchanie);
– różnorodnością kulturową;
– różnicami językowymi;
– ilością i szybkością transferu informacji;
– brakiem zaufania do źródeł informacji;
– oddziaływaniem stanów emocjonalnych i zdrowotnych;
– złą organizacją system obiegu i dystrybucji informacji;
– stosowaniem nieodpowiednich nadawców oraz niewłaściwych narzędzi i kanałów przekazu informacji[424].

Jedną z najbardziej rozbudowanych, ale posiadającą walor przejrzystości klasyfikację opartą na ustaleniach T.D. Wilsona zaproponowała M. Świgoń. Według tej autorki istnieją cztery zasadnicze kategorie barier informacyjnych, w ramach których mieszczą się ich bardziej szczegółowe subkategorie. W obrębie pierwszej kategorii, związanej z czynnikami indywidualnymi (intelektualnymi, edukacyjnymi i psychologicznymi) charakteryzującymi użytkownika informacji, przywoływana badaczka wymienia bariery:

– nieświadomości, powstające na gruncie nieuświadamiania sobie przez dany podmiot potrzeb informacyjnych;
– terminologiczne, związane z trudnościami w odbiorze informacji o specjalistycznym charakterze;
– języków obcych (brak lub słaba znajomość tych języków);
– niewystarczającego przygotowania do poszukiwania i pozyskiwania informacji;
– braku motywacji do poszukiwania informacji;
– niechęci do korzystania z nowoczesnych technologii informacyjnych oraz usług podmiotów oferujących dostęp do informacji.

Druga zasadnicza kategoria ma charakter interpersonalny[425]. Podstawowe bariery w tej grupie to:

– opór psychiczny osób poszukujących informacji przed zadawaniem pytań specjalistom, współpracownikom lub personelowi obsługującemu zasoby informacyjne;

[424] Zob. M. Rzemieniak, K. Kamińska, *Wewnętrzne public relations w sytuacjach kryzysowych*, Lublin 2012, s. 18–20.
[425] M. Świgoń zwraca uwagę, że mogą to być bariery występujące zarówno po stronie osób poszukujących informacji, jak i osób udzielających informacji.

– brak pomocy ze strony osób stanowiących źródło informacji.

Trzecia zasadnicza kategoria wymieniona przez M. Świgoń wiąże się z bliższym lub dalszym otoczeniem użytkowników informacji. W jej obrębie występują bariery:

– prawne (ochrona: własności intelektualnej i przemysłowej, tajemnic, danych osobowych, archiwaliów);
- finansowe (niedostatek środków finansowych koniecznych do zdobycia dostępu do informacji);
– geograficzne (konieczność korzystania na miejscu z zasobów informacyjnych, których nie poddano digitalizacji lub nie wprowadzono w innej formie do obiegu publicznego);
– polityczne (przeszkody wynikające z aktualnej sytuacji politycznej w sferze międzynarodowej czy wewnątrzpaństwowej);
– kulturowe (związane z różnicami kulturowymi);
– organizacyjne (powstające na bazie kultury danej organizacji, atmosfery i relacji pomiędzy pracownikami, a także przepływu wiedzy).

Ostatnia zasadnicza kategoria to bariery związane ze źródłami informacji. Obejmuje ona bariery:

– nadmiaru informacji i niedoboru wiedzy w nich zawartej;
– słabej jakości informacji i wiedzy;
– dominacji języka angielskiego w międzynarodowych systemach komunikacji;
– opóźnień w upublicznianiu informacji;
– ograniczeń w dostępie do informacji;
– informacji nierelewantnej;
– niedoskonałości narzędzi wyszukiwawczych;
– związane z ułomnością działania instytucji gromadzących i udostępniających zasoby informacyjne[426].

Z perspektywy przedstawionych przykładów klasyfikacyjnych oraz aktualnego stanu wiedzy można stwierdzić, że najczęściej w ramach tematycznych publikacji bariery informacyjne dzielone są na:

– obiektywne i subiektywne;
– zewnętrzne i wewnętrzne;
– makrobariery (uwzględniające warunki ekonomiczne i geopolityczne);

[426] Zob. M. Świgoń, *Bariery informacyjne,* [w:] *Nauka o informacji*, W. Babik (red.), Warszawa 2016, s. 460–462.

– mikrobariery (uwzględniające cechy psychologiczne użytkownika)[427].

Opierając się na przestawionych przykładach podziału barier informacyjnych, w autorskim ujęciu[428] można wymienić następujące ich kategorie:

– bariery związane z postawami użytkowników informacji;
– bariery o charakterze geograficznym;
– bariery techniczno-technologiczne;
– bariery ekonomiczne;
– bariery społeczno-edukacyjne;
– bariery czasowe;
– bariery mentalne;
– bariery percepcyjne;
– bariery zdrowotne i emocjonalne;
– bariery językowo-terminologiczne;
– bariery prawno-administracyjne;
– bariery organizacyjne.

Syntetycznie charakteryzując poszczególne rodzaje barier, należy zwrócić uwagę, że:

– bariery dotyczące postaw użytkowników informacji dotyczą: odmiennych sposobów odbioru i oceniania tej samej informacji, nonszalancji i lekceważenia w jej przyjmowaniu, nieprecyzyjnego przekazywania, wybiórczego odbioru treści, przypisywania zbyt dużego znaczenia informacjom błahym;
– bariery geograficzne wiążą się z ograniczeniami w zakresie przekazu informacji na dłuższe dystanse. Przez wieki należały one do kluczowych. Jednak dzięki postępowi w dziedzinie środków komunikowania się i przesyłu informacji osiągniętemu w XIX i XX oraz systematycznemu ich doskonaleniu w XXI stuleciu bariery te zostały przełamane i w zasadzie[429] odeszły do historii. Współcześnie informacja (szczególnie ta o charakterze bieżącym) może być natychmiast przekazana pomiędzy najbardziej nawet oddalonymi miejscami, chociaż ze względu na granice państwowe oddzielające różne systemy polityczne jej przepływ (zwłaszcza w zakresie treściowym) może być ograniczany;

[427] Zob. O. Wasiuta, R. Klepka, dz. cyt., t. 1, s. 60.
[428] Zob. W. Fehler, *Bariery informacyjne…*, s. 23–27.
[429] Jednak bariery geograficzne przypominają o sobie, kiedy chcemy pozyskiwać informacje bezpośrednio u źródeł znajdujących się w geograficznie odległych miejscach.

– bariery techniczno-technologiczne to przeszkody wynikające z braku zastosowania lub niedostosowania urządzeń i technologii. Z jednej strony wiążą się z technicznym i technologicznym zapóźnieniem części państw (rejonów geograficznych) oraz warstw społecznych w kwestii dostępu do najnowszych rozwiązań w sferze informacyjnej. Druga strona to nienadążanie rozwoju techniki i technologii za lawinowym przyrostem ilości informacji;
– bariery ekonomiczne obejmujące brak lub niedostatek środków finansowych potrzebnych do zaspokojenia potrzeb informacyjnych na satysfakcjonującym dany podmiot poziomie. Mogą być one związane z ograniczeniami w zakupie informacji lub z niemożnością nabycia sprzętu służącego do sprawnego i wydajnego korzystania z informacji, np. komputerów czy oprogramowania, może to być także brak środków pieniężnych na rozbudowę infrastruktury informacyjnej;
– bariery społeczno-edukacyjne powstające na gruncie: niedostatków w zakresie wykształcenia, braku aspiracji rozwojowych, braku wiedzy ogólnej, deficytu zdolności i motywacji do poszukiwania i przyswajania treści informacji, braku orientacji w odniesieniu do istnienia informacji mogących zaspokoić potrzeby informacyjne, ograniczeń uniemożliwiających lub utrudniających osobom niepełnosprawnym swobodne porozumiewanie się i/lub przekazywanie informacji;
– bariery czasowe (temporalne) wiążą się z niedostatkiem czasu na pozyskiwanie, przetworzenie i analizę, przyswojenie oraz interpretację informacji;
– bariery mentalne powstają w świadomości ludzkiej i są powodowane: niezrozumieniem, niewiedzą, utrwalonymi stereotypami i uprzedzeniami w odniesieniu do źródeł informacji. Do barier mentalnych zalicza się również: pasywne podejście do poszukiwania informacji, niechęć do podejmowania wysiłku intelektualnego, postrzeganie informacji przez pryzmat nieuzasadnionych merytorycznie, obiegowych (potocznych) opinii;
– bariery zdrowotne i emocjonalne wiążą się z różnymi formami stanów emocjonalnych (np. gniew, strach, złość) autorów i odbiorców informacji. Może to być także niechęć żywiona wobec niektórych środków przekazu, książek czy tytułów prasowych. W przypadku barier zdrowotnych rodzą je niesprawności i schorzenia, tak fizyczne, jak i psychiczne,

generujące problemy z dostępem do informacji oraz z jej przetwarzaniem i przyswajaniem;
– bariery percepcyjne związane z indywidualną odmiennością postrzegania określonych danych i informacji odbieranych za pomocą zmysłów i opartą na tym interpretacją dostarczanego przez wrażenia materiału informacyjnego;
– bariery językowo-terminologiczne wiążące się z faktem używania przez globalną populację dużej ilości języków. Bariery terminologiczne powstają z powodu stosowania terminologii hermetycznej – nieznanej lub słabo znanej odbiorcom informacji. Bariery terminologiczne tworzy także posługiwanie się ograniczonym zasobem słów oraz słownictwem prymitywnym. Do barier terminologicznych zaliczyć trzeba rozległe systemowe deformacje językowe o charakterze polityczno-poprawnościowym, reklamowym czy populistyczno-prostackim. Specyficzną barierę terminologiczną stanowi pseudonaukowy (zachowujący pozory naukowości), oparty na pustosłowiu nasyconym fasadowo-rozbudowaną frazeologią język stosowany w szeregu publikacji;
– bariery prawno-administracyjne to przede wszystkim różne rozwiązania prawno-administracyjne reglamentujące i ograniczające dostęp do informacji (np. prawo autorskie, prawo ochrony danych osobowych, prawo regulujące kwestie tajemnic informacyjnych), decyzje administracyjne ograniczające swobodę ich dystrybucji (np. wydawanie koncesji na działalność stacji telewizyjnych czy radiowych, utrudnianie działalności informacyjnej przez nakładanie wysokich podatków i opłat administracyjnych na media informacyjne). Szczególny rodzaj barier administracyjnych stanowią: cenzura, ograniczanie dostępu do informacji poprzez nieuzasadnione określanie jej jako poufnej lub tajnej oraz utrudnianie korzystania z informacji o charakterze publicznym;
– bariery organizacyjne związane z wadliwą konstrukcją systemów wytwarzania, gromadzenia, udostępniania i przesyłania informacji występują przede wszystkim w sferze publicznej. Generuje je m.in. zła organizacja (struktura) instytucji i ośrodków gromadzących i udostępniających zasoby informacyjne (archiwa, biblioteki, ośrodki dokumentacji, agencje informacyjne).

Podsumowując powyżej przedstawione rozważania i charakterystyki, należy podkreślić, że w pełni uzasadniają one analizowanie barier informacyjnych jako czynników mających wpływ na bezpieczeństwo informacyjne.

Ujawnia się ono przede wszystkim w obszarze dostępności, swobody przekazu i użyteczności informacji. Trzeba zauważyć, że każdy z podmiotów korzystających z informacji, mimo ciągłego pojawiania się nowych możliwości w zakresie dostępu do niej, musi mierzyć się z różnymi rodzajami barier informacyjnych. We wzajemnie przenikających się konfiguracjach oddziaływają one negatywnie nie tylko na potrzeby informacyjne i zachowania informacyjne związane z pozyskiwaniem informacji, ale także na całość procesów informacyjnych. Powodowane przez nie trudności zakłócają system komunikowania się poszczególnych osób i grup społecznych oraz obieg informacji między podmiotami procesów informacyjnych. Tym samym bariery wywierają niekorzystny wpływ na bezpieczeństwo informacyjne oraz bezpieczeństwo informacji, obniżając jego poziom i wymuszając angażowanie dodatkowych zasobów w celu jego zapewnienia.

Z dotychczas zgromadzonych ustaleń naukowych oraz doświadczeń praktycznych jednoznacznie wynika, że bariery informacyjne są (i będą) elementem stale obecnym w procesach kształtowania przestrzeni informacyjnej jednostek, organizacji i społeczeństw. Mając świadomość, że problematyka tych barier pozostaje od wielu lat w sferze eksploracji badawczych ekologii informacji, zajmującej się wzajemnymi oddziaływaniami człowieka na informację i odwrotnie, a także relacjami informacyjnymi między ludźmi w prywatnej i publicznej przestrzeni informacyjnej, za celowe należy uznać zintensyfikowanie zainteresowania nią ze strony przedstawicieli nauk o bezpieczeństwie.

Aby ograniczać ilość barier informacyjnych i skalę ich oddziaływania, niezbędna jest ich identyfikacja i poznanie. Dotyczy to również miejsc występowania generowanych przez wspomniane bariery szkód. Tego rodzaju spojrzenie pozwoli na: wypracowywanie sposobów zapobiegania i przełamywania barier informacyjnych, minimalizowanie skutków istnienia tych, których przełamać w danym momencie nie można, oraz efektywne zapobieganie powstawaniu nowych.

Ważnym nurtem działań w zakresie ograniczania wpływu barier na bezpieczeństwo informacyjne powinno być konsekwentne budowanie i rozwijanie indywidualnych i zespołowych kompetencji informacyjnych oraz aktywizacja informacyjna. Tą drogą nie tylko można ograniczać oddziaływanie istniejących, ale także przeciwdziałać powstawaniu nowych barier informacyjnych, a przez to wywierać dodatni wpływ na kształtowanie stanu bezpieczeństwa informacyjnego. Jest to istotne, dlatego że bariery często wzmacniane są postawami społecznymi. Duży wpływ na ograniczanie i likwidację barier ma

odpowiednio prowadzona polityka bezpieczeństwa informacyjnego, a w jej ramach uświadamianie społeczeństwu problemów informacyjnych. Trzeba podkreślić, że choć nie ma złotego środka służącego do likwidacji barier informacyjnych, to bardzo ważne jest indywidualne spojrzenie i budowanie trwałych postaw sprzyjających ich przełamywaniu. Służy temu między innymi pomoc edukacyjna i techniczna świadczona na rzecz osób najbardziej dotkniętych występowaniem omawianych barier.

4. Bezpieczeństwo informacyjne i bezpieczeństwo informacji

4.1. Bezpieczeństwo informacyjne

Bezpieczeństwo informacyjne to jeden z podstawowych wyodrębnionych przy użyciu kryterium przedmiotowego wymiarów bezpieczeństwa. Nieustanny wzrost roli informacji związany m.in. z dynamicznym rozwojem społeczeństwa informacyjnego, w którym informacja stanowi kluczowy produkt, a wiedza niezbędne bogactwo, wręcz skokowo z dnia na dzień podnosi i tak wysoką rangę tego aspektu bezpieczeństwa. Podejmując problem określenia istoty bezpieczeństwa informacyjnego, należy podkreślić, że tak jak nie ma jednej, szeroko akceptowanej ogólnej definicji bezpieczeństwa – tak i nie ma uniwersalnego ujęcia terminu „bezpieczeństwo informacyjne" oraz pojęć blisko z nim związanych. W warunkach funkcjonowania społeczeństwa informacyjnego, które zresztą wyraźnie ewoluuje w kierunku oparcia się na sztucznej inteligencji, wysiłki zmierzające do sprecyzowania tego, czym jest bezpieczeństwo informacyjne, stanowią zadanie ważne nie tylko z punktu widzenia dorobku teorii bezpieczeństwa, ale także z perspektywy potrzeb związanych z optymalizacją zarządzania tym systematycznie zyskującym na znaczeniu wymiarem bezpieczeństwa. Dążenie do poszukiwania jak najbardziej adekwatnych i odpowiadających wymogom współczesności ujęć teoretycznych bezpieczeństwa informacyjnego jest istotne także dlatego, że w przypadku tej kategorii bezpieczeństwa i związanego z nim aparatu pojęciowego istnieje duże zamieszanie. Jego skalę i zakres ukazują m.in. funkcjonujące w literaturze przedmiotu, i to w znacznej liczbie, definicje czy opisy ograniczające pojęcie bezpieczeństwa informacyjnego do kwestii ochrony informacji niejawnych czy też bezpieczeństwa systemów teleinformatycznych. Taka sytuację dostrzegł

m.in. Krzysztof Liedl, stwierdzając, że „bezpieczeństwo informacyjne bardzo często rozumiane jest jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania”[430]. Podobną ocenę sformułował także R. Kwećka, który bazując na dostępnej literaturze przedmiotu stwierdził, że „bezpieczeństwo informacyjne utożsamiane jest z reguły z bezpieczeństwem w cyberprzestrzeni, przestrzeni informatycznej lub infrastrukturze telekomunikacyjnej podmiotu”[431]. Cytowany autor podkreślił również, że to samo zjawisko występuje w opracowaniach amerykańskich, gdzie bezpieczeństwo informacyjne definiuje się „przez pryzmat przestrzeni informatycznej lub infrastruktury telekomunikacyjnej, zawężając tym samym obszar tego bezpieczeństwa tylko i wyłączne do struktury i poziomu zabezpieczeń istniejących w jego przestrzeni informatycznej”[432]. Konsekwencją takiego podejścia do problemu jest rozmywanie istoty bezpieczeństwa informacyjnego[433]. Przykładem może być jedno ze słownikowych ujęć, gdzie jest ono opisane jako „…rodzaj bezpieczeństwa dotyczący informacji na wszystkich etapach ich wytwarzania, przetwarzania, przechowywania i przesyłania, realizowanego poprzez przeciwdziałanie przed bezprawnym dostępom i jakąkolwiek ingerencją w dane, informacje i systemy informatyczne. Obejmuje metody i narzędzia ochrony zasobów informacyjnych, takie jak antywirusową ochronę komputerów i ich zasobów; zabezpieczenie techniczne wszelkich postaci danych osobowych w zakresie identyfikacji i tożsamości, tajemnicy lekarskiej, poufności bankowej, karalności, gwarancji tajemnicy korespondencji sieciowej; ochronę parametrów komputerów zarządzających systemami w przemyśle, bankowości, ochronie zdrowia, energetyce i łączności; procedury reagowania na ataki; ochronę prawną zasobów i systemów informacyjnych. Współcześnie przenika i krzyżuje się z wszystkimi dziedzinami bezpieczeństwa państwa”[434]. Jak widać, mimo dużej objętości treściowej przywołane

[430] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008, s. 19.
[431] R. Kwećka, *Bezpieczeństwo informacyjne*, [w:] *Podstawy bezpieczeństwa narodowego (państwa)*, J. Pawłowski (red.), Warszawa 2017, s. 408.
[432] Tamże.
[433] Zob. tamże.
[434] J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, *Słownik terminów z zakresu bezpieczeństwa*, Toruń 2020, s. 24. Cyt. za: T.R. Aleksandrowicz, *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze,* Warszawa 2021, s. 85.

spojrzenie jest bardzo wąskie przedmiotowo i w sumie ograniczone do ochrony zasobów informacyjnych, narzędzi i procedur ochrony danych, informacji i systemów informacyjnych. Przykładem podobnie zawężonego i mocno nieadekwatnego ujęcia jest propozycja sformułowana przez Agnieszkę Bógdał-Brzezińską oraz Marcina F. Gawryckiego, którzy bezpieczeństwo informacyjne opisują jako „…dział bezpieczeństwa, uznający wzrost roli informacji w podtrzymywaniu stabilności współczesnych gospodarek i systemów społecznych. Bezpieczeństwo informacyjne w szerszym wymiarze obejmuje zabezpieczenie przed atakiem sieciowym i skutkami takiego ataku fizycznego, który niósłby destrukcję dla funkcjonowania nowoczesnego państwa”[435]. Przygotowana na podstawie Strategicznego Przeglądu Bezpieczeństwa Narodowego *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej* z 2013 r. zagadnienie bezpieczeństwa informacyjnego również traktuje w sposób mało czytelny. Przedstawia ją bowiem przede wszystkim jako ochronę informacji niejawnych, chociaż wspomina także dość ogólnikowo o rosnącym znaczeniu bezpieczeństwa informacyjnego oraz jego cybernetycznych aspektów[436]. Takie stanowisko zaowocowało wysoce niefortunnym przedstawieniem tego wymiaru bezpieczeństwa w załączniku ze zbiorem głównych kategorii pojęciowych. Autorzy *Białej Księgi* zamieścili w nim bowiem następującą definicję – „Bezpieczeństwo informacyjne (w tym cyberbezpieczeństwo) państwa – transsektorowy obszar bezpieczeństwa, którego treść (cele, warunki, sposoby, środki) odnosi się do środowiska informacyjnego (w tym cyberprzestrzeni) państwa”[437]. Taka forma definiowania oprócz tego, że jest klasycznym przykładem logicznie błędnej konstrukcji opartej na formule *idem per idem* (to samo przez to samo), to w żaden sposób nie przyczynia się do tworzenia ładu pojęciowego w sferze bezpieczeństwa informacyjnego. W nieco zmienionym i rozbudowanym kształcie ujęcie to zostało powtórzone w projekcie doktryny bezpieczeństwa informacyjnego RP z 24 lipca 2015 r. który określa bezpieczeństwo informacyjne państwa jako „transsektorowy obszar bezpieczeństwa, którego treść odnosi się do środowiska informacyjnego (w tym cyberprzestrzeni) państwa; proces, którego celem jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej, krajowej infosferze oraz efektywną ochronę interesów

[435] A. Bógdał-Brzezińska, M.F. Gawrycki, dz. cyt., s. 323.
[436] Zob. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013, s. 171–172.
[437] Tamże, s. 248.

narodowych w zewnętrznej (obcej) infosferze. Osiąga się to poprzez realizację takich zadań, jak: zapewnienie adekwatnej ochrony posiadanych zasobów informacyjnych oraz ochrony przed wrogimi działaniami dezinformacyjnymi i propagandowymi (w wymiarze defensywnym) przy jednoczesnym zachowaniu zdolności do prowadzenia wobec ewentualnych przeciwników (państw lub innych podmiotów) działań ofensywnych w tym obszarze. Zadania te konkretyzowane są w strategii (doktrynie) bezpieczeństwa informacyjnego (operacyjnej i preparacyjnej), a do ich realizacji utrzymuje się i rozwija odpowiedni system bezpieczeństwa informacyjnego"[438]. Trudno także jako adekwatne potraktować stanowisko Piotra Potejki, który uważa, że „bezpieczeństwo informacyjne stanowi zbiór działań, metod, procedur, podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem"[439]. Nieadekwatność powyższego poglądu polega przede wszystkim na mylnym wskazywaniu instrumentów oraz sposobów (metod) ich używania służących do zapewniania bezpieczeństwa informacyjnego zamiast ukazania cech i charakterystyki tego stanu i procesu.

W nieco innym kierunku, ale także ograniczającym istotę bezpieczeństwa informacyjnego do działań ochronnych, podąża Maciej Marczyk, który wskazuje, że bezpieczeństwo informacyjne „to ochrona informacji przed niepożądanym dostępem, zniszczeniem czy ujawnieniem"[440]. W kontekście powyższych mocno zawężonych i w znacznej mierze błędnych ujęć bezpieczeństwa informacyjnego warto przywołać pogląd Elżbiety Ury oraz Stanisława Pieprznego, którzy podkreślają, że pojęcia bezpieczeństwa informacyjnego nie należy odnosić jedynie do obszaru cyberprzestrzeni i teleinformatyki oraz mylić go z bezpieczeństwem teleinformatycznym. Pojęcie to bowiem, podobnie jak pojęcie bezpieczeństwa informacji, jest węższe od bezpieczeństwa informacyjnego[441]. Przed przedstawieniem stanowisk, które cechuje dążenie do uchwycenia istoty bezpieczeństwa informacyjnego w sposób adekwatny, trzeba wspomnieć również o poglądach, które można nazwać „kunktatorskimi".

[438] *Doktryna bezpieczeństwa informacyjnego…*, s. 3.
[439] P. Potejko, *Bezpieczeństwo informacyjne*, [w:] *Bezpieczeństwo państwa*, K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), Warszawa 2009, s. 194.
[440] M. Marczyk, *Bezpieczeństwo teleinformatyczne wobec ataków terrorystycznych*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa XXI wieku*, M. Górka (red.), Warszawa 2014, s. 50.
[441] Zob. E. Ura, S. Pieprzny, *Bezpieczeństwo wewnętrzne państwa*, Rzeszów 2015, s. 35–36.

Prezentują je badacze, którzy z jednej strony deklarują dostrzeganie wielowymiarowości i szerokiego zakresu pojęcia „bezpieczeństwo informacyjne", z drugiej zaś unikają podejmowania wysiłków na rzecz sformułowania czytelnych definicji lub formułują je w sposób zagmatwany, z pozoru zachowując cechy naukowości, w rzeczywistości jednak nie wykazując dbałości o ich merytoryczną i logiczną poprawność. Egzemplifikacją pierwszej sytuacji są treści zawarte w pracy Andrzeja Nowaka i Waldemara Scheffsa poświęconej zarządzaniu bezpieczeństwem informacyjnym. Wspomniani autorzy najpierw niezbyt poprawnie językowo stwierdzają, że „kategoria »bezpieczeństwa informacyjne« jest najbardziej ogólna, ponieważ obejmuje wszystkie procesy technologiczne od pozyskania, poprzez transmisję, przetwarzanie, do przechowywania informacji w systemach informacyjnych"[442], a następnie wskazują, że „kiedy mówimy o bezpieczeństwie informacyjnym, to zawsze dotyczy to podmiotu, który jest zagrożony przez brak informacji lub możliwość utraty zasobów informacyjnych"[443]. Przykładem drugiej kategorii zachowań jest definicja bezpieczeństwa informacyjnego R. Kwećki, który formułuje ją następująco: „Bezpieczeństwo informacyjne podmiotu to proces (lub jego chwilowy stan) realizowany (utrzymywany) w kooperacji wzajemnej pozytywnej, prowadzonej przez narzędzia będące w dyspozycji podmiotu i przeznaczone do działań w przestrzeni bezpieczeństwa informacyjnego. Działania te realizowane są w ramach zintegrowanego systemu bezpieczeństwa narodowego podmiotu. Bezpieczeństwo informacyjne przejawia się w działaniach i procesach zapewniających: integralność zasobów informacyjnych podmiotu, skuteczność w ich pozyskiwaniu oraz w celowej realizacji działań socjotechnicznych i propagandowych zmierzających do wywołania pożądanych postaw lub zachowań społecznych w warunkach rzeczywistych lub potencjalnych zagrożeń wynikających z procesów informacyjnych niemających źródła w klasycznej wojnie"[444]. Z przedstawionych powyżej sformułowań wynika – po pierwsze „samodzielność" narzędzi prowadzących bez udziału ich posiadacza (operatora) politykę bezpieczeństwa informacyjnego, ponadto bezpieczeństwo informacyjne sprowadzone zostaje do roli składnika zintegrowanego sytemu bezpieczeństwa narodowego podmiotu (w domyśle – być może chodzi o państwo?). Wspomniany autor dodaje do tego kuriozalną myśl (w swoisty sposób przekreślającą wszystko to, co teoria bezpieczeństwa mówi na temat istoty elementów

[442] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, Warszawa 2010, s. 24.
[443] Tamże, s. 25.
[444] R. Kwećka, dz. cyt., s. 411.

składowych systemu bezpieczeństwa), a mianowicie stwierdza, że „bezpieczeństwo informacyjne jest zatem istotnym podsystemem systemu bezpieczeństwa narodowego, obejmuje określone struktury i narzędzia podmiotu, nakreśla jego ogólne zdolności, niezbędne do stabilnego rozwoju i przetrwania w warunkach wykorzystania szans i minimalizacji zagrożeń”[445]. W podobnym duchu próbują opisywać istotę bezpieczeństwa informacyjnego Joanna Werner i Edyta Szczepaniuk, które proponują traktować je „jako stan, w którym:

- elementy tworzące system bezpieczeństwa cechuje zdolność do ochrony przed obecnymi i przyszłymi zakłóceniami (zagrożeniami) funkcjonowania lub utraty określonych wartości – system jest odporny na zagrożenia (wewnętrzne, zewnętrzne, przypadkowe, celowe);
- bezpieczeństwo informacji jest osiągnięte i utrzymywane na założonym poziomie poufności, integralności i dostępności;
- bezpieczeństwo świadczonych usług jest osiągnięte i utrzymywane na założonym poziomie niezawodności, dostępności i integralności usług;
- zapewniona jest autentyczność i rozliczalność podmiotów związana z autoryzacją użytkowników korzystających z określonych informacji i usług;
- użytkownicy informacji i usług (pracownicy organizacji) oraz odbiorcy informacji i usług (obywatele, przedsiębiorcy, pracownicy zatrudnieni w innych organizacjach) mają świadomość i nie są podatni na zagrożenia bezpieczeństwa informacyjnego;
- aktorzy zagrożeń (także napastnicy wewnętrzni) mają małe możliwości wykorzystania systemów teleinformatycznych do generowania zagrożeń przez wykorzystanie słabości, podatności i luk w systemie zabezpieczeń”[446].

Istnieje jednak grono badaczy, którzy dążą do szerszego i bardziej precyzyjnego ujmowania istoty tego ważnego wymiaru bezpieczeństwa. Spojrzenie takie prezentuje np. Leszek F. Korzeniowski, według którego „przez bezpieczeństwo informacyjne podmiotu (człowieka lub organizacji) należy rozumieć możliwość pozyskania dobrej jakości informacji, zdolność do jej przetwarzania i wykorzystania oraz ochronę posiadanej informacji przed jej utratą”[447]. W podobnym duchu wypowiada się znany badacz problematyki bezpieczeństwa

[445] Tamże.
[446] J. Werner, E. Szczepaniuk, *Bezpieczeństwo informacyjne organizacji*, „Zeszyty Naukowe AON” 2016, nr 4, s. 17.
[447] L.F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Warszawa 2017, s. 184.

informacyjnego, Krzysztof Liderman, stwierdzający, że „bezpieczeństwo informacyjne dotyczy podmiotu (człowieka lub organizacji), który może być zagrożony utratą zasobów informacyjnych lub otrzymaniem informacji złej jakości. Zatem bezpieczeństwo informacyjne oznacza uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej oraz wykorzystywanej informacji”[448]. Zbliżony do powyżej przywołanych autorów sposób rozumowania prezentują również Józef Janczak oraz Andrzej Nowak, podkreślający, „że kiedy mówi się o bezpieczeństwie informacyjnym, to zawsze dotyczy to podmiotu, który jest zagrożony poprzez brak informacji lub możliwość utraty zasobów informacyjnych”[449]. Wymienieni badacze zaznaczają również, że „kategoria »bezpieczeństwo informacyjne« jest bardziej ogólna, ponieważ obejmuje wszystkie procesy technologiczne – od pozyskania, poprzez transmisję, przetwarzanie, do przechowywania w systemach informacyjnych”[450]. Stosunkowo czytelnie istotę bezpieczeństwa informacyjnego ujmuje Marek Madej, który podkreśla, że termin ten dotyczy „zagwarantowania sobie przez dany podmiot (np. państwo) integralności, kompletności oraz wiarygodności posiadanych zasobów informacyjnych w każdej formie, nie tylko elektronicznej. Odnosi się więc zarówno do wszelkiego rodzaju wysiłków, służących ochronie posiadanych informacji, istotnych w kontekście bezpieczeństwa (a więc mających wpływ na sprawne funkcjonowanie struktur państwowych i społeczeństwa), jak i zapewnianiu przewagi informacyjnej przez zdobywanie nowych lub bardziej aktualnych danych oraz akcje dezinformacyjne wobec ewentualnych przeciwników (państw lub innych podmiotów)”[451]. Eugeniusz Nowak i Maciej Nowak zwracają uwagę, że bezpieczeństwo informacyjne to taki stan uwarunkowań wewnętrznych i zewnętrznych, który pozwala państwu na rozwój społeczeństwa informacyjnego. Jednocześnie cytowani autorzy przedstawiają listę warunków wpływających na stan bezpieczeństwa informacyjnego, zaliczając do nich m.in. zapewnienie:

- wysokiej jakości informacji będących w dyspozycji organów państwa;
- niezakłóconego przepływu informacji w państwie;
- skutecznej ochrony informacji niejawnych oraz danych osobowych;
- poszanowania i ochrony prawa obywateli do prywatności;

[448] K. Liderman, dz. cyt., s. 22.
[449] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013, s. 18.
[450] Tamże, s. 17.
[451] M. Madej, *Rewolucja informatyczna…*, s. 18.

– nieskrępowanego dostępu do informacji publicznych[452].

Bardziej spoistą, aczkolwiek zawierającą również sporo wyliczeń przedmiotowych definicję bezpieczeństwa informacyjnego zaproponował Waldemar Kitler, wskazując, że „bezpieczeństwo informacyjne państwa stanowi transsektorową dziedzinę bezpieczeństwa narodowego[453] (węziej: bezpieczeństwa państwa), będąc procesem polegającym na dążeniu do zapewnienia wolnego od zakłóceń funkcjonowania i rozwoju państwa, w tym władzy publicznej i społeczeństwa, podmiotów rynkowych i pozarządowych w przestrzeni informacyjnej, przez swobodny dostęp do informacji[454]z jednoczesną ochroną przed negatywnymi jego skutkami (materialnymi[455] i niematerialnymi[456]) ochronę zasobów i systemów informacyjnych przed wrogimi działaniami innych podmiotów lub skutkami działania sił natury i awarii technicznych, przy jednoczesnym zachowaniu zdolności do informacyjnego oddziaływania na zachowania i postawy podmiotów międzynarodowych i krajowych"[457].

Dokonując krytycznej analizy przytoczonych na początku tego fragmentu rozważań przykładów mało adekwatnych ujęć istoty bezpieczeństwa informacyjnego oraz dostrzegając wartościowe treści w propozycjach L.F. Korzeniowskiego, K. Lidermana, J. Janczaka i A. Nowaka oraz E. Nowaka i M. Nowaka, dążących do przełamania błędnych i mających stereotypowy charakter stanowisk definicyjnych[458], należy stwierdzić, iż poprawna, odpowiadająca

[452] Zob. E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, s. 103.
[453] „To wyrażenie „zapożyczono" z projektu doktryny bezpieczeństwa informacyjnego, opracowanej w BBN" –przypis komentujący W. Kitlera, autora cytowanej definicji.
[454]„Prawo dostępu do informacji publicznej (nie każda informacja ma taki charakter!) obejmuje takie zagadnienia jak: informacja o działalności organów władzy publicznej i osób pełniących funkcje publiczne, informacje będące w posiadaniu władz publicznych oraz informacje dotyczące sfery faktów…" – przypis rozszerzający W. Kitlera, autora cytowanej definicji.
[455] „A więc stratami materialnymi i finansowymi, konsekwencjami zdrowotnymi (np. uzależnienia od Internetu), uszkodzeniami, katastrofami w transporcie i awariami technicznymi" – przypis rozszerzający W. Kitlera, autora cytowanej definicji.
[456] „Kulturowymi, ideologicznymi, społecznymi, psychologicznymi, moralnymi etc." – przypis rozszerzający W. Kitlera, autora cytowanej definicji.
[457] W. Kitler, *Organizacja bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty ustrojowe, prawno-administracyjne i systemowe*, Toruń 2018, s. 462.
[458] W przypadku E. Nowaka i M. Nowaka widać pewien brak konsekwencji w zakresie prezentowanych poglądów, bowiem obok przywołanego wcześniej ujęcia propagują oni także niezrozumiałą i nieprzystającą do rzeczywistości istniejącej w sferze informacyjnej definicję bezpieczeństwa informacyjnego, zgodnie z którą jest to „stan uzyskany w rezultacie działalności łączącej w sobie szereg cząstkowych ujęć, które odnieść należy do narzędzi i procedur ochrony danych, informacji i systemów informacyjnych. Podstawą bezpieczeństwa informacyjnego jest sposób postrzegania komputera w teoriach walki informacyjnej jako magazynu informacji i jako narzędzia sterowania" – E. Nowak, M. Nowak, dz. cyt., s. 163.

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, uwzględniając wnioski z przeprowadzonych badań oraz aktualny stan rozwoju społeczeństwa informacyjnego, uzasadnione jest sformułowanie poglądu, że bezpieczeństwo informacyjne to proces i ciąg stanów, w ramach których zapewniana jest zgodna z 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[459]. W świetle powyższej definicji zgodzić się trzeba z poglądem T.R. Aleksandrowicza, że „(...) bezpieczeństwo informacyjne ma charakter transsektorowy, ma bardzo szeroki zakres przedmiotowy i dotyczy każdego podmiotu bezpieczeństwa. Musi być zatem traktowane w kategoriach analizy systemowej”[460].

Reasumując, należy stwierdzić, iż w kwestiach związanych z pojmowaniem istoty bezpieczeństwa informacyjnego, mimo istnienia wielu publikacji naukowych, które starają się ukazać ten problem przez pryzmat nauko o bezpieczeństwie, nadal istniej sytuacja, którą można określić mianem chaosu. Jest on w dużej mierze zwiększany przez propagowanie (często na zasadzie bezrefleksyjnego powielania cudzych poglądów) definicji nieadekwatnych i nieprecyzyjnych bądź też nieaktualnych i nieodzwierciedlających aktualnego stanu wiedzy. Warto też zauważyć, iż rozważania dotyczące bezpieczeństwa informacyjnego bardzo często nadają mu formę inkluzywną, ograniczającą się tylko do ochrony informacji (w tym zwłaszcza tych niejawnych) oraz cyberprzestrzeni i zachodzących tam procesów. Jednak dostrzegając i doceniając stale rosnącą rolę i rangę technologii informatycznych, nie można w myśleniu i działaniu na rzecz bezpieczeństwa informacyjnego pomijać tradycyjnej, „klasycznej” części sfery informacyjnej, która przecież nadal funkcjonuje i jako taka musi być uwzględniana w myśleniu i działaniu na rzecz tegoż bezpieczeństwa.

---

[459] *Leksykon bezpieczeństwa wewnętrznego*, W. Fehler, J.J. Piątek, R. Podgórzańska (red.), Szczecin 2017, s. 74.
[460] T.R. Aleksandrowicz, *Zagrożenia dla bezpieczeństwa informacyjnego…*, s. 87.

4.2. Bezpieczeństwo informacji

Podejmując rozważania dotyczące istoty pojęcia „bezpieczeństwo informacji", należy zaznaczyć, iż w części publikacji termin ten stosuje się zamiennie z terminem „bezpieczeństwo informacyjne"[461]. Wprawdzie niektórzy z autorów podejmujących problematykę bezpieczeństwa informacyjnego, jak np. A. Nowak i W. Scheffs czy J. Janczak i A. Nowak, dostrzegają tą niepoprawność i zwracają uwagę, że bezpieczeństwo informacji jest częścią składową bezpieczeństwa informacyjnego[462], jednak nie jest to pogląd dominujący. Nie można w tym względzie pozostawić żadnych wątpliwości i z naciskiem trzeba podkreślić, iż bezpieczeństwo informacyjne oraz bezpieczeństwo informacji to nie synonimy. Pojęcie „bezpieczeństwo informacji" dotyczy bowiem konkretnych produktów informacyjnych, które mogą być uważane za bezpieczne wtedy, gdy będą miały niezbędne z punktu widzenia wytwórcy czy użytkownika cechy oraz będą właściwie w stosunku do przyjętych (obowiązujących) standardów bezpieczeństwa traktowane. Dostępne próby opisu istoty terminu „bezpieczeństwo informacji", podobnie zresztą jak pojęcia „bezpieczeństwo informacyjne", są nacechowane wysokim stopniem ogólności i często towarzyszącej jej nieadekwatności. Na przykład cytowany wcześniej P. Potejko bezpieczeństwo informacji odnosi „do ochrony danych, poufności danych, informacji niejawnych i informacji strategicznych"[463]. Szerzej, ale także w sposób podobny do tego wcześniej przedstawionego (ograniczając się tylko do danych), pojęcie to postrzegają J. Janczak i A. Nowak, według których bezpieczeństwo informacji to ochrona wszystkich form (także werbalnych) wymiany, przechowywania i przetwarzania danych)[464]. Niezbyt wiele (mimo występowania pewnych elementów racjonalnej diagnozy) na temat istoty bezpieczeństwa informacji dowiadujemy się z ustaleń Zbigniewa Modrzejewskiego, według którego oznacza ono „ochronę własności intelektualnej wypracowanej w danej instytucji. Nie jest to więc tylko bezpieczeństwo danych komputerowych"[465]. Nieco bardziej adekwatny (chociaż ograniczony tylko do systemów

[461] Rozważania zawarte w tym fragmencie monografii stanowią rozwinięcie ustaleń poczynionych przez autora w: W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*…, s. 30-32.
[462] Zob. A. Nowak, W. Scheffs, dz. cyt., s. 25; także J. Janczak, A. Nowak, dz. cyt., s. 18.
[463] P. Potejko, dz. cyt., s. 194.
[464] Zob. J. Janczak, A. Nowak, dz. cyt., s. 20.
[465] Z. Modrzejewski, *Operacje informacyjne*, Warszawa 2015, s. 59.

teleinformatycznych) charakter ma próba zdefiniowania bezpieczeństwa informacji zawarta w *Doktrynie systemów łączności i informatyki Sił Zbrojnych RP*, zgodnie z którą „bezpieczeństwo informacji ma na celu zapewnienie systemom i sieciom teleinformatycznym oraz informacji wytwarzanej, przetwarzanej, przechowywanej lub przekazywanej w tych systemach i sieciach takich cech, jak: dostępność, integralność, autentyczność, poufność i niezaprzeczalność”[466]. Zdecydowanie celniej istotę bezpieczeństwa informacji charakteryzuje natomiast K. Liderman, który twierdzi, że oznacza ono „uzasadnione (np. analizą ryzyka i przyjętymi metodami postępowania z ryzykiem) zaufanie, że nie zostaną poniesione potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego) ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej, przetwarzanej i przesyłanej w określonym systemie jej obiegu”[467]. Cytowany autor stwierdza również, z czym należy się zgodzić, że „bezpieczeństwo informacji jest składową bezpieczeństwa informacyjnego – informację należy najpierw pozyskać, a potem w trakcie jej wykorzystania przez podmiot (przechowywania, przetwarzania, przesyłania) odpowiednio chronić”[468]. Zgodnie z treściami normy PN-ISO/IEC 27001:2007 bezpieczeństwo informacji to „zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność”[469]. W innej normie – PN-ISO/IEC17799:2007 – bezpieczeństwo informacji jest ujmowane, z naciskiem na przedstawienie jego znaczenia dla działalności biznesowej, jako „ochrona przed szerokim spektrum zagrożeń w celu zapewnienia ciągłości działania, minimalizacji ryzyka i maksymalizacji zwrotu z inwestycji oraz możliwości biznesowych”[470]. Zauważając zarówno słabości, jak i zalety powyżej pokazanych propozycji definicyjnych, można przyjąć, iż bezpieczeństwo informacji to stan i proces, w ramach którego zapewnia się w całym cyklu życia informacji (powstanie, przekazanie, przetworzenie, kopiowanie, wykorzystywanie, przechowywanie, gromadzenie, niszczenie) osiąganie i utrzymywanie, z uwzględnieniem zaprogramowanych (obowiązujących) standardów jakościowych i ilościowych, na pożądanym

[466] *Doktryna systemów łączności i informatyki Sił Zbrojnych RP D/6*, Bydgoszcz 2013, s. 20.
[467] K. Liderman, dz. cyt., s. 22.
[468] Tamże.
[469] PN-ISO/IEC 27000:2012, *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji. Przegląd i terminologia*, Warszawa 2012, s. 10.
[470] PN-ISO/IEC 27000:2007, *Technika informatyczna – Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji – Wymagania*, Warszawa 2007, s. 9.

przez dany podmiot poziomie takich fundamentalnych właściwości informacji, jak: dostępność, użyteczność, integralność, autentyczność, niezaprzeczalność, rozliczalność oraz tam, gdzie jest to potrzebne, także poufność czy tajność. Bazując na istniejącym dorobku naukowym, w tym m.in. na wynikach badań prezentowanych przez Jacka Łuczaka i Marcina Tyburskiego[471], K. Lidermana[472], J. Janczaka i A. Nowaka[473], Paulinę Motylińską[474] czy Katarzynę Materską[475] oraz obowiązujących definicjach legalnych (prawnych), można dokonać syntetycznego scharakteryzowania wymienionych powyżej atrybutów decydujących o tym, że informację można traktować jako bezpieczną.

Na bazie treści rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności „dostępność" można traktować jako właściwość określającą, że zasób informacyjny jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy z tym zasobem[476]. W bardziej szczegółowym ujęciu informacja jest dostępna wtedy, gdy podawana jest w takiej formie i w taki sposób, który pozwala każdemu zainteresowanemu użytkownikowi uzyskanie dotarcia do jej treści na równych zasadach z innymi. Informacja dostępna to taka informacja, która umożliwia wszystkim korzystającym łatwą orientację w jej treści oraz może być skutecznie odbierana i rozpoznawana przy użyciu dostępnych kanałów percepcyjnych[477]. Dostępność można postrzegać zarówno w sposób wąski, jak i szeroki. W ujęciu wąskim istotę dostępności określa to, że podmiot uprawniony może korzystać z informacji (ma do niej dostęp) zawsze wtedy, kiedy jest mu ona potrzebna. W szerszym znaczeniu o dostępności możemy mówić w kontekście istnienia i skutecznego egzekwowania prawa dostępu do informacji oraz swobody

[471] Zob. J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji*, Poznań 2010, s.19–28.
[472] Zob. K. Liderman, dz. cyt., s. 18–20.
[473] Zob. J. Janczak, A. Nowak, dz. cyt., s. 18.
[474] Zob. O. Wasiuta, R. Klepka, dz. cyt., t. 2, s. 652.
[475] Zob. K. Materska, *Zarządzanie informacją i wiedzą*…, s. 370–378.
[476] Zob. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017, poz. 2247).
[477] Zob. Wytyczne dla dostępności informacji. Technologie informacyjno-komunikacyjne (TIK) w zapewnianiu dostępności informacji w procesie uczenia się (ICT4IAL), European Agency for Special Needs and Inclusive Education 2015, s. 10, https://www.europeanagency.org/sites/default/files/Guidelines%20for%20Accessible%20Information_PL.pdf [dostęp: 17.05.2021 r.].

wytwarzania[478] i wymiany informacji, dla której fundamentalne znaczenie posiada zakaz stosowania cenzury prewencyjnej. Dostępność ma także aspekt międzynarodowy, określony m.in. w Konwencji o ochronie praw człowieka i podstawowych wolności sporządzonej w Rzymie dnia 4 listopada 1950 roku, która mówi o prawie do „otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe"[479]. W podobnym kierunku idą także normy Międzynarodowego Paktu Praw Obywatelskich i Politycznych otwartego do podpisu w Nowym Jorku dnia 19 grudnia 1966 roku, w którym zawarto prawo do swobody „poszukiwania, otrzymywania i rozpowszechniania wszelkich informacji i poglądów, bez względu na granice państwowe, ustnie, pismem lub drukiem, w postaci dzieła sztuki bądź w jakikolwiek inny sposób według własnego wyboru"[480].

Użyteczność to kolejna cecha bezpiecznej informacji, którą należy rozumieć jako posiadanie walorów decydujących o tym, że informacja nadaje się do wykorzystania przez podmiot, który ją posiada lub w jakiś inny sposób nią dysponuje. Jak podkreślają Katarzyna Ciach i Jarosław Dębski, użyteczność informacji określana jest także przez przydatność w procesie decyzyjnym. Użyteczną informacją jest taka, na podstawie której jej użytkownik może przeprowadzić ocenę sytuacji i zdarzeń w różnych perspektywach i w rezultacie podjąć decyzję o ograniczonym ryzyku popełnienia błędu. Użyteczność informacji budowana jest m.in. na gruncie jej zrozumiałości, wiarygodności, kompletności, terminowości, odpowiedniości, sprawdzalności i neutralności. Ta ostatnia właściwość oznacza, że informacja jest wolna od odchyleń mających wymusić jakiś sposób zachowania bądź końcowy rezultat[481].

W odniesieniu do użyteczności możemy stosować jej podział na realną i potencjalną. Klasyfikacja ta wiąże się z faktem, że pewne informacje możemy wykorzystywać na bieżąco z chwilą ich pozyskania, w odniesieniu do innych zaś cechy, które czynią je użytecznymi, pojawiają się dopiero w jakiejś perspektywie czasowej, np. dzięki powiązaniu ich z nowymi informacjami lub

[478] Szerzej na ten temat zob. K. Machowicz, *Wolność wypowiedzi w Polsce wobec ochrony prawa do prywatności*, Warszawa 2018.
[479] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, art. 10 (Dz.U. 1993, nr 61, poz. 284).
[480] Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r., art. 19 (Dz.U. 1977, nr 38, poz. 167).
[481] Zob. K. Ciach, J. Dębski, *Użyteczność informacji finansowych: wybrane aspekty*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2015, nr 117, s. 32–33.

zaistnieniu nowych potrzeb informacyjnych. Warto zwrócić uwagę, że cecha użyteczności w wielu przypadkach może zmaterializować się dopiero wtedy, gdy zgromadzimy znaczną ilość informacji na jakiś temat. Potrzebna jest w związku z tym zdolność do oceny, czy dana informacja może być przydatna teraz czy w przyszłości oraz czy trzeba ją uzupełnić bądź przetworzyć, aby uzyskała walor użyteczności. Dla budowania użyteczności informacji bardzo istotne jest zapewnienie pluralizmu informacyjnego w sferze publicznej oraz dostępu do różnorodnych źródeł i zasobów informacyjnych. Jest to niezbędne, aby zagwarantować możliwości weryfikacji otrzymywanych informacji pod kątem ich wiarygodności, co pozwala na unikanie lub minimalizowanie zakresu oddziaływania szeregu zagrożeń informacyjnych, w tym zwłaszcza dezinformacji i manipulacji. W odniesieniu do integralności informacji można wskazać na następujące przykładowe jej ujęcia w literaturze przedmiotu:

– własność wykluczająca niekontrolowane wprowadzenie zmian do informacji[482];
– cecha oznaczająca, że dane i informacje są poprawne, nienaruszone i nie były poddane manipulacji[483];
– cecha polegająca na zachowaniu spójności, dokładności i wiarygodności danych w całym ich cyklu życia, a także chronieniu ich tak, żeby w sposób nieautoryzowany nie zostały zmienione, dodane lub usunięte[484].

W oparciu o treść wspomnianego już wcześniej rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności integralność informacji można określić jako właściwość polegającą na tym, że informacja czy zasób informacyjny nie zostały zmodyfikowane w sposób nieuprawniony[485]. Generalnie o zapewnieniu informacji cechy integralności możemy mówić wówczas, gdy zablokowana jest możliwość umyślnej lub nieumyślnej nieautoryzowanej zmiany czy usunięcia informacji. Informacje integralne to takie, które poprawnie oddają istotę danego stanu rzeczy oraz nie zostały naruszone w drodze od wytwórcy (źródła) do odbiorcy. Inaczej rzecz ujmując, są to informacje, które nie zostały poddane manipulacji. W tym miejscu należy

[482] Zob. W. Gogołek, W. Cetera, *Logistyka i zarządzanie w mediach. Leksykon tematyczny. Zarządzanie, IT*, Warszawa 2014, s. 103.
[483] Zob. K. Liderman, dz. cyt., s. 19.
[484] Zob. S. Kaczmarek, *Integralność danych, czyli imperatyw kategoryczny bezpieczeństwa IT*, http://it-filolog.pl/integralnosc-danych-czyli-imperatyw-kategoryczny-bezpieczenstwa-it/ [dostęp: 20.05.2021 r.].
[485] Zob. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności…

podkreślić, iż integralności informacji nie narusza jej interpretacja. Jednak istotne jest w tym przypadku zaznaczenie i wyraźne odseparowanie informacji pierwotnej od ocen i komentarzy z nią związanych.

Jeżeli zbadać autentyczność, to w świetle kilkakrotnie już przywoływanych Krajowych Ram Interoperacyjności jest to właściwość polegająca na tym, że pochodzenie lub zawartość informacji opisujących obiekt jest taka, jak deklarowana. W bardziej rozwiniętej formie można powiedzieć, że autentyczność oznacza pewność zarówno co do autorstwa, jak i treści informacji, w tym zapewnienie, że tożsamość (pochodzenie) podmiotu operującego informacją lub zasobu informacyjnego jest taka, jak przedstawiają to stosowne deklaracje.

Niezaprzeczalność to cecha pozwalająca na ustalenie, że uczestnictwo danej osoby w wymianie informacji jest niepodważalne. Na tak rozumianą niezaprzeczalność składają się:

– zapewnienie niezaprzeczalności otrzymania informacji rozumianej jako zdolność do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie;
– zapewnienie niezaprzeczalności rozumianej jako zdolność do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie.

Niezaprzeczalność to nic innego jak brak możliwości wyparcia się przez podmiot lub podmioty uczestniczące w procesach tworzenia i wymiany informacji swego w nich uczestnictwa (w całości lub w części). Z cechą niezaprzeczalności ściśle związana jest rozliczalność, czyli taki atrybut bezpieczeństwa informacji, która zapewnia, że określone działania podmiotu pozostające w związku z daną informacją mogą być jednoznacznie przypisane temu podmiotowi[486]. W stosunku do rozliczalności można powiedzieć również, że jest to właściwość systemu przechowywania i obiegu informacji, która pozwala przypisać określone działanie w tym systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie[487].

Atrybut poufności oznacza, że informacja jest dostępna tylko dla podmiotów uprawnionych, posiadających odpowiednie prawa dostępu i nie jest udostępniana lub wyjawiana podmiotom nieupoważnionym. Poufność wiąże się z zapewnieniem ochrony przed niedozwolonym lub niezgodnym z prawem

[486] Zob. J. Kowalewski, M. Kowalewski, *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm,* Warszawa 2017, s. 25–26.
[487] Zob. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności…

przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem informacji poufnej za pomocą odpowiednich środków technicznych lub organizacyjnych. Ujmując poufność szerzej, można ją traktować jako udostępnianie informacji do użytku jakiegoś określonego grona osób (podmiotów organizacyjnych) i jednoczesne blokowanie dostępu do niej tym osobom i podmiotom, które nie powinny się z nią zapoznać. Dodatkowo bardzo często zachowanie poufności ma uniemożliwić wykrycie źródła, miejsca przeznaczenia informacji itp. Zapewnienie poufności informacji to nie tylko ograniczenie do niej dostępu, ale także stworzenie takich warunków posługiwania się informacją poufną, aby nie można było się z nią zapoznać w sposób nieuprawniony. Poufność jest również normą etyczną obowiązującą w moralności powszechnej oraz etyce szeregu zawodów (lekarze, psychoterapeuci, adwokaci, notariusze, bankowcy i inni). W obu systemach istnieją jednak istotne różnice co do mocy jej obowiązywania. W moralności powszechnej przyjmuje się, że należy dochować poufności, a więc nie ujawniać informacji, co do zatajenia których zostaliśmy przez osobę posiadającą owe informacje zobowiązani. Oznacza to, że za poufną uznaje się tę informację, o której nieujawnianie zwrócił się do nas jej powiernik. Poufność rozciąga się także na właściwe, czyli zgodne z przyjętymi zobowiązaniami gospodarowanie informacjami, które dany podmiot otrzymuje wraz z zastrzeżeniem zachowania ich tylko dla siebie lub wskazanego kręgu odbiorców. Tak rozumiana poufność nakłada się na pojęcie dyskrecji, która jest elementem dobrego wychowania, kultury osobistej, kultury politycznej czy biznesowej i nakazuje powściągliwość w rozpowszechnianiu czy używaniu informacji przekazanych w opisanym wyżej trybie.

W przypadku etyki zawodowej zasada poufności jest znacznie silniejsza. Zostają nią objęte wszelkie informacje uzyskane w procesie kontaktów zawodowych. Informacje uzyskane przez przedstawicieli zawodów zaufania publicznego (adwokatów, radców prawnych, lekarzy, psychoterapeutów i innych) w związku z pełnieniem przez nich ról zawodowych stają się „automatycznie" poufne. Nie wymagają dodatkowej obligacji czy złożenia obietnicy. To, co w moralności ogólnej jest dopuszczalne, staje się nakazane w etyce szeregu zawodów zaufania publicznego, bowiem osoby wykonujące takie zawody są powiernikami danych i informacji o szczególnym znaczeniu dla ich klientów (pacjentów). Stan taki wyklucza więc rozwiązania o połowicznym charakterze[488].

[488] Zob. A. Bogatyńska-Kucharska, *Normy poufności i taktu w etyce ogólnej oraz w etyce zawodowej psychoterapeutów*, „Etyka" 2019, nr 2, s. 108–109.

Jeżeli przyjrzeć się tajności, to ten atrybut bezpieczeństwa informacji wskazuje i informuje o wymaganym (stosowanym) poziomie ochrony przed nieuprawnionym dostępem. Poziom tej ochrony jest uzgadniany przez podmioty dostarczające i otrzymujące informacje[489]. Tajność w praktyce oznacza wprowadzanie zdecydowanie bardziej rygorystycznego w porównaniu do poufności reżimu postępowania dotyczącego warunków (prawnych, osobowych, organizacyjnych czy techniczno-technologicznych) wytwarzania, przechowywania i przekazywania informacji określanych jako tajne. Do przestrzegania szeregu tajemnic obligują nas przepisy prawa, ale także nasze tajemnice są przedmiotem ochrony. Prawo chroni m.in. tajemnicę zawodową, bankową, lekarską, tajemnicę głosowania, komunikowania się, nasze dane osobowe i wiele innych. Jak słusznie podkreśla Agnieszka Kukla, zachowanie prawa do tajemnicy jest istotnym wyróżnikiem systemów demokratycznych, zaś jej pozbawianie – symptomem totalitaryzacji[490].

Podsumowując powyższe rozważania, należy jeszcze raz podkreślić znaczną i wyraźną autonomiczność pojęcia „bezpieczeństwo informacji" w sensie semantyczno-treściowym w odniesieniu do bezpieczeństwa informacyjnego, ale jednocześnie także istnienie bezpośrednich i ścisłych związków tych dwóch pojęć na płaszczyźnie funkcjonalnej informacyjnego wymiaru bezpieczeństwa. Zaznaczyć należy również, że katalog cech, które wpływają na bezpieczeństwo informacji, jest dość szeroki, jednak, jak wskazano w powyższych analizach, można i należy wśród nich wyodrębniać te o znaczeniu fundamentalnym, bez uwzględnienia których nie może być mowy o informacji bezpiecznej.

4.3. Polityka bezpieczeństwa informacyjnego

Kwestia tego, jak zapewniać i utrzymywać odpowiedni poziom bezpieczeństwa, stanowi jeden z centralnych punktów zainteresowań wszystkich tych podmiotów (państw, ich sojuszniczych związków, organizacji międzynarodowych), które mają w swoich kompetencjach powinność jego zagwarantowania. Generalnie należy uznać, że w działaniach mających zapewnić bezpieczeństwo chodzi o uzyskanie kontroli nad tym, co zagraża cenionym przez dany podmiot

[489] Zob. K. Liderman, dz. cyt., s. 19.
[490] Zob. A. Kukla, *Tajność i jawność w kontekście ochrony informacji*, „Civitas. Studia z Filozofii Polityki" 2017, nr 20, s. 119–120.

(jednostkowy, zbiorowy) wartościom, w taki sposób, aby nie tylko nie było zagrożone jego przetrwanie, ale żeby miał on również zapewnione możliwości realizacji swoich aspiracji rozwojowych. Jednym z najważniejszych narzędzi służących do osiągania tego celu jest polityka bezpieczeństwa. Ponieważ jak dotychczas w toku rozwoju cywilizacyjnego nie ukształtowały się inne niż państwa podmioty, które posiadałyby możliwości i były gotowe do brania kompleksowej odpowiedzialności za bezpieczeństwo w skali tak wewnątrzpaństwowej, jak i w relacjach międzynarodowych, politykę bezpieczeństwa rozpatrywać trzeba przede wszystkim z perspektywy państwowej. Politykę taką należy rozumieć jako celową, planową, zorganizowaną w ramach państwa oraz pod kierownictwem organów państwowych działalność (koncepcyjną oraz praktyczną) podmiotów państwowych, społecznych i prywatnych, ukierunkowaną na uzyskiwanie i utrzymywanie jak najwyższego w danych warunkach poziomu bezpieczeństwa, połączoną z tworzeniem rozwiązań zapewniających zdolności do sprawnych i skutecznych reakcji na pojawiające się wyzwania i materializujące się zagrożenia[491]. W ramach realizacji polityki bezpieczeństwa państwa sięgają po różnorodne dostępne im zasoby, stosują także zróżnicowane instrumenty i metody. Jak wiadomo, bezpieczeństwo, które figuruje na czołowym miejscu listy wartości pożądanych i chronionych zarówno przez jednostki, jak i podmioty zbiorowe, ma złożoną strukturę podmiotową i przedmiotową. Jednym z jej elementów na poziomie przedmiotowym jest bezpieczeństwo informacyjne. W związku z tym uzyskanie i utrzymanie możliwie najlepszego stanu bezpieczeństwa wymaga również działań na rzecz jego informacyjnego wymiaru. Jest to szczególnie istotne w warunkach funkcjonowania społeczeństwa informacyjnego, w którym rola i ranga informacji systematycznie wzrasta. Jak wcześniej ustalono, bezpieczeństwo informacyjne to proces i ciąg stanów, w ramach których zapewniana jest zgodna z standardami demokratycznego państwa prawa swoboda wytwarzania, dostępu, gromadzenia, przetwarzania i przepływu odpowiedniej ilości wysokiej jakości informacji, połączona z racjonalnym, prawnym i zwyczajowym wyodrębnianiem takich ich kategorii, które podlegają szczególnej ochronie bądź reglamentacji ze względu na bezpieczeństwo podmiotów, których one dotyczą[492]. Jednocześnie wiadomo, co także potwierdza przyjęta definicja, że działania na rzecz

[491] Zob. W. Fehler, *Polityka bezpieczeństwa jako szczególny wymiar polityki państwa*, [w:] *Współczesne bezpieczeństwo polityczne*, S. Jaczyński, M. Kubiak, M. Minkina (red.), Warszawa-Siedlce 2012, s. 342.
[492] Zob. podrozdział 4.1, *Bezpieczeństwo informacyjne.*

bezpieczeństwa informacyjnego nie są przedsięwzięciami prostymi i łatwymi do realizacji. Wynika to zarówno ze złożonej natury informacji, jak i całego środowiska informacyjnego, która powoduje, że mimo ciągle powiększanego zasobu wiedzy teoretycznej oraz doświadczeń praktycznych, wspieranych przez nowoczesne rozwiązania techniczne, zapobieganie i zwalczanie zagrożeń godzących w bezpieczny pod względem informacyjnym byt i rozwój rodzaju ludzkiego jest niekończącą się misją. Trzeba także uznać fakt istnienia mniej eksponowanych, ale nie mniej ważnych z punktu widzenia bezpieczeństwa barier informacyjnych. Występując pod różnymi postaciami, nieustannie towarzyszą one sferze bezpieczeństwa informacyjnego, nie tylko jako pewien negatywny potencjał blokujący czy utrudniający rozwój infosfery, ale także jako konkretyzujące się w różnych formach przeszkody w zakresie osiągania założonego poziomu bezpieczeństwa informacyjnego, zwłaszcza zaś w zakresie szeroko rozumianego dostępu do informacji. Uwzględniając powyżej przedstawiony sposób pojmowania bezpieczeństwa informacyjnego oraz jego uwarunkowania, przyjęto, że polityka bezpieczeństwa informacyjnego to celowa i zorganizowana działalność państwa prowadzona z udziałem podmiotów społecznych i prywatnych, ukierunkowana na tworzenie i utrzymywanie w jak najlepszym jakościowo i ilościowo kształcie własnych zasobów informacyjnych i mechanizmów ich użytkowania, połączona z efektywną ochroną przed destrukcyjnym oddziaływaniem zdarzeń losowych, podmiotów konkurencyjnych, nieprzyjaznych czy wrogich oraz usuwaniem i minimalizowaniem barier[493].

W ramach tak rozumianej polityki bezpieczeństwa informacyjnego należy uporczywie dążyć zarówno do oddalania, minimalizowania i przejmowania kontroli nad zagrożeniami, jak i zmniejszania niedogodności związanych z istnieniem barier informacyjnych. Jest to jeden z fundamentalnych nurtów aktywności państw na rzecz funkcjonowania w bezpiecznym środowisku informacyjnym. Jednak nie zawsze udaje się go w sposób efektywny łączyć z drugim nurtem działań polegającym na tworzeniu warunków maksymalnie ograniczających możliwości powstawania barier i „wydajność" źródeł zagrożeń, co powoduje, że sfera bezpieczeństwa informacyjnego staje się niestabilna i podatna na różnego rodzaju turbulencje. Ponieważ, jak już wskazywano, bezpieczeństwo informacyjne to pewien pożądany stan, ale i ciągle trwający proces, to jego poziom i perspektywa utrzymania w założonym odcinku czasu podlega

[493] Zob. W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*…, s. 33.

dynamicznym przeobrażeniom stosownie do występujących zmian uwarunkowań. Ta zmienność i brak stałości bezpieczeństwa informacyjnego powoduje, że jednym z najważniejszych elementów działań w zakresie polityki bezpieczeństwa informacyjnego musi być systematyczne obserwowanie, diagnozowanie i ocenianie jego stanów oraz towarzyszących im uwarunkowań oraz doskonalenie środków i stosowanych w ich ramach instrumentów służących do jego zapewnienia. Nie należy to do zadań łatwych, ponieważ:

- istnieje duża rozbieżność interesów w sferze bezpieczeństwa informacyjnego podmiotów państwowych, które o nie zabiegają;
- część działań państw w infosferze ma zaplanowany wrogi wobec innych charakter i trudno poddaje się kompromisowym uzgodnieniom;
- występuje duża zmienność jakości i ilości zagrożeń dla bezpieczeństwa informacyjnego;
- zagrożenia płyną z różnych stron i nie wszystkie z nich można zidentyfikować;
- skryta natura niektórych zagrożeń informacyjnych ogranicza możliwości diagnostyczne i reaktywne;
- mimo zniwelowania części barier nadal stanowią one liczące się przeszkody, a na miejsce tych usuwanych pojawiają się nowe (np. bariera nadmiaru informacji).

Polityka bezpieczeństwa informacyjnego należy do tej sfery aktywności państw, która ze względu na swoje fundamentalne znaczenie dla ich egzystencji i rozwoju wymaga szczególnie przemyślanych poczynań ze strony wszystkich tworzących oraz realizacyjnych ją podmiotów. Istotnym wsparciem dla tego typu działań jest prowadzenie różnorodnych analiz dotyczących zarówno praktyki, jak i teorii. W tym kontekście jako konieczny jawi się wymóg stosowania w miarę ujednoliconego i odpowiadający aktualnemu stanowi wiedzy aparatu pojęciowego. Zważywszy na to, niezbędne są również systematycznie prowadzone dociekania badawcze, które pozwolą na adekwatne ujmowanie istoty, celów, środków, instrumentów oraz metod polityki bezpieczeństwa informacyjnego. Należy dodać, że zgodnie z paradygmatem systemowym chodzi nie tylko o to, aby sprecyzować ich zakres znaczeniowy, ale również ustalić i scharakteryzować zachodzące pomiędzy nimi związki. Wskazana problematyka posiada złożony charakter, co ujawnia się już na poziomie definiowania istoty polityki bezpieczeństwa informacyjnego. Kompleksowe ujęcie tej polityki musi obejmować ograniczenie negatywnych impulsów pochodzących ze strony innych państw, szeroko rozumianego środowiska międzynarodowego

i wewnętrznego oraz zapewnienie wewnętrznej stabilności i harmonii informacyjnej m.in. poprzez ochronę i pomnażanie tych zasobów informacyjnych, które mają największą wartość dla danego państwa i jego mieszkańców.

Powstają także sytuacje, w których siła zagrożeń informacyjnych i/lub skala wyzwań uniemożliwia lub czyni mało wydajnymi zabiegi o uzyskanie i utrzymanie pożądanego poziomu bezpieczeństwa informacyjnego. Istnienie takich opcji obliguje do poszukiwania koncepcji postępowania najbardziej efektywnych w danych warunkach. Nie da się ich wypracować w odpowiednim dla potrzeb danego państwa kształcie bez uwzględnienia aktualnego i perspektywicznego stanu środowiska informacyjnego. Nie może to nastąpić także w oderwaniu od realiów ogólnych uwarunkowań bezpieczeństwa oraz racji stanu i wypływających z niej strategicznych wizji polityki bezpieczeństwa danego państwa. Płaszczyzną, na której można skutecznie dążyć do rozwiązywania i redukowania tych problemów, jest polityka bezpieczeństwa informacyjnego. Zapewnienie odpowiedniego (pożądanego) poziomu realizacji polityki bezpieczeństwa informacyjnego wymaga zastosowania właściwych metod zarządzania. Zasady skutecznego zarządzania narzucają z kolei ustanowienie reguł prowadzenia i odpowiedniego modyfikowania polityki bezpieczeństwa informacyjnego. Rosnąca złożoność uwarunkowań związanych z dynamicznym rozwojem globalnego społeczeństwa informacyjnego, w tym szczególnie skomplikowana natura wielu wyzwań i zagrożeń informacyjnych oraz istnienie barier informacyjnych, powoduje, iż poprawnie konceptualizowana i realizowana polityka bezpieczeństwa informacyjnego musi uwzględniać działania podejmowane samodzielnie oraz we współpracy z innymi podmiotami. Wymaga to posiadania zdolności do zawierania kompromisów i równoważenia interesów oraz długofalowej współpracy. Zmienny charakter sfery bezpieczeństwa informacyjnego narzuca także konieczność odpowiedniego reagowania na zachodzące lub przewidywane przeobrażenia środowiska bezpieczeństwa, szczególnie zaś jego informacyjnego wymiaru. Powinno to następować w trybie okresowych audytów polityki bezpieczeństwa informacyjnego i stosownego do ich wyników rekonfigurowania jej celów i zadań. W przypadku zaistnienia daleko idących zmian o charakterze systemowym (np. prawnych czy technologicznych) powinno się dokonywać zredefiniowania tej polityki. W związku z tym niezbędne jest szerokie włączanie w proces tworzenia i realizacji polityki bezpieczeństwa informacyjnego odpowiednio przygotowanych ekspertów. Muszą oni posiadać wiedzę przydatną zarówno do tworzenia merytorycznych podstaw w zakresie wytyczania celów i podejmowania

decyzji strategicznych, jak i do wspierania procesów decyzyjnych związanych z bieżącą realizacją polityki bezpieczeństwa informacyjnego. Niezależnie od konieczności szerokiego używania wiedzy eksperckiej, tworzenie przemyślanej i odpowiedniej do potrzeb danego państwa polityki bezpieczeństwa informacyjnego wymaga stosowania określonych reguł postępowania. Do podstawowego ich zbioru należą:

- przyjęcie adekwatnego do istniejącego stanu wiedzy teoretycznej i praktyki sposobu definiowania i interpretowania pojęcia „bezpieczeństwo informacyjne";
- uchwycenie, skatalogowanie oraz zhierarchizowanie bieżących oraz perspektywicznych uwarunkowań bezpieczeństwa informacyjnego;
- przyjęcie norm określających poziom bezpieczeństwa informacyjnego, który dany podmiot chce osiągać na poszczególnych etapach realizacji polityki bezpieczeństwa informacyjnego;
- ustalenie sposobów bieżącej oraz okresowej oceny stanu bezpieczeństwa informacyjnego;
- określenie metod monitorowania oraz prognozowania sytuacji w dziedzinie bezpieczeństwa informacyjnego;
- określenie możliwych do zastosowania środków realizacji polityki bezpieczeństwa informacyjnego;
- wybór instrumentów realizacyjnych polityki bezpieczeństwa informacyjnego oraz metod ich stosowania;
- ustalenie zasad i sposobów kontrolowania skuteczności implementacji polityki bezpieczeństwa informacyjnego.

Trzeba zaznaczyć, że – aby polityka bezpieczeństwa informacyjnego mogła osiągnąć walor poprawnego sformułowania i uzyskać możliwość właściwego wprowadzenia w życie – oprócz zastosowania przy jej tworzeniu powyższych reguł, powinna być konstruowana z uwzględnieniem dwóch aspektów kształtujących fundamenty bezpieczeństwa informacyjnego:

- obiektywnego – dotyczącego istnienia realnych i potencjalnych zagrożeń, wyzwań oraz barier na drodze do osiągania tego bezpieczeństwa;
- subiektywnego – związanego z percepcją zagrożeń, wyzwań i barier oraz budowania na tej bazie koncepcji ich przezwyciężania i oddalania.

Polityka bezpieczeństwa informacyjnego może być tworzona i realizowana w ramach szerokiego (pozytywnego) postrzegania bezpieczeństwa informacyjnego lub też spojrzenia wąskiego (negatywnego). W razie wyboru wariantu pierwszego jej założenia obejmować będą takie środki, instrumenty

i metody oddziaływania na środowisko informacyjne (zewnętrzne i wewnętrzne), aby sprzyjało ono efektywnemu i stabilnemu funkcjonowaniu podmiotu tej polityki w wymiarze informacyjnym i zapewniało możliwość osiągania i utrzymywania stosownego do potrzeb poziomu bezpieczeństwa informacyjnego. W drugim wariancie jej założenia koncentrować się będą na przedsięwzięciach mających zapewnić skuteczną ochronę w przypadku zmaterializowania się zagrożeń i powstania barier. Najbardziej celowe jest jednak łączenie w sposób zrównoważony (odpowiednio do stawianych diagnoz) rozwiązań z zakresu obydwu wariantów.

Polityka bezpieczeństwa informacyjnego zapewnia solidne podstawy dla bezpieczeństwa państwa i bezpieczeństwa ludzi. Jedną z ważniejszych korzyści płynących z faktu konceptualizacji i realizacji takiej polityki jest tworzenie wspólnej dla całego społeczeństwa wizji sprzyjającej rozwojowi i bezpiecznemu bytowi infosfery. Polityka ta pomaga także zapewnić spójność procesów decyzyjnych i ustalić porządek priorytetów między różnymi uczestniczącymi w nich podmiotami. Polityka bezpieczeństwa informacyjnego w szczególności pozwala na:

– zdefiniowanie szerokiej wizji bezpieczeństwa informacyjnego z uwzględnieniem różnorodnych potrzeb poszczególnych podmiotów zbiorowych i jednostkowych;
– opracowanie skutecznych zasad realizacji wspólnej wizji bezpieczeństwa informacyjnego;
– zwiększenie odpowiedzialności instytucji działających w sektorze bezpieczeństwa informacyjnego;
– budowanie narodowego konsensusu w sprawach bezpieczeństwa informacyjnego;

W ramach polityki bezpieczeństwa informacyjnego dąży się przede wszystkim do:

– identyfikacji i oddalania zagrożeń;
– minimalizacji skutków tych zagrożeń, których nie udało się zażegnać;
– budowania potencjału (organizacyjnego, materialnego, personalnego) pozwalającego na skuteczne reagowanie na zagrożenia w informacyjnej sferze bezpieczeństwa;
– skutecznego podejmowania wyzwań w sferze bezpieczeństwa informacyjnego;

– kształtowania otoczenia w taki sposób, aby generowało ono jak najmniej zagrożeń i wyzwań dla bezpieczeństwa informacyjnego oraz sprzyjało rozwojowi pozytywnych cech społeczeństwa informacyjnego.

Podsumowując analizy dotyczące polityki bezpieczeństwa informacyjnego, należy stwierdzić, że głównym jej kreatorem musi być państwo. Tylko ono bowiem posiada odpowiedni zestaw środków mogących w sposób wielopłaszczyznowy i uwzględniający ponadjednostkowe potrzeby społeczne zapewnić to, co w bezpieczeństwie informacyjnym najważniejsze, czyli: dostęp do wysokiej jakości informacji, odpowiednią do potrzeb jej ilość, swobodny przepływ informacji, ochronę poufności (tajności) tych informacji, które muszą być taką ochroną objęte a także skuteczne zapobieganie i przeciwdziałanie zagrożeniom bezpieczeństwa informacyjnego oraz usuwanie (niwelowanie) barier informacyjnych. Aby jednak nie absolutyzować roli państwa, trzeba dodać (zgodnie z treścią przyjętej definicji), że w ramach polityki bezpieczeństwa informacyjnego uwzględnia się również aktywność podmiotów pozapaństwowych.

4.4. Polityka bezpieczeństwa informacji

Podejmując problematykę istoty polityki bezpieczeństwa informacji, należy po raz kolejny podkreślić, że współcześnie dobrej jakości informacja determinuje warunki funkcjonowania tak podmiotów indywidualnych, jak i zbiorowych oraz stanowi jeden z ich najistotniejszych (w wielu przypadkach strategicznych) zasobów. Wszyscy zatem jej posiadacze i dysponenci muszą dbać o to, aby posiadała ona pożądane przez nich cechy oraz była odpowiednio do możliwych (realnych i potencjalnych) zagrożeń oraz wymogów prawnych i zwyczajowych chroniona. W przypadku ochrony bardzo istotne jest to, aby nie ograniczała ona w nadmierny i nieuzasadniony sposób dostępu do informacji, a co za tym idzie – swobody w jej wykorzystaniu. Chodzi szczególnie o to, aby za parawanem poufności czy tajności nie ukrywano nie tylko informacji potrzebnych np. do właściwego załatwiania spraw urzędowych czy rozwiązywania problemów w relacjach z administracją publiczną, ale również tych dotyczących nadużyć, przestępstw oraz takich, które opisują rzeczywisty negatywny obraz otoczenia, np. informacji o złym stanie środowiska naturalnego, słabych wynikach gospodarczych czy narastających zagrożeniach społecznych. Aby móc to osiągnąć, należy w odpowiedni sposób przygotować

zasoby informacyjne, a następnie należycie z nich korzystać. Trzeba więc we właściwy sposób ustanowić i realizować nie tylko politykę bezpieczeństwa informacyjnego, ale także opartą na jej założeniach politykę bezpieczeństwa informacji.

Przechodząc do kwestii określenia w sposób odpowiedni do współczesnych realiów i potrzeb istoty polityki bezpieczeństwa informacji, należy zaznaczyć, że bardzo często zamiennie dla tego terminu używane bywa pojęcie „polityka bezpieczeństwa informacyjnego". Takie ujęcie należy ocenić jako mylne i podkreślić, że politykę bezpieczeństwa informacji trzeba traktować jako pochodną w stosunku do zakresu znaczeniowego pojęcia „polityka bezpieczeństwa informacyjnego". Dążąc do poprawnego zdefiniowania tego, czym jest polityka bezpieczeństwa informacji, należy wspomnieć, że wielu autorów posługuje się, charakteryzując tę politykę, wąską definicją (ograniczoną do kwestii bezpieczeństwa informatycznego) zawartą w normie ustalonej przez Międzynarodową Organizację Normalizacyjną (International Organization for Standardization – ISO). Jest tam ona opisywana jako wdrażanie zbioru systemowych zabezpieczeń, na który składają się polityki, procesy, procedury, struktury organizacyjne oraz funkcje oprogramowania i sprzętu[494]. W innym powtarzanym dosyć często ujęciu polityka bezpieczeństwa informacji jest przedstawiana jako zestaw praw, reguł oraz doświadczeń praktycznych regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonego systemu[495]. Z lakonicznej formuły prawnej zaczerpniętej z Krajowych Ram Interoperacyjności wynika, że polityka bezpieczeństwa informacyjnego to „zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania"[496]. Formułowane są też poglądy traktujące politykę bezpieczeństwa informacji jako zbiór reguł i procedur uwzględniający wartość posiadanych informacji, źródło agresji, poziom ochrony, wskazania służb odpowiedzialnych za ochronę informacji[497]. W podobnym duchu wypowiadają się Tomasz Lech oraz Grzegorz Podgórski, wskazując na kluczowe znaczenie polityki bezpieczeństwa informacji

[494] Zob. PN ISO/IECI17799:2007, *Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem*, Warszawa 2007, s. 9.
[495] Zob. PN-I-02000:2002, *Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia*, Warszawa 2002, s. 13.
[496] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności…
[497] Zob. P. Tyrała, *Zarządzanie kryzysowe: ryzyko, bezpieczeństwo, obronność*, Toruń 2003, s. 64.

i określając ją mianem planu lub sposobu działania przyjmowanego w celu skutecznego zapewnienia bezpieczeństwa systemów i sieci teleinformatycznych oraz ochrony danych[498].

Stosowanie tego rodzaju definicji polityki bezpieczeństwa informacji jako punktu wyjścia do poprawnej jej konceptualizacji i realizacji powoduje, że już na wstępie obarczona zostaje ona szeregiem ograniczeń, co w konsekwencji pozostawia poza jej oddziaływaniem wiele obszarów narażonych na zagrożenia. Przede wszystkim należy wskazać, że nie da się skutecznie zabiegać o bezpieczeństwo informacji, koncentrując uwagę tylko na systemach informatycznych i pomijając tak ważne elementy, jak tradycyjne nośniki i środki przekazu informacji. Ponadto z powyżej przedstawionych przykładów definiowania polityki bezpieczeństwa informacji wynika, że bazują one na negatywnym ujęciu kwestii bezpieczeństwa informacji, czyli koncentrują się na ochronie niektórych jej kategorii przed zagrożeniami, z pominięciem tak fundamentalnej sprawy, jaką jest troska o posługiwanie się informacją wysokiej jakości, posiadającą przy tym wszystkie atrybutywne cechy informacji bezpiecznej, takie jak dostępność, użyteczność, integralność, autentyczność, niezaprzeczalność, rozliczalność, a w określonych przypadkach również poufność czy tajność.

W świetle powyższych uwag uzasadnione jest przyjęcie definicji, zgodnie z którą polityka bezpieczeństwa informacji to uporządkowany w celowy sposób zestaw praw, norm i praktyk regulujących: pozyskiwanie, gromadzenie, przechowywanie, przetwarzanie, dystrybucję, ochronę oraz niszczenie informacji, zapewniający stosowny do potrzeb i warunków działania danego podmiotu poziom ilościowy oraz jakość tej informacji. Głównym celem tak pojmowanej polityki bezpieczeństwa informacji jest zapewnienie, aby informacja, którą posługuje się dany podmiot była bezpieczna w każdej fazie jej życia[499]. Polityka bezpieczeństwa informacji określa ogólne zasady zapewnienia bezpieczeństwa, zasady zarządzania ryzykiem, przygotowuje podstawy podziału kompetencji i zadań osób uczestniczących w procesach związanych z tworzeniem i wykorzystywaniem zasobów informacyjnych oraz zarządzaniem ochroną informacji. Polityka określa również warunki, jakie muszą spełniać systemy, w których są gromadzone, przetwarzane i przesyłane informacje. Polityka bezpieczeństwa informacji musi być zakotwiczona w polityce bezpieczeństwa informacyjnego, musi uwzględniać także wymogi narzucane przez

[498] Zob. T. Lech, G. Podgórski, *Bezpieczeństwo w sieci*, [w:] *Społeczeństwo informacyjne*, J. Papińska-Kacperek (red.), Warszawa 2008, s. 265.
[499] Zob. W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*…, s. 35.

systemowe rozwiązania w zakresie bezpieczeństwa informacyjnego (regulacje prawne, działalność instytucji kontrolnych i nadzorczych).

W ramach polityki bezpieczeństwa informacji przyjmuje się pakiet założeń uwzględniających przepisy prawa powszechnie obowiązującego oraz regulacje wewnętrzne danego podmiotu, jego funkcje i zadania, struktury organizacyjne, możliwości personalne, techniczne, finansowe itp. Aby stworzyć odpowiednią do potrzeb danego podmiotu politykę bezpieczeństwa informacji, należy wziąć pod uwagę również cechy i czynniki określające jego specyficzność czy nawet unikatowość.

Politykę bezpieczeństwa informacji należy konstruować w oparciu o wspomniany powyżej zestaw założeń, z uwzględnieniem kilku uniwersalnych reguł obejmujących:

– zinwentaryzowanie zasobów informacyjnych, którymi dysponuje podmiot polityki bezpieczeństwa informacji, oraz określenie, jak przedstawiają się ich parametry ilościowe i jakościowe;
– ustalenie bieżących i perspektywicznych potrzeb w obszarze informacyjnym;
– zorganizowanie systemu zarządzanie informacją obejmującego jej pozyskiwanie, gromadzenie, przetwarzanie, przechowywanie, przekazywanie i niszczenie;
– wydzielenie w ramach posiadanych zasobów informacyjnych składników mających znaczenie strategiczne, taktyczne i operacyjne;
– wyodrębnienie informacji wrażliwych (w tym informacji poufnych i tajemnic);
– wskazanie personalnej odpowiedzialności dotyczącej zarządzania informacją, w tym także zasobami obejmującymi informacje wrażliwe[500].

Polityka bezpieczeństwa informacji powinna obejmować także określony zestaw celów. Do najistotniejszych z nich, o charakterze uniwersalnym, należą:

– zapewnienie dobrej jakości informacji;
– zagwarantowanie użyteczności i dostępności informacji;
– zapewnianie poufności informacji;
– zagwarantowanie bezpiecznego oraz poprawnego i ciągłego funkcjonowania systemów służących do pozyskiwania, gromadzenia, przetwarzania, przesyłania i niszczenia informacji;

[500] Zob. *Leksykon bezpieczeństwa wewnętrznego...*, s. 414.

– ograniczenie możliwości pojawienia się zagrożeń i barier informacyjnych;
– zapewnienie sprawnej reakcji na incydenty godzące w bezpieczeństwo informacji.

Oprócz tego polityka bezpieczeństwa informacji powinna także dawać wytyczne i wskazówki dotyczące:

– rodzajów działań, jakie należy podjąć (w tym określenie form i metod tych działań), niezbędnych do wypełnienia obowiązków ciążących na wytwórcy, dysponencie (użytkowniku) informacji;
– ustanowienia zasad i wymagań organizacyjno-technicznych oraz prawnych dla zapewnienia skutecznej ochrony informacji wrażliwych;
– dokumentowania przypadków naruszenia bezpieczeństwa informacji oraz trybu działania w celu przywrócenia tego bezpieczeństwa.

Główne etapy tworzenia polityki bezpieczeństwa informacji obejmują:

– podjęcie decyzji o stworzeniu takiej polityki;
– zaprojektowanie założeń i celów strategicznych;
– opracowanie celów operacyjnych.

Polityka bezpieczeństwa informacji powinna być kształtowana i realizowana w oparciu o obowiązujące regulacje prawne oraz prawidłowo prowadzoną politykę bezpieczeństwa informacyjnego na różnych szczeblach jako polityka bezpieczeństwa informacji urzędów wchodzących w skład administracji publicznej czy organizacyjnych podmiotów pozapaństwowych[501]. Na etapie wdrażania oraz realizacji polityki bezpieczeństwa informacji powinno się uwzględnić:

– zorganizowanie monitoringu skuteczności w drodze wykonywania audytów wewnętrznych i zewnętrznych;
– tryb i sposoby aktualizacji oraz modyfikacji;

[501] Zob. np. Zarządzenie Ministra Sprawiedliwości z dnia 27 marca 2019 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości (Dziennik Urzędowy Ministra Sprawiedliwości 2019, poz. 118); Zarządzenie Ministra Inwestycji i Rozwoju z dnia 20 marca 2019 r. w sprawie Polityki Bezpieczeństwa Informacji w Ministerstwie Inwestycji i Rozwoju (Dziennik Urzędowy Ministra Inwestycji i Rozwoju 2019, poz. 7); *Polityka Bezpieczeństwa Informacji Uniwersytetu Muzycznego Fryderyka Chopina*, https://www.google.com/search? q=Polityka+Bezpiecze%C5%84stwa+Informacji+Uniwersytetu+Muzycznego+Fryderyka+ Chopina&oq=Polityka+Bezpiecze%C5%84stwa+Informacji+Uniwersytetu+Muzycznego+Fryderyka+Chopina+&aqs=chrome..69i57.2027j0j15&sourceid=chrome&ie=UTF-8 [dostęp: 18.05.2021 r.]; *Polityka bezpieczeństwa informacji – MPWiK Lubin*, https://mpwik.lubin.pl/pdf/ Polityka-bezpieczenstwa-informacji.pdf, [dostep:18.05.2021 r.].

- sposób informowania zainteresowanych o prowadzonych działaniach i wprowadzanych udoskonaleniach;
- założenie potrzebnej dokumentacji oraz zorganizowanie nadzoru nad tą dokumentacją;
- właściwy dobór osób, które będą odpowiadać za zapewnienie bezpieczeństwa określonych zasobów (zasobu) informacji;
- wdrożenie niezbędnych zabezpieczeń organizacyjnych i technicznych;
- zapoznanie pracowników (współpracowników), wykonawców i innych osób realizujących zadania z wykorzystaniem zasobów informacyjnych podmiotu z właściwymi dla nich obowiązkami wynikającymi z przyjętej polityki oraz towarzyszących jej procedur;
- zorganizowanie systemu szkoleń (podstawowych i specjalistycznych) z dziedziny bezpieczeństwa informacji dla pracowników.

Dokonując konceptualizacji oraz konstruując politykę bezpieczeństwa informacji, należy pamiętać, iż mimo narastającej dominacji systemów elektronicznych informacja nadal jest gromadzona i użytkowana w tradycyjnych formach, nie można zatem pomijać ani lekceważyć tego faktu. W związku z tym polityka bezpieczeństwa informacji powinna obejmować wszystkie osoby związane z danym podmiotem organizacyjnym (z zachowaniem, rzecz jasna, odpowiednich przyporządkowanych do ich miejsca w strukturze organizacyjnej praw i obowiązków).

Uogólniając powyższe ustalenia, trzeba podkreślić, że polityka bezpieczeństwa informacji powinna zapewnić adekwatny i proporcjonalny do potrzeb użytkowników i dysponentów dostęp do informacji oraz przestrzeganie wymogów prawa obowiązujących w stosunku do poszczególnych kategorii informacji i danych. Jednocześnie powinna być dopasowana do poziomu zagrożeń występujących w stosunku do pozyskiwanych, przetwarzanych, wykorzystywanych i przekazywanych bądź utylizowanych informacji. Założenia polityki bezpieczeństwa informacji muszą być również adekwatne do oszacowanych ryzyk związanych z jej pozyskiwaniem, przetwarzaniem, używaniem, gromadzeniem oraz niszczeniem. Jak już wskazywano, do podstawowych kwestii związanych z adekwatnym rozumieniem i realizowaniem polityki bezpieczeństwa informacji należy zapewnienie odpowiedniej jakości informacji oraz cech charakterystycznych dla informacji bezpiecznej, takich jak dostępność, użyteczność, integralność, autentyczność, niezaprzeczalność, rozliczalność, a w określonych przypadkach również poufność czy tajność.

Jeżeli chodzi o jakość informacji, to odzwierciedla ona stopień zaspokojenia potrzeb i wymagań jej użytkownika, jest więc pojęciem subiektywnym (uzależnionym od oczekiwań odbiorcy) i kategorią zależną od zmieniającego się otoczenia[502]. Podstawowym działaniem mającym zapewnić odpowiednią jakość informacji w obecnej sytuacji jej dużej podaży i względnie szerokiej dostępności jest selekcja dokonywana w oparciu o kryteria ustalane przez odbiorcę (użytkownika), który musi dodatkowo posiadać zdolności do sprawdzania tej jakości np. poprzez ekspertów. Do zapewnienia właściwej jakości informacji ważne jest również jej pochodzenie (źródło), podmiot autoryzujący czy renoma wytwórcy. Jak już wspomniano, kwestia jakości wiąże się ze zindywidualizowanym spojrzeniem zainteresowanych podmiotów, jednak nie mogą one pomijać pewnych generalnych cech jakościowych, które za K. Lidermanem można ująć w zestaw obejmujący:

– relewantność (określającą, czy informacja jest istotna dla odbiorcy i związana z tym, czego on poszukuje);
– dokładność (oznaczającą, że informacja jest precyzyjna oraz zaprezentowana w sposób przystający do poziomu wiedzy odbiorcy);
– aktualność (oznaczającą, że informacja jest modyfikowana w rytmie dopasowanym do zmian opisywanych obiektów);
– kompletność (oznaczającą, że informacja jest dostępna w ilości i stopniu uszczegółowienia zgodnym z wymaganiami odbiorcy);
– spójność (wskazującą, że poszczególne fragmenty informacji są niesprzeczne, odnoszą się do danej tematyki oraz są przekazywane w jednolitej formie);
– odpowiedniość formy (oznaczającą przedstawienie informacji w sposób minimalizujący błędy interpretacyjne);
– wiarygodność[503] (oznaczającą, że informacja zawiera elementy dające pewność rzetelności niesionego przez nią przekazu)[504].

Dodać należy, że hierarchia ważności poszczególnych cech jakościowych informacji kształtowana jest w zależności od dziedziny, w której użytkownik (odbiorca) planuje informację wykorzystać.

[502] Zob. A. Lasota-Jądrzak, *Jak mierzyć jakość informacji?*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej" 2016, nr 4, s. 179.
[503] Informacja wiarygodna to informacja wzbudzająca zaufanie i postrzegana jako zgodna z prawdą. Nieprawdziwa informacja też może zostać przekazana w sposób wiarygodny, trzeba zatem pamiętać, że nie każda wiarygodna informacja jest prawdziwa.
[504] Zob. K. Liderman, dz. cyt., s. 18.

Zapewnienie dostępności wiąże się przede wszystkim z utworzeniem i sprawnym działaniem powszechnie dostępnych i wysokowydajnych systemów wytwarzania i dystrybucji informacji, na które składają się:

– rozwiązania techniczne zapewniające cyfrowe udostępnienie informacji sektora publicznego ze źródeł administracyjnych i zasobów nauki;
– komercyjne i niekomercyjne media radioelektroniczne oraz prasa;
– pisma naukowe, publikacje książkowe i ich zbiory biblioteczne;
– system publikacji aktów prawnych oraz innych aktów urzędowych;
– sieci łączności telefonicznej;
– system edukacyjny;
– ośrodki naukowo-badawcze;
– specjalistyczne ośrodki informacyjne oraz repozytoria;
– Internet z wolnym do niego dostępem.

Dostępność zapewnia także niewygórowany poziom kosztów związanych z korzystaniem z poszczególnych kanałów dystrybucji informacji (np. ceny gazet, książek, opłaty za łącza internetowe czy wysokość abonamentów radiowo-telewizyjnych). Dla zapewnienia dostępności konieczny jest również odpowiedni system edukacyjny, pozwalający na uzyskiwanie kompetencji do wykorzystywania źródeł i systemów dostarczania informacji oraz poprawny dobór oraz odbiór informacji.

Zapewnienie użyteczności informacji wiąże się przede wszystkim z prawidłowym określeniem potrzeb informacyjnych podmiotu. Następnie zaś trzeba zająć się pozyskiwaniem potrzebnych informacji, które będą zrozumiałe, wiarygodne i kompletne. Istotnym warunkiem zapewnienia użyteczności jest także dysponowanie odpowiednim zasobem kadr i sprzętu pozwalającym w pełni wykorzystywać posiadane przez dany podmiot informacje.

Integralność informacji, czyli właściwość polegającą na tym, że informacja nie została zmodyfikowana w sposób nieuprawniony, można zapewnić poprzez:

– kontrole dostępu w trakcie jej wytwarzania i przekazywania;
– odpowiednie zabezpieczenie kanałów przekazu i dystrybucji informacji zapewniające blokadę dostępu dla osób postronnych.

Autentyczność, czyli właściwość polegającą na tym, że pochodzenie lub zawartość informacji opisujących obiekt są takie, jak deklarowane, może być zapewniana poprzez:

– uwierzytelnienie źródła informacji;
– sprawdzenie autorstwa i treści informacji.

Niezaprzeczalność, rozumiana jako brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany informacji przez jeden z podmiotów uczestniczących w tej wymianie[505], jest zapewniana m.in. przez zgromadzenie odpowiedniej ilości materiału dowodowego dokumentującego dokonanie operacji wymiany informacji, co ogranicza możliwość nieuzasadnionego wyparcia się jej przez strony. Niezaprzeczalność sprawia, że bardzo trudno jest skutecznie zaprzeczyć, skąd pochodzi informacja, a także autentyczności tej informacji.

Rozliczalność, czyli właściwość pozwalającą przypisać określone działanie w stosunku do danej informacji osobie fizycznej oraz umiejscowić ją w czasie, zapewnia się przede wszystkim dzięki stosowaniu:

– systemów służących do określania listy użytkowników danych zasobów informacyjnych i ich upoważnień do czynności wykonywanych przy użyciu tych informacji;
– systemów zarządzania tożsamością służących do identyfikacji użytkowników informacji;
– systemów autoryzujących służących do przeprowadzenia procesu identyfikacji upoważnień danego użytkownika informacji.

Zagwarantowanie poufności dokonuje się na drodze sklasyfikowania określonych informacji jako poufnych, a następnie ich ochrony przed nieautoryzowanym wykorzystaniem czy ujawnieniem podmiotom niemającym prawa dostępu. W celu zapewnienia skutecznej ochrony informacji poufnych tworzy się listy osób upoważnionych do pracy z takimi informacjami. Osoby te muszą być odpowiednio przeszkolone w zakresie postępowania z informacjami poufnymi i przestrzegać odpowiednich zasad wynikających z polityki bezpieczeństwa informacji. Istotnym elementem zapewnienia poufności jest stworzenie rozwiązań pozwalających na dostęp do informacji poufnych tylko w sposób autoryzowany oraz minimalizowanie prawdopodobieństwa wydostania się tych informacji poza mechanizm kontroli dostępu do nich. Stąd stosowane uwierzytelnianie użytkowników, autoryzacja i kontrola dostępu oraz odpowiednie zabezpieczenia techniczne i infrastrukturalne związane z przechowywaniem oraz udostępnianiem informacji poufnych, które nie pozwalają skorzystać z nich osobom nieupoważnionym.

[505] Zob. Rozporządzenie Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz.U. 2019, poz. 1969).

W odniesieniu do zapewnienia tajności znajdują zastosowanie podstawowe wymagania w zakresie ochrony informacji poufnych. Ponadto wdraża się także inne, bardziej rygorystyczne przedsięwzięcia związane z faktem nadania informacji klauzuli tajności, obejmujące:

– przechowywanie i przetwarzanie w warunkach uniemożliwiających ich nieuprawnione ujawnienie;
– udostępnianie wyłącznie osobom uprawnionym do dostępu do tego typu informacji przy zachowaniu zasady wiedzy niezbędnej (ang. *need-to-know*);
– dopuszczenie do prac związanych z dostępem do informacji tajnych osób odpowiednio przeszkolonych w zakresie ochrony tajemnic;
– certyfikacja personelu pracującego z wykorzystaniem informacji tajnych pod kątem tego, czy dają pewność zachowania powierzonych im tajemnic.

W celu właściwej ochrony informacji tajnych wyznacza się również strefy bezpieczeństwa, w których są one wytwarzane, przetwarzane i przechowywane. Jednostki organizacyjne danego podmiotu, w których są gromadzone i wykorzystywane informacje tajne, muszą stosować odpowiednie środki bezpieczeństwa fizycznego, np. systemy zabezpieczające przed podsłuchem czy poglądem, odpowiedniej klasy zamki, drzwi i okna do pomieszczeń, w których przechowuje się i przetwarza informacje tajne, bezpieczne stanowiska komputerowe, sejfy na dokumenty i inne nośniki informacji. Odpowiednio powinny być także chronione klucze i kody szyfrowe dające dostęp do pomieszczeń, w których pracuje się z informacjami tajnymi[506]. Stosuje się również klasyczne formy ochrony, takie jak nadzór personelu ochronnego (służb ochrony) i systemy kontroli dostępu. Jednym z powszechnie praktykowanych rozwiązań w dziedzinie zapewnienia odpowiedniego poziomu ochrony informacji określonych jako tajne jest tworzenie specjalnych komórek organizacyjnych – kancelarii tajnych.

Reasumując, należy podkreślić, że polityka bezpieczeństwa informacji musi odnosić się do właściwie zdefiniowanego bezpieczeństwa informacji oraz być konceptualizowana i realizowana w ścisłym powiązaniu z polityką bezpieczeństwa informacyjnego. Polityka bezpieczeństwa informacji oddziaływać powinna na każdą fazę życia informacji i zawierać rozwiązania pozwalające

[506] Zob. W. Drogoń, D. Mąka, M. Skawina, *Jak chronić tajemnice? Ochrona informacji w instytucjach państwowych i przedsiębiorstwach prywatnych*, Warszawa 2004, s. 90–92.

czuwać nad każdym etapem jej wykorzystywania pod kątem zagwarantowania jej bezpieczeństwa. Jednym z podstawowych źródeł kreowania polityki bezpieczeństwa informacji jest, na co już wcześniej wskazywano, szacowanie ryzyka. Dzięki identyfikacji zagrożeń i wyzwań oraz ujawnianiu barier można określić właściwy (pożądany) pułap wymagań umożliwiający osiąganie i zachowanie optymalnego w danych warunkach poziomu bezpieczeństwa informacji. W tak nakreślonym kontekście należy dodać, że polityka bezpieczeństwa informacji musi uwzględniać także sposoby reagowania na zagrożenia. Kolejny ważny element polityki bezpieczeństwa informacji wiąże się z odpowiednim postępowaniem z czynnikiem ludzkim. Ludzie, niezależnie od postępującej technicyzacji, zwłaszcza zaś informatyzacji, nadal są najważniejsi w polityce bezpieczeństwa informacji. Dotyczy to nie tylko tych obsługujących systemy przetwarzające informacje, ale także tworzących informacje, analizujących informacje czy formułujących zapotrzebowania informacyjne. Są oni twórcami kształtującymi bezpieczną informację w tych fazach jej istnienia, z którymi mają do czynienia, a jednocześnie ogniwem zabezpieczeń przed zagrożeniami, na których skuteczność wpływa ich przygotowanie w zakresie dotyczącym bezpiecznego posługiwania się aktywami informacyjnymi. Obejmuje ono zapewnienie odpowiedniej wiedzy w zakresie pojawiających się zagrożeń oraz metod ochrony. Zaznaczyć należy, że polityka bezpieczeństwa informacji musi być systematycznie aktualizowana w oparciu m.in. o analizy ryzyka i audyty uwzględniające nie tylko funkcjonowanie systemu bezpieczeństwa informacji oraz systemu zarządzania informacją danego pomiotu, ale także zmiany zachodzące w ich otoczeniu.

Zakończenie

Bezpieczeństwo informacyjne należy do tych wymiarów bezpieczeństwa, które są szczególnie ważne dla współczesnych społeczeństw. Jego podstawę stanowią takie elementy, jak dysponowanie wysokiej jakości informacją, wolność w zakresie dostępu i obrotu informacją, sprawny i bezpieczny transfer informacji pomiędzy zainteresowanymi podmiotami (m.in. poprzez ogólnodostępne wysokowydajne kanały komunikacji), adekwatna do potrzeb ochrona i reglamentacja informacji istotnych z punktu widzenia bezpieczeństwa jednostek oraz zbiorowości społecznych, w tym także państw. Fakt funkcjonowania społeczeństwa informacyjnego oraz przechodzenie tej formacji społeczno-gospodarczej w nową fazę rozwoju związaną z ekspansją rozwiązań opartych na sztucznej inteligencji powoduje nie tylko zwiększanie rangi bezpieczeństwa informacyjnego, ale przekłada się również na konieczność intensyfikacji wysiłków na rzecz jego zapewnienia. Generalnie, na podstawie zgromadzonej wiedzy naukowej oraz istniejącej praktyki, można zauważyć bezpośredni wysoki stopień zależności pomiędzy posiadanymi przez podmioty bezpieczeństwa informacjami wraz z technologiami służącymi do ich gromadzenia, selekcji, przetwarzania i wykorzystywania a poziomem bezpieczeństwa tych podmiotów. Syntetycznie ujmując tę zależność, można powiedzieć, że im większa jest ilość dobrej jakości (bezpiecznej) informacji w posiadaniu podmiotów bezpieczeństwa, tym o lepszy poziom tego bezpieczeństwa (w tym także informacyjnego) mogą one skutecznie zabiegać.

Powyżej zarysowane uwarunkowania stworzyły sytuację, z której wynika niezbędność podejmowania szeregu mających ciągły charakter działań praktycznych oraz prac naukowych ukierunkowanych na usprawnianie i zwiększanie skuteczności budowania bezpieczeństwa informacyjnego, a także zarządzania tym bezpieczeństwem. Badania mające na celu rozpoznawanie, wyjaśnianie oraz systematyzowanie istniejących w infosferze problemów, a także projektowanie nowych rozwiązań odnoszących się do różnorodnych (technicznych, społecznych, politycznych ekonomicznych, militarnych

i innych) aspektów bezpieczeństwa informacyjnego należy traktować jako przedsięwzięcia o fundamentalnym znaczeniu. Szczególne miejsce w takich badaniach siłą rzeczy zająć muszą kwestie związane z właściwym określaniem istoty fundamentalnych pojęć oraz towarzyszącej im terminologii. W tym nurcie badań ważnym zadaniem dla uczonych jest nie tylko tworzenie nowego, stosownego do istniejących nowatorskich rozwiązań praktycznych aparatu pojęciowego, lecz także krytyczna analiza zgromadzonego dorobku naukowego w celu jego aktualizacji oraz poprawy adekwatności używanych terminów, klasyfikacji i charakterystyk. W rezultacie wysiłku poznawczego, w ramach którego podjęto próbę rozwiązania głównego problemu badawczego dotyczącego tego, jak współcześnie powinno się rozumieć istotę bezpieczeństwa informacyjnego i jakie zasadnicze składniki decydują o jego kształcie, ustalono, że pojęcie to należy rozumieć szeroko, koncentrując się na nieskrępowanym dostępie i swobodzie obrotu informacją, zapewnieniu jej wysokiej jakości oraz racjonalnym, opartym na czytelnych kryteriach chronieniu niektórych informacji ważnych dla bezpieczeństwa podmiotów, których one dotyczą.

Nawiązując do szczegółowych problemów badawczych, w świetle uzyskanych wyników badań należy stwierdzić:

W odniesieniu do pojmowania, klasyfikowania informacji oraz jej cech i pełnionych funkcji prawdą jest, że nie sposób przyjąć jednej mającej uniwersalny charakter definicji terminu „informacja". Można także stwierdzić, że informacje stanowią podstawę budowania wiedzy i określania sposobów jej wykorzystywania. Kształtują one sposób postrzegania i interpretacji zjawisk zachodzących w środowisku otaczającym człowieka oraz w nim samym. Jednocześnie umożliwiają adaptowanie się do zmiennej rzeczywistości oraz pozwalają na jej przekształcanie w celu sprawnego funkcjonowania. Dzięki informacjom możemy uzmysławiać sobie istniejące problemy i szukać ich rozwiązania.

Uznać należy także, iż informacja posiada szereg specyficznych cech i pełnić może różnorodne funkcje, które czynią ją instrumentem niezbędnym w większości procesów, pozwalającym stosownie do zamierzeń użytkowników (dysponentów) kreować odpowiednie decyzje oraz skutecznie działać na rzecz dobra wspólnego i rozwoju. Pogłębianie wiedzy w zakresie rozpoznania cech i funkcji informacji służy także udoskonalaniu sposobów jej pozyskiwania, przetwarzania i wykorzystywania, co daje również niezaprzeczalnie korzystne efekty praktyczne. W powyższym kontekście należy zaznaczyć, że informacja stanowi bardzo ważny składnik bezpieczeństwa w szerokim tego

słowa znaczeniu. Nie da się bowiem skutecznie zabiegać o wysoki poziom żadnego ze znanych wymiarów bezpieczeństwa (politycznego, ekonomicznego, ekologicznego, militarnego, społecznego, kulturowego, międzynarodowego, państwowego, jednostkowego i wielu innych) bez uwzględnienia roli odgrywanej przez informację. Tego rodzaju oceny dodatkowo wzmacniają wyniki analiz związanych z rolą informacji jako zasobu. W ich rezultacie dodać należy, że zasoby informacyjne mają charakter odnawialny i są traktowane nie tylko jako wysoce użyteczne, ale także (w coraz szerszym zakresie) jako zasoby strategiczne. W związku ze swoim znaczeniem i wartością wymagają ponoszenia kosztów na pozyskiwanie, utrzymywanie oraz eksploatację. Zasoby te mogą być używane do osiągania różnorodnych i skomplikowanych celów pod warunkiem odpowiedniego ich kształtowania oraz zarządzania nimi. Do ciągłego zwiększania roli zasobów informacyjnych przyczyniają się także procesy związane z rosnącymi mocami obliczeniowymi komputerów, dynamicznym rozwojem robotyki i sztucznej inteligencji, upowszechnianiem programów komputerowych sterujących zarządzaniem w różnych sferach życia publicznego, takich jak np. administracja, edukacja, ochrona zdrowia czy komunikacja i transport.

W odniesieniu do społeczeństwa informacyjnego jako formacji społeczno-gospodarczej, w ramach której obecnie żyjemy i funkcjonujemy, uzyskano potwierdzenie, że z racji posiadanych cech i ukształtowanych funkcji formacja ta nie tylko w znaczący sposób wpłynęła na tempo rozwoju cywilizacyjnego, ale nadal generuje dużą liczbę różnorodnych możliwości rozwojowych. Towarzyszą temu jednak różne szkodliwe i niebezpieczne formy nadużywania i niekontrolowanych oddziaływań potęgi informacyjnej tej formacji. Społeczeństwo informacyjne to twór o dużym stopniu złożoności, który oprócz informacji tworzą również inne składniki – techniczne, cywilizacyjne, kulturowe czy światopoglądowe, w związku z tym musi być ono badane w sposób interdyscyplinarny. Dość powszechna opinia, że dzięki technologiom informacyjnym wytwarzanie informacji, budowanie na jej bazie wiedzy, przetwarzanie, magazynowanie i szerokie udostępnianie oraz przyswajanie tej wiedzy stwarza optymalne warunki dla rozwoju poznawczego człowieka i w efekcie postępu cywilizacyjnego, budzi sporo zastrzeżeń i wymaga pogłębionej, krytycznej oceny. W świetle dokonanych w monografii analiz nie sposób bowiem traktować społeczeństwa informacyjnego w kategoriach deterministycznych jako nowego, wspaniałego świata. Społeczeństwo to powinniśmy analizować przy użyciu trzech perspektyw: optymistycznej, pesymistycznej i zrównoważonej. W pierwszej perspektywie pojawia się obraz społeczeństwa szybko

uwalniającego się od przymusu pracy, posiadającego dużą ilość wolnego czasu (który można spożytkować np. na samorealizację), dysponującego coraz lepszą siecią komunikacji korzystnie wpływającą na społeczną homeostazę. Perspektywa druga ukazuje społeczeństwo zdezintegrowane i zindywidualizowane, poddawane różnym formom (jawnej i niejawnej) kontroli oraz rozległemu nadzorowi przy zastosowaniu nowoczesnych technologii informacyjnych.

W trzeciej perspektywie obserwuje się społeczeństwo ze zmieniającą się strukturą zatrudnienia, nasycane coraz bardziej zawansowanymi technologiami we wszystkich sferach życia, kształtujące swe struktury ewolucyjnie, zwalczające wady i niedoskonałości, zachowujące równościowe, demokratyczne i wolnościowe zasady oraz humanistyczną aksjologię. Chociaż nie można dokładnie i pewnie przewidywać dalszych losów społeczeństwa informacyjnego, to można stwierdzić, że będzie ono trwało i rozwijało się. Ocena taka wynika z faktu, że na obecnym etapie informatyzacji i cyfryzacji większość instytucji, organizacji, społeczeństw oraz państw nie może już funkcjonować poza mechanizmami tego społeczeństwa**.** Jednak eksponowane przez niektórych oceny, iż społeczeństwo informacyjne oraz kolejna formacja społeczno-gospodarcza oparta na sztucznej inteligencji rozwiążą większość problemów, z jakimi się borykamy obecnie, jest zbyt optymistyczna. Co więcej, w niesprzyjających okolicznościach, w przypadku dezintegracji rozrastających się systemów informatyczno-informacyjnych, na których opiera się współczesny świat, może dojść do głębokiego kryzysu**.** Źródłem szeregu nowych problemów może stać się również zaburzenie równowagi między zdobyczami technik informacyjnych a aksjologicznymi i emocjonalnymi fundamentami życia ludzkiego gatunku. Dlatego też należy działać tak, aby nadchodząca era sztucznej inteligencji w przyszłości nie okazała się tworem nieludzkim.

W kontekście zakresu postrzegania i adekwatnego definiowania głównych rodzajów zagrożeń i barier informacyjnych potwierdzono, że stan współczesnej cywilizacji, w którym narzędzia i technologie informacyjne dostarczają coraz więcej informacji, radykalnie zmienił położenie globalnej społeczności. Jednak mimo coraz lepszego przygotowania ludzi do użytkowania skomputeryzowanych systemów informacyjnych, korzystania z usług opartych na nowoczesnych systemach komunikowania się, nie jesteśmy w stanie unikać szeregu zagrożeń i konsekwencji istnienia barier informacyjnych. Są w tej liczbie bariery i zagrożenia związane z zawodnością i niedoskonałością techniki oraz błędami i deficytem umiejętności ludzi, ale nie mniej liczne są te generowane na drodze intencjonalnego wykorzystywania możliwości społeczeństwa

informacyjnego w celu osiągania celów zaprogramowanych w ramach działań przestępczych, manipulacyjnych, dezinformacyjnych czy związanych z prowadzeniem walk informacyjnych. Przegląd i analiza różnorodnych klasyfikacji kategorii zagrożeń dla bezpieczeństwa informacyjnego pozwala przyjąć, że podstawowymi ich rodzajami są: deficyt informacji, nadmiar (niekontrolowany napływ ilościowy) informacji, bezprawne ujawnianie informacji chronionych, naruszanie praw obywatelskich w sferze informacyjnej, manipulowanie przekazem informacji, dezinformacja, przestępstwa informacyjne, różne formy walk informacyjnych oraz perspektywa wojen informacyjnych. Katalogowi zagrożeń towarzyszy niemały zbiór barier informacyjnych, czyli przeszkód, które zakłócają procesy przepływu informacji. Mogą one oddziaływać na użytkowników informacji niezależnie od ich świadomości lub poprzez tę świadomość. Wspomniane bariery powodują, że informacje nie są wykorzystywane, dlatego że użytkownik nie wie o ich istnieniu, nie korzysta ze znanych źródeł informacji lub ma utrudniony dostęp do tych źródeł z różnych przyczyn. Do najbardziej znaczących barier w ujęciu ogólnym należą te związane z:

– przeszkodami występującymi ze strony podmiotów współpracujących z poszukującymi informacji;
– ograniczeniami w sferze umiejętności użytkowników informacji;
– procesami i stanami psychicznymi użytkowników informacji.

Wspomniane bariery informacyjne funkcjonują w życiu społecznym w sposób o wiele mniej spektakularny niż zagrożenia informacyjne, ale także znacząco przeszkadzają w dokonywaniu właściwych wyborów, podejmowaniu racjonalnych decyzji, sprawnym rozwiązywaniu problemów czy skutecznym realizowaniu procesów edukacyjnych. Ograniczają one również możliwości weryfikowania informacji, sprzyjają wykluczeniu informacyjnemu oraz rodzą trudności adaptacyjne w stosunku do wymagań ery informacyjnej. W rezultacie przeprowadzonych analiz i dokonanych na ich bazie uogólnień można przyjąć istnienie dwóch zasadniczych grup zagrożeń dla bezpieczeństwa informacyjnego: o charakterze antropogenicznym oraz środowiskowo-technicznym. W pierwszej grupie wskazać trzeba przede wszystkim na: wytwarzanie i rozpowszechnianie informacji niskiej jakości, błędy i braki w percepcji i dystrybucji dobrej jakościowo i ważnej informacji, fałszowanie informacji i jej kradzież, niszczenie informacji, manipulowanie informacją, ukrywanie informacji, utratę informacji, wykorzystywanie informacji nieaktualnej. W grupie zagrożeń środowiskowo-technicznych dominują: strata lub uszczuplenie informacji jako efekt destrukcyjnych działań sił przyrody (powodzie, trzęsienia ziemi,

huragany itp.), utrata lub fragmentaryzacja informacji w wyniku awarii sprzętu komputerowego, generowanie informacji złej jakości w wyniku błędów w oprogramowaniu.

W konsekwencji zaistnienia zagrożeń dla bezpieczeństwa informacyjnego i bezpieczeństwa informacji oraz barier powstających na gruncie różnie skonfigurowanych sytuacji, zdarzeń i działań podmioty korzystające, wytwarzające czy przetwarzające informację mogą mieć do czynienia z informacją niepełną, niewiarygodną (niepewną), zmanipulowaną, sfałszowaną, nieczytelną czy pozyskaną nielegalnie. Zagrożenia i bariery informacyjne mają różny zasięg i często mimo podobnych przejawów generują różne skutki – zależy to przede wszystkim od istniejących rozwiązań realizowanych przez konkretne podmioty w ramach ich polityk bezpieczeństwa informacyjnego. Żeby wspomniane zagrożenia i bariery efektywnie rozpoznawać, przeciwdziałać im oraz minimalizować ograniczenia i straty związane z ich występowaniem, niezbędne są nie tylko zaawansowane działania oparte na rozwiązaniach technicznych i organizacyjnych, ale w coraz większym stopniu te ukierunkowane na budowanie odpowiedniego poziomu świadomości wytwórców i użytkowników informacji. Należy w tym kontekście zwrócić uwagę, że każdy wynalazek, innowacja czy etap rozwojowy posiada swoją drugą stronę – ograniczenia technologiczne, bariery rozwoju, elementy regresu, które to elementy nie zawsze są szybko i łatwo dostrzegalne. Nie powinno się zatem dopuścić do tego, aby na pożywce niewątpliwego postępu technologiczno-informatycznego wytworzył się specyficzny, nadmiernie afirmatywny (a przez to zwodniczy) stosunek do możliwości i osiągnięć związanych erą informacyjną. Taka postawa może skutecznie ograniczać, a w skrajnych przypadkach nawet uniemożliwiać rozpoznawanie istoty zagrożeń i barier informacyjnych i tym samym utrudniać radzenie sobie z jej skutkami. Trzeba pamiętać, że żadne z istniejących list zagrożeń bezpieczeństwa informacyjnego oraz bezpieczeństwa informacji czy barier informacyjnych, w tym również przedstawione w monografii, nie mogą być listami zamkniętymi, ponieważ wraz ze zmianami w środowisku informacyjnym przeobrażeniom ulega także związany z nim obszar zagrożeń i barier. Dlatego ważnym zadaniem każdego dbającego o swoje bezpieczeństwo podmiotu jest ciągłe monitorowanie i diagnozowanie zagrożeń i barier związanych z jego środowiskiem informacyjnym tak wewnętrznym, jak i zewnętrznym. Jest to szczególnie ważne w społeczeństwie bazującym na danych i informacjach, które tworzą podstawy jego rozwoju i sukcesów, ale mogą także zostać wykorzystane w celu zachwiania jego bezpieczeństwem.

Jest to szczególne istotne w sytuacji, gdy powstają ciągle nowe (często posiadające unikatowe możliwości) rozwiązania programistyczne oraz narzędzia informatyczne, szybko wchodzące do szerokiego, a w wielu przypadkach do masowego użytku. Szybka identyfikacja potencjalnych zagrożeń pozwoli na modyfikację oraz ulepszenie istniejących rozwiązań tak, aby skuteczniej eliminować bądź zmniejszać prawdopodobieństwo wystąpienia któregoś z nich, a tym samym tworzyć właściwe podstawy do osiągania odpowiedniego bezpieczeństwa informacji i bezpieczeństwa informacyjnego.

W ramach rozwiązania problemu badawczego dotyczącego tego, jak powinno być postrzegane i rozumiane bezpieczeństwo informacyjne, bezpieczeństwo informacji oraz polityki ich dotyczące, ustalono, że w dotychczasowym dorobku dominuje nieprecyzyjne i zawężone podejście do ujmowania istoty bezpieczeństwa informacyjnego związane m.in. z pomijaniem aspektów swobody dostępu i obrotu informacją, ograniczaniem istoty tego pojęcia do ochrony informacji tajnych i poufnych czy umieszczaniem poza sferą bezpieczeństwa informacyjnego jako zupełnie odrębnej kategorii cyberbezpieczeństwa. Towarzyszy temu brak głębszej refleksji na gruncie naukowym dotyczącej tego, czym jest bezpieczeństwo informacji, i traktowanie go w wielu przypadkach jako pojęcia tożsamego z pojęciem bezpieczeństwa informacyjnego. W odniesieniu do problematyki polityki bezpieczeństwa informacyjnego oraz polityki bezpieczeństwa informacji, po przeprowadzeniu analizy poglądów na kwestię dotychczasowego pojmowania tych pojęć, ustalono szereg istotnych luk oraz istnienie bardzo ograniczonego dorobku w zakresie ich definiowania. Stwierdzono także deficyt reguł służących do konceptualizacji i realizacji wspomnianych polityk. W konsekwencji rodzi to ocenę, że aktualnie stosowany aparat pojęciowy odnoszący się do sfery pojmowania bezpieczeństwa informacyjnego i bezpieczeństwa informacji ze względu na ograniczoną adekwatność nie pozwala na w pełni skuteczne działania na rzecz zapewnienia tego bezpieczeństwa i wymaga redefinicji.

Jeżeli chodzi o postawione w monografii hipotezy, to w wyniku przeprowadzonych w ramach procesu badawczego czynności weryfikacyjnych w odniesieniu do hipotezy głównej potwierdzono, że bezpieczeństwo informacyjne stanowi integralny, ciągle zyskujący na znaczeniu składnik bezpieczeństwa państw, grup społecznych oraz jednostek i w celu programowania i podejmowania skutecznych działań na rzecz jego zapewnienia musi być ono adekwatnie definiowane i właściwie rozumiane.

Ponadto w odniesieniu do hipotez szczegółowych:

Potwierdzono, że pojmowanie, kategoryzacja oraz przypisywanie informacji określonych ról i funkcji w decydującym zakresie jest uzależnione od dziedzin aktywności ludzkiej, w której jest ona wykorzystywana. Właściwemu korzystaniu z informacji sprzyja system klasyfikacji, który jest narzędziem zapewniającym efektywne używanie poszczególnych rodzajów informacji w obrębie różnorodnych sfer aktywności podmiotów indywidualnych i zbiorowych. System klasyfikacji informacji pozwala również na właściwe nią zarządzanie i przypisywanie do określonych kategorii zasobów informacyjnych. Nie oznacza to jednak, że jest on w pełni przejrzysty, funkcjonalny i spójny. Istnieje zatem potrzeba jego doskonalenia, zwłaszcza w zakresie radzenia sobie z nadmiarem informacji oraz ilością informacji w sposób nieuprawniony uznawanej za poufną, a nawet tajną czy w inny sposób wyłączaną z dostępu w trybie prawa do informacji publicznej. Badania potwierdziły również, że zasoby informacyjne w bardzo wielu przypadkach są zaliczane do kategorii zasobów strategicznych.

Potwierdzono, że powstanie i rozwój społeczeństwa informacyjnego wywarły istotny wpływ na ewolucję postrzegania bezpieczeństwa informacyjnego oraz jego uwarunkowania. Bardzo istotne jest w tym aspekcie ciągłe doskonalenie sprawnego i efektywnego wykorzystywania wszechobecnej informacji tak, aby maksymalizować pozytywne efekty w ramach realizacji różnorodnych funkcji społeczeństwa informacyjnego. Należy jednak zwrócić uwagę, że obok szeregu pozytywnych aspektów ta formacja społeczno-gospodarcza stworzyła także wiele problemów, co zmusza do sformułowania oceny, że społeczeństwo informacyjne, mimo wielu zalet, nie stanowi jednak panaceum na wszystkie problemy społeczne czy gospodarcze. Mechanizmy funkcjonowania tego społeczeństwa posiadają także szereg słabych stron, które powodują, że walory życia w ramach tej formacji społeczno-gospodarczej są w sposób istotny ograniczane przez powstające na ich gruncie zagrożenia i bariery dotykające znacznych grup społecznych. Wymaga to nie tylko ustanowienia nowych form ochrony i podejmowania działań na rzecz ich usuwania ze strony decydentów państwowych, ale jest także ważną wskazówką dla badaczy, podpowiadającą konieczność intensyfikacji badań dotyczących negatywnych konsekwencji istnienia społeczeństwa informacyjnego, w tym także badań takich samych konsekwencji w odniesienia do kolejnego jego etapu rozwojowego, czyli sztucznej inteligencji.

Potwierdzono, że istniejący (szeroki) katalog zagrożeń i barier informacyjnych oraz ich zmienna natura rodzi potrzebę ciągłego rozpoznawania, tworzenia nowych systematyzacji oraz precyzowania istniejących i wprowadzania nowych pojęć związanych z tym obszarem. Jest to istotne i mające podstawowy charakter działanie umożliwiające kroki diagnostyczne, a następnie podejmowanie racjonalnych i skutecznych działań zmniejszających ilość zagrożeń, niwelujących ich wpływ oraz sprzyjających likwidowaniu barier informacyjnych. Skala i zasięg zagrożeń i barier informacyjnych wskazuje, że działania na rzecz ich ograniczania i likwidacji nie powinny odnosić się jedynie do bieżącego reagowania oraz monitorowania i sporządzania dokumentów analitycznych. Niezbędne jest także planowanie i sprawne wdrażanie konkretnych rozwiązań w sposób ciągły podnoszących standardy bezpieczeństwa informacyjnego i bezpieczeństwa informacji.

Potwierdzono, że aktualnie stosowany aparat pojęciowy odnoszący się do kwestii pojmowania bezpieczeństwa informacyjnego i bezpieczeństwa informacji ze względu na ograniczoną adekwatność nie pozwala na w pełni skuteczne działania na rzecz zapewnienia tego bezpieczeństwa i wymaga redefinicji. Wspomniany stan rzeczy wynika z przyczyn leżących zarówno po stronie uczonych, jak i instytucji państwowych należących do różnych sfer władzy (ustawodawczej, wykonawczej, sądowniczej), które nie przykładają należytej wagi do zagadnień związanych z bezpieczeństwem informacyjnym czy bezpieczeństwem informacji, co generuje negatywne skutki dla państwa i obywateli oraz ogranicza możliwości działania w zakresie skutecznej walki z zagrożeniami informacyjnymi i usuwania barier informacyjnych.

Generalne wnioski przedstawiają się następująco:

- problematyka bezpieczeństwa informacyjnego w kontekście analiz dotyczących jego istoty stanowi temat coraz częściej podejmowany, ale zazwyczaj w ujęciu raczej hasłowym;
- w zakresie analiz sfery bezpieczeństwa informacyjnego dominują rozważania odnoszące się do konkretnych problemów szczegółowych;
- istota bezpieczeństwa informacyjnego jest deformowana poprzez absolutyzowanie i nadawanie charakteru odrębnego bytu cyberbezpieczeństwu;
- w prowadzonych analizach widoczny jest deficyt głębszego skupienia się na kwestiach teoretycznych dotyczących istoty bezpieczeństwa informacyjnego oraz brakuje prac o systemie bezpieczeństwa informacyjnego;

– panuje swoista inercja definicyjna w odniesieniu do ważnych pojęć związanych z bezpieczeństwem informacyjnym, takich jak walka informacyjna, wojna informacyjna, polityka bezpieczeństwa informacyjnego, polityka bezpieczeństwa informacji, polegająca w dużej mierze na powielaniu nieadekwatnych czy niezbyt aktualnych ujęć;
– niedomaga wymiar praktycznych wskazań, który nie powinien polegać tylko na przeglądzie aktualnych rozwiązań organizacyjnych, prawnych czy instytucjonalnych, ale także na przedstawianiu na bazie wyników realizowanych badań konkretnych propozycji zmian.

Jeżeli chodzi o wskazanie wypływających z przedstawionych wyników badań oraz sformułowanych wniosków generalnych kierunków dalszych badań, to można je pogrupować w ramach czterech obszarów.

Pierwszy obejmuje weryfikację i precyzowanie funkcjonujących pojęć oraz wprowadzanie terminów adekwatnie ujmujących nowe elementy, o które sfera informacyjna bezpieczeństwa ciągle się wzbogaca. Dodać należy, że takie podejście wpisuje się w potrzeby rozwoju teorii bezpieczeństwa w ogóle, a bezpieczeństwa informacyjnego w szczególności.

Drugi obszar to tworzenie na bazie ustaleń i rozstrzygnięć teoretycznych modelowych propozycji rozwiązań praktycznych w sferze bezpieczeństwa informacyjnego, przystających do współczesnych i perspektywicznych potrzeb społecznych i instytucjonalnych. W tym obszarze ważne jest również kształtowanie adekwatnych do aktualnej fazy rozwoju społecznego sposobów rozumienia bezpieczeństwa informacyjnego wraz z ugruntowywaniem w świadomości społecznej jego znaczenia.

Trzeci obszar to przygotowywanie skutecznych rozwiązań profilaktycznych oraz reaktywnych odpowiedzi na pojawiające się zagrożenia i wyzwania w sferze bezpieczeństwa informacyjnego, ze szczególnym uwzględnieniem dezinformacji, walki i wojny informacyjnej, niwelowania barier informacyjnych oraz skutecznego zapewnienia wolności informacyjnej. Ważne jest na tym gruncie również tworzenie instrumentów do diagnozowania stanu bezpieczeństwa informacyjnego.

Czwarty obszar to intensyfikacja badań interdyscyplinarnych, łączących wysiłki badaczy z kręgu nauki o bezpieczeństwie z przedstawicielami innych nauk, m.in. w zakresie doskonalenia rozwiązań prawnych, instytucjonalnych i organizacyjnych służących do zapobiegania i zwalczania przestępczości informacyjnej, prawnych i etycznych aspektów funkcjonowania sztucznej inteligencji oraz prowadzenia walk i wojen informacyjnych.

Należy podkreślić, że przeprowadzone analizy i sporządzone w oparciu o nie charakterystyki i oceny w pełni upoważniają do stwierdzenia, że bezpieczeństwo informacyjne stanowi współcześnie nie tylko szczególnie doniosłą, ale również bardzo wrażliwą dziedzinę. Ta specyficzna wrażliwość związana jest z powszechnym wykorzystaniem informacji oraz powstawaniem na tym gruncie obok szans (wykorzystywanych w dużej mierze) także wielu wyzwań i zagrożeń dla kształtowania i utrzymania pożądanego (odpowiedniego) poziomu tego bezpieczeństwa. Nie ulega zatem wątpliwości, że obok działań praktycznych muszą być prowadzone również systematyczne badania naukowe o charakterze teoretycznym. Badania te powinny podążać w kierunku interdyscyplinarności, albowiem, jak podkreślano w poszczególnych częściach monografii, skutecznych rozwiązań w zakresie bezpieczeństwa informacyjnego nie sposób wypracować bez udziału i oparcia się na dorobku innych obok nauki o bezpieczeństwie nauk, jak chociażby informatologii, infoekologii, informatyki, kryminologii, nauki o polityce i administracji czy nauk prawnych. Istotnym wymiarem takiej działalności badawczej powinno być również analizowanie na gruncie naukowym, przy zastosowaniu adekwatnie ujmowanych pojęć podstawowych, takich jak np. bezpieczeństwo informacyjne czy bezpieczeństwo informacji, poprawności oraz efektywności istniejących i projektowanych rozwiązań dotyczących bezpieczeństwa informacyjnego. Wprowadzanie niezbędnej ich modernizacji, a w wielu aspektach sięganie po zupełnie nowe instrumenty i metody budowania i zarządzania tym bezpieczeństwem. Można też sformułować kolejną ocenę, mówiącą, że zarządzanie sferą bezpieczeństwa informacyjnego jest obecnie nie tylko jedną z najdynamiczniej rozwijających się dziedzin działalności w zakresie bezpieczeństwa, ale powinno być ono traktowane także jako dziedzina newralgiczna (priorytetowa) dla całościowo postrzeganego zarządzania bezpieczeństwem. Taki stan rzeczy stanowi jedną z konsekwencji funkcjonowania globalnego społeczeństwa informacyjnego, które znajduje się obecnie w fazie przechodzenia do nowej formy – coraz szerzej korzystającej z rozwiązań opartych na sztucznej inteligencji. Tym przemianom nieustannie towarzyszy pojawianie się nowych wyzwań, zagrożeń, ale również szans. Zapobieganie tym zagrożeniom, podejmowanie wyzwań i optymalne wykorzystywanie pojawiających się szans wymaga stosowania coraz to nowych rozwiązań: prawnych, organizacyjnych, edukacyjnych, technicznych i innych. Rozważania dotyczące teoretycznych aspektów bezpieczeństwa informacyjnego, których efekty, jak już wspomniano, powinny służyć usprawnianiu działań praktycznych na rzecz jego

zapewnienia. Nie mogą zatem pozostawać zamknięte w ramach zgromadzonego już dorobku, lecz muszą systematycznie wraz z przyrostem nowych rozwiązań i możliwości w sferze informacyjnej służyć eksplorowaniu zmieniającej się szybko rzeczywistości. Zważywszy, że jest to obszar rozległy, nie wydaje się możliwym stworzenie odnoszącego się do tej problematyki opracowania o charakterze kompleksowym, podejmującego wszystkie jej aspekty. W związku z powyższym przedstawione w publikacji rozważania przyjęły formułę oceny i analizy pewnego jej wycinka, z pozostawieniem szerokiej perspektywy do dalszych badań szczegółowych.

W konkluzji, w świetle tytułu monografii autor pragnie podkreślić, że nie traktuje kwestii bezpieczeństwa informacyjnego jako nadrzędnej wobec innych sfer bezpieczeństwa. Jednak rozwój społeczeństwa informacyjnego, zdarzenia indywidualne i zbiorowe, w których jako członkowie tego społeczeństwa uczestniczymy, pokazują, że nie jesteśmy w stanie bez dostępu do dobrej jakości informacji bezpiecznie funkcjonować. Jednocześnie w coraz większej ilości sytuacji, gdy wytwarzamy jakieś informacje, komuś je przekazujemy w postaci różnorodnych komunikatów, czy też je odbieramy i przetwarzamy, za każdym razem wspomagani jesteśmy narzędziami i systemami teleinformatycznymi, bez których większości z tych czynności nie można już wykonać. Przesuwa to ludzkość coraz szybciej do punktu, w którym będzie musiała ona bezpieczeństwo informacyjne umieścić w miejscu centralnym, dominującym nad innymi wymiarami bezpieczeństwa. Sfera bezpieczeństwa informacyjnego już dziś jest szczególnym aspektem ludzkiego życia indywidualnego i zbiorowego. Dużo w niej rozlicznych sytuacji, w których człowiek konfrontuje się z rozpoznanymi i uświadamianymi oraz istniejącymi obiektywnie, lecz subiektywnie pozostającymi enigmatami zagrożeniami i wyzwaniami. Można powiedzieć, że z bezpieczną i mniej bezpieczną oraz szkodliwą (niebezpieczną) informacją spotykamy się w codziennym życiu. Wiąże się to z tym, że ciągle coś poznajemy, zdobywamy nową wiedzę na różne tematy, a na tej bazie dokonujemy poznawczych i praktycznych wyborów. W oparciu o informacje i zmienianą przy ich pomocy wiedzę modyfikujemy nastawienia czy wyobrażenia, podejmujemy także decyzje, które zawsze w jakiś sposób (często zasadniczy) zmieniają nasze życie. Takie powiązanie informacji, poznania i wiedzy czynią z bezpieczeństwa informacyjnego i bezpieczeństwa informacji specyficzny konstrukt, który autor starał się jak najlepiej przedstawić, będąc przekonanym o korzyściach z tego płynących zarówno dla praktyki, jak i nauki.

Bibliografia

I. Akty prawne i dokumenty

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, Dz.U. 1993, nr 61, poz. 284.

Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r., Dz.U. 1977, nr 38, poz. 167.

Rezolucja Parlamentu Europejskiego z dnia 16 lutego 2017 r., zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki, 2015/2103(INL).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Dz.U. 1994, nr 24, poz. 83 z późn. zm.

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz.U. 1997, nr 88, poz. 553 z późn. zm.

Ustawa z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej, Dz.U. 2001, nr 49, poz. 508 z późn. zm.

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, Dz.U. 2019, poz. 1429.

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

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

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2017, poz. 2247.

Zarządzenie Ministra Inwestycji i Rozwoju z dnia 20 marca 2019 r. w sprawie Polityki Bezpieczeństwa Informacji w Ministerstwie Inwestycji i Rozwoju, Dziennik Urzędowy Ministra Inwestycji i Rozwoju 2019, poz. 7.

Zarządzenie Ministra Sprawiedliwości z dnia 27 marca 2019 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości, Dziennik Urzędowy Ministra Sprawiedliwości 2019, poz. 118.

II. Monografie

Aleksandrowicz T.R., *Podstawy walki informacyjnej*, Warszawa 2016.

Aleksandrowicz T.R*., Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze,* Warszawa 2021.

Babik W., *Ekologia informacji*, Kraków 2014.

Balcerowicz B., *O pokoju. O wojnie. Między esejem a traktatem*, Warszawa 2013.

Barta J., Markiewicz R., *Komentarz do ustawy o prawie autorskim i prawach pokrewnych*, Warszawa 2003.

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

Bostrom N., *Superinteligencja. Scenariusze, strategie, zagrożenia*, Gliwice 2016.

Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2000.

Bratnicki M., *Kompetencje przedsiębiorstwa. Od określenia kompetencji do zbudowania strategii*, Warszawa 2000.

Celarek K., *Prawo informacyjne. Problem badawczy teorii prawa administracyjnego*, Warszawa 2013.

Clausewitz C. von, *O naturze wojny*, Warszawa 2010.

Darczewska J., Anatomia *rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, Warszawa 2014.

Davenport T.H., Prusak L., *Working Knowledge*, Boston 1998.

Deacon R., *Spyclopaedia*, London 1989.

Deja M., Rożej A., Stochaj J., Stolarski J., *Organizowanie i monitorowanie przepływu informacji w jednostkach administracyjnych,* Warszawa 2015.

Dembowska M*., Nauka o informacji naukowej (informatologia). Organizacja i problematyka badań w Polsce*, Warszawa 1991.

Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.

Drogoń W., Mąka D., Skawina M., *Jak chronić tajemnice? Ochrona informacji w instytucjach państwowych i przedsiębiorstwach prywatnych*, Warszawa 2004.

Ficoń K., *Sztuczna inteligencja. Nie tylko dla humanistów*, Warszawa 2013.

Flasiński M., *Wstęp do sztucznej inteligencji*, Warszawa 2011.

Goban-Klas T., *Media i komunikowanie masowe: teorie analizy prasy, radia, telewizji i Internetu*, Warszawa 2005.

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

Gogołek W., Cetera W., *Logistyka i zarządzanie w mediach. Leksykon tematyczny. Zarządzanie, IT*, Warszawa 2014.

Golicyn A., *Nowe kłamstwa w miejsce starych. Komunistyczna strategia podstępu i dezinformacji,* Warszawa 2007.

Griffin R.W., *Podstawy zarządzania organizacjami,* Warszawa 2000.

Hetmański M., *Świat informacji,* Warszawa 2015.

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

Jaroszewska I., *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017.

Kaczmarek J., Staciwa C., Zapolski S., *Doktryna wojenna*, Warszawa 1982.

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

Kisielnicki J., Gwiazda T., *Wstęp do informatyki w zarządzaniu*, Warszawa 2004.

Kisielnicki J., *Zarządzanie i informatyka*, Warszawa 2014.

Kitler W., *Organizacja bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty ustrojowe, prawno-administracyjne i systemowe*, Toruń 2018.

Korzeniowski L.F., *Firma w warunkach ryzyka gospodarczego*, Kraków 2002.

Korzeniowski L.F., *Podstawy nauk o bezpieczeństwie*, Warszawa 2017.

Kossecki J., *Totalna wojna informacyjna XX wieku a II RP*, Kielce 1997.

Kotarbiński T., *Traktat o dobrej robocie*, Warszawa 1982.

Kowalczyk E., *O pojęciu informacji,* Warszawa 1981.

Kowalewski J., Kowalewski M., *Polityka bezpieczeństwa informacji w praktyce*, Wrocław 2014.

Kowalewski J., Kowalewski M., *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm,* Warszawa 2017.

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

Kunicka-Michalska B., *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości. Rozdział XXX i XXXIII Kodeksu karnego. Komentarz*, Warszawa 2000.

Kurzweil R., *Nadchodzi osobliwość. Kiedy człowiek przekroczy granice biologii*, Warszawa 2016.

Larecki T.H., *Wielki leksykon tajnych służb świata*, Warszawa 2017.

Libicki M.C., *What Is Information Warfare*, Islamabad 1995.

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

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

Lubański M., *Filozoficzne zagadnienia teorii informacji*, Warszawa 1974.

Łuczak J., Tyburski M., *Systemowe zarządzanie bezpieczeństwem informacji*, Poznań 2010.

Machiavelli N., *Książę. Rozważania nad pierwszym dziesięcioksięgiem historii Rzymu Liwiusza*, Warszawa 1984.

Machowicz K., *Wolność wypowiedzi w Polsce wobec ochrony prawa do prywatności*, Warszawa 2018.

Madej M., *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007.

Malara Z., Rzęchowski J., *Zarządzanie informacją na rynku globalnym. Teoria i praktyka*, Warszawa 2011.

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

Modrzejewski Z., *Operacje informacyjne*, Warszawa 2015.

Mrozowski M., *Media masowe. Władza, rozrywka i biznes*, Warszawa 2001.

Newcourt-Nowodworski S., *Czarna propaganda. Polska, Niemcy, Wielka Brytania. Tajemnice największych oszustw II wojny światowej*, Kraków 2008.

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

Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011.

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

Oleński J., *Elementy ekonomiki informacji*, Warszawa 2000.

Osgood R.E., *Limited War: The Challenge To American Security,* University of Chicago Press, 1957.

Pacepa I.M., Rychlak R.J., *Dezinformacja. Były szef wywiadu ujawnia metody dławienia wolności, zwalczania religii i wspierania terroryzmu*, Gliwice 2015.

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

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

Przelaskowski W., *Problemy informacji naukowej*, Warszawa 1979.

Razjer M., *Strategie dywersyfikacji przedsiębiorstw*, Warszawa 2001.

Redelbach A., *Prawa naturalne, prawa człowieka, wymiar sprawiedliwości. Polacy wobec Europejskiej Konwencji Praw Człowieka*, Toruń 2000.

Rowecki S., *Propaganda w przygotowaniu kraju*, Warszawa 1933.

Rusinek M., *Tajemnica zawodowa i jej ochrona w polskim procesie karnym*, Warszawa 2007.

Rutkowski L., *Metody i techniki sztucznej inteligencji. Inteligencja obliczeniowa*, Warszawa 2005.

Rzemieniak M., Kamińska K., *Wewnętrzne public relations w sytuacjach kryzysowych*, Lublin 2012.

Schmitt C., *Teologia polityczna i inne pisma*, Kraków-Warszawa 2000.

Schwartau W., *Information Warfare,* 2nd Ed., New York 1996.

Shannon C.E., *The Mathematical Theory of Communication*, Illinois 1945.

Skibiński F., *Rozważania o sztuce wojennej*, Warszawa 1978.

Skowronek-Mielczarek A., Leszczyński Z., *Controlling – analiza i monitoring w zarządzaniu przedsiębiorstwem*, Warszawa 2007.

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

Stefanowicz B., *Informacja,* Warszawa 2004.

Stefanowicz B., *Informacja. Wiedza. Mądrość*, Warszawa 2013.

Stoner J.A.F., Freeman R.E., Gilbert D.R., *Kierowanie*, Warszawa 2001.

Sun Tzu, *Sztuka wojny*, Warszawa 1994.

Szewc T., *Publicznoprawna ochrona informacji*, Warszawa 2007.

Szpyra R., *Operacje informacyjne państwa w działaniach sił powietrznych*, Warszawa 2002.

Ścibiorek Z., *Podejmowanie decyzji,* Warszawa 2003.

Świgoń M., *Bariery informacyjne: podstawy teoretyczne i próba badań w środowisku naukowym*, Warszawa 2006.

Tiwana A., *Przewodnik po zarządzaniu wiedzą*, Warszawa 2003.

Tyrała P., *Zarządzanie kryzysowe: ryzyko, bezpieczeństwo, obronność*, Toruń 2003.

Unold J., *Systemy informacyjne marketingu*, Wrocław 2009.

Unold J., *Zarządzanie informacją w cyberprzestrzeni,* Wrocław 2015.

Ura E., Pieprzny S., *Bezpieczeństwo wewnętrzne państwa*, Rzeszów 2015.

Volkoff V., *Dezinformacja – oręż wojny*, Warszawa 1991.

Wiener N., *Cybernetyka i społeczeństwo*, Warszawa 1960.

Wojciechowska-Filipek S., *Zarządzanie jakością informacji w organizacjach zhierarchizowanych*, Warszawa 2015.

Wright Q., *A Study of War*, Chicago 1942.

Wrzosek M., *Wojny przyszłości. Doktryna, technika, operacje militarne*, Warszawa 2018.

Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, Wrzosek M. (red.), Warszawa 2019.

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

III. Artykuły i rozdziały w opracowaniach zbiorowych

Aleksandrowicz T.R., *Bezpieczeństwo informacyjne państwa*, „Studia Politologiczne" 2018, nr 49.

Babik W., *Środowisko informacyjne człowieka*, [w:] *Nauka o informacji*, W. Babik (red.), Warszawa 2016.

Banasik M., *Znaczenie nowoczesnych technologii dla bezpieczeństwa*, „Rocznik Bezpieczeństwa Międzynarodowego" 2018, vol. 12, nr 2.

Batorowska H., *Bezpieczeństwo informacyjne w dyskursie naukowym – kierunki badań*, [w:] *Bezpieczeństwo informacyjne w dyskursie naukowym*, H. Batorowska, E. Musiał (red.), Kraków 2017.

Batorowska H., *Nauka o informacji (informatologia) z perspektywy nowych wyzwań edukacyjnych,* „Edukacja – Technika – Informatyka" 2015, nr 3.

Bernatek-Zaguła I., *Informacja jako kategoria prawna*, „Dyskurs Prawniczy i Administracyjny" 2018, nr 1.

Bielawski R., Ziółkowska A., *Media społecznościowe a kształtowanie bezpieczeństwa państwa*, [w:] *Człowiek a technologia cyfrowa – przegląd aktualnych doniesień*, P. Szymczyk, K. Maciąg (red.), Lublin 2018.

Bogatyńska-Kucharska A., *Normy poufności i taktu w etyce ogólnej oraz w etyce zawodowej psychoterapeutów*, „Etyka" 2019, nr 2.

Bojar-Fijałkowski T., Dostęp *do informacji publicznej – wybrane zagadnienia materialnoprawne i proceduralne z uwzględnieniem informacji o środowisku i jego ochronie jako szczególnego rodzaju informacji publicznej*, [w:] *Dostęp do informacji publicznej Wybrane aspekty teorii i praktyki,* A. Lusińska, A. Kalinowska-Żeleźnik (red.), Gdańsk 2014.

Borecki J., *Dezinformacja jako zagrożenie dla prywatnych i publicznych przedsiębiorstw*, „The Warsaw Institute Review" – edycja specjalna, 2017.

Chlebowicz P., *Interpretacja pojęcia dezinformacji w świetle art.132 k.k.*, „Studia Prawnoustrojowe" 2012, nr 15.

Ciach K., Dębski J., *Użyteczność informacji finansowych: wybrane aspekty*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2015, nr 117.

Ciborowski L., *Pojęciowa interpretacja terminu „informacja" i jej pochodnych*, „Zeszyty Naukowe AON" 2010, nr 4.

Ciborowski L., *Potencjalne zagrożenia – identyfikacja i charakterystyka*, „Myśl Wojskowa" 2000, nr 4.

Cieślarczyk M., *Psychospołeczne i prakseologiczne aspekty bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne w XXI wieku*, M. Kubiak, S. Topolewski (red.), Siedlce-Warszawa 2016.

Daniluk P., *Wojna informacyjna – złożona przeszłość i niepewna przyszłość*, „Rocznik Bezpieczeństwa Międzynarodowego" 2019, nr 2.

Daniluk P., *Współczesne wymiary konfrontacji informacyjnej*, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, nr 2.

Dąbrowski A., *Filozofia informacji Luciano Floridiego (ekspozycja nieformalno-logiczna)*, „Zagadnienia Naukoznawstwa" 2015, nr 4.

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

Drozd A., *Uprawnienie podmiotu zatrudniającego do pozyskiwania informacji o kandydacie na pracownika*, „Państwo i Prawo" 2000, nr 12.

Fehler W., *Sztuczna inteligencja – szansa czy zagrożenie*, „Studia Bobolanum" 2017, nr 3.

Fehler W., *Bariery informacyjne jako czynnik kształtujący współczesne bezpieczeństwo informacyjne*, [w:] *Prawne aspekty informacji chronionych*, M. Kubiak (red.), Siedlce 2020.

Fehler W., *Informacja jako przedmiot polityki bezpieczeństwa informacyjnego*, „Studia Humanistyczno-Społeczne" 2018, t. 22.

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

Fehler W., *Polityka bezpieczeństwa jako szczególny wymiar polityki państwa,* [w:] *Współczesne bezpieczeństwo polityczne*, S. Jaczyński, M. Kubiak, M. Minkina (red.), Warszawa-Siedlce 2012.

Fehler W., *Społeczeństwo informacyjne jako składnik procesu globalizacji*, [w:] *Problemy polityki bezpieczeństwa wobec procesów globalizacji*, J. Świniarski, J. Tymanowski (red.), Toruń 2003.

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

Floridi L., *A look in to the future impact of ICT on our lives,* „The Information Society" 2007, no. 23.

Floridi L., *Open problems in the philosophy of information*, "Metaphilosophy" 2004, no. 35 (4).

Furmanek W., *Piąta rewolucja przemysłowa. Eksplikacja pojęcia*, „Edukacja – Technika – Informatyka" 2018, nr 2 (24).

Galewski T., *Bariery informacyjne w przedsiębiorstwie*, „Zarządzanie i Finanse" 2012, nr 1.

Galewski T., *Psychologiczne bariery informacyjne w społeczeństwie informacyjnym*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Informatica" 2012, nr 29.

Garwol K., *Droga do powstania społeczeństwa informacyjnego we współczesnych* demokracjach, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2010, nr 57.

Garwol K., *Negatywny wpływ technologii teleinformatycznej na obywateli społeczeństwa informacyjnego, wybrane aspekty, „*Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2011, nr 67.

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

Gospodarek T., *Elastyczność zasobu informacyjnego*, [w:] *Elastyczność organizacji*, R. Krupski (red.), Wrocław 2008.

Górny M., Nauka *o informacji jako dyscyplina naukowa*, [w:] *Nauka o informacji*, W. Babik (red.), Warszawa 2016.

Grabowski T., *Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014-2016),* „Horyzonty Polityki" 2017, nr 20.

Gronowska-Starzeńska A., *Walka informacyjna – wybrane problemy w ujęciu cybernetycznym,* „Zeszyty Naukowe Akademii Sztuki Wojennej" 2017, nr 4.

Gutowski P., *Podstawowe cechy, funkcje i determinanty kreujące społeczeństwo informacyjne w nowoczesnej gospodarce,* „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2009, nr 46.

Harmon G., *The measurement of information*, "Information Processing and Management" 1984, no. 1–2.

Hoc S., *Przestępstwo dezinformacji wywiadowczej w kodeksie karnym*, „Przegląd Sądowy" 2000, nr 5.

Kamuda D., *Wybrane aspekty przestępczości skierowanej przeciwko informacjom niejawnym – art. 265 i 266 k.k.*, „Modern Management Review" 2018, nr 1.

Kęsy M., *Społeczeństwo informacyjne w rozwoju cywilizacyjnym ludzkości*, „Dydaktyka Informatyki" 2011, nr 6.

Kisiel A., *Społeczeństwo informacyjne – wybrane przykłady szans i zagrożeń*, „Studies & Proceedings of Polish Association for Knowledge Management" 2011, t. 51.

Kisilowska M., *Przestrzeń informacyjna jako termin informatologiczny*, „Zagadnienia Informacji Naukowej" 2011, nr 2.

Kocoń P., *Militarne operacje dezinformacyjne w perspektywie interakcjonizmu symbolicznego*, „Zeszyty Naukowe WSOWL" 2012, nr 4.

Kopeć R., *Robotyzacja wojny*, „Społeczeństwo i Polityka" 2016, nr 4 (49).

Kraft J., *Jakość dostępu i umiejętności użytkowników – nierozpoznane elementy wykluczenia cyfrowego w społeczeństwie informacyjnym*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2009, nr 35.

Krakowska M., *Zachowania informacyjne człowieka*, [w:] *Nauka o informacji*, W. Babik (red.), Warszawa 2016.

Kukla A., *Tajność i jawność w kontekście ochrony informacji*, „Civitas. Studia z Filozofii Polityki" 2017, nr 20.

Kulikowski J.L., *Człowiek i infosfera*, „Problemy" 1978, nr 3.

Kunasz M., *Zasoby przedsiębiorstwa w teorii ekonomii*, „Gospodarka Narodowa" 2006, nr 10.

Kwećka R., *Bezpieczeństwo informacyjne,* [w:] *Podstawy bezpieczeństwa narodowego (państwa*), J. Pawłowski (red.), Warszawa 2017.

Lasota-Jądrzak A., *Jak mierzyć jakość informacji?*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej" 2016, nr 4.

Lech T., Podgórski G., *Bezpieczeństwo w sieci*, [w:] *Społeczeństwo informacyjne*, J. Papińska-Kacperek (red.), Warszawa 2008.

Lelonek A., *Wojna informacyjna, operacje informacyjne i psychologiczne: pojęcia, metody i zastosowanie*, [w:] *Potencjał słowa. Międzynarodowe stosunki i komunikacja: stan i perspektywy*, A. Lelonek (red.), Warszawa-Lwów 2016.

Lubański M., *Społeczeństwo informacyjne a cywilizacja informatyczna*, [w:] *Dylematy cywilizacji informatycznej*, A. Szewczyk (red.), Warszawa 2004.

Maciejewski M., *Prawo informacji – zagadnienia podstawowe*, [w:] *Prawo informacji. Prawo do informacji*, W. Góralczyk jr. (red.), Warszawa 2006.

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

Madej M.*, Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009.

Marciniak M., *Informacja w procesie decydowania politycznego*, „Rocznik Nauk Politycznych" 2010, nr 1.

Marczyk M., *Bezpieczeństwo teleinformatyczne wobec ataków terrorystycznych*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa XXI wieku*, M. Górka (red.), Warszawa 2014.

Materska K., *Zarządzanie informacją i wiedzą*, [w:] *Nauka o informacji*, W. Babik (red.), Warszawa 2016.

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

Nogalski B., Surawski B.M., *Informacja strategiczna w zarządzaniu przedsiębiorstwem*, [w:] *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystanie*

i ochrona (wybrane problemy teorii i praktyki), R. Borowiecki, M. Kwieciński (red.), Kraków 2003.

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

Ochman P., *Spór o pojęcie dokumentu w prawie karnym*, „Prokuratura i Prawo" 2009, nr 1.

Osika G., *Czekając na osobliwość – o modelach interpretacji techniki*, „Filo-Sofija" 2017, nr 39/1.

Pałęga M., Knapiński M., Rydz D., *Identyfikacja i ocena zagrożeń bezpieczeństwa informacji za pomocą wybranych instrumentów zarządzania jakością*, [w:] *Innowacje w zarządzaniu i inżynierii produkcji*, R. Knosala (red.), t. II, Opole 2018.

Pieszko G., *Społeczno-prawne aspekty penalizacji fałszowania dokumentów*, „Studia Prawnoustrojowe" 2015, nr 29.

Piórkowska-Flieger J., *Prawne i społeczne uzasadnienie karalności fałszu dokumentu*, „Studia Iuridica Lublinensia" 2003, nr 1.

Polak A., *Wojna. Definicje, teorie, klasyfikacje*, „Zeszyty Naukowe AON" 2010, nr 4.

Potejko P., *Bezpieczeństwo informacyjne*, [w:] *Bezpieczeństwo państwa*, K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), Warszawa 2009.

Przybysz P., *Czy należy obawiać się superinteligencji?*, „Studia Metodologiczne" 2017, nr 38.

Roman W.K., Między *archiwistyką a architekturą informacji*, „Archiwa – Kancelarie – Zbiory" 2018, nr 9.

Różanowski K., *Sztuczna inteligencja: rozwój, szanse i zagrożenia*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2007, nr 2.

Schoch F., *Zagadnienie równowagi między wolnością informacyjną a ochroną danych w niemieckim profesorskim projekcie Kodeksu Informacyjnego*, [w:] *Internet. Ochrona wolności, własności i bezpieczeństwa*, G. Szpor (red.), Warszawa 2011.

Schroeder M.J., *Spór o pojęcie informacji,* „Studia Metodologiczne" 2015, nr 4.

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

Sienkiewicz P., Świeboda H., *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009.

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

Sienkiewicz P., *Zagrożenia dla demokracji w społeczeństwie informacyjnym*, [w:] *Transformacja demokracji*, L.W. Zacher (red.), Warszawa 2011.

Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8.

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

Sosińska-Kalata B., *Obszary badań współczesnej informatologii (nauki o informacji),* „Zagadnienia Informacji Naukowej – Studia Informacyjne" 2013, nr 2.

Stefanowicz M., *Cyberprzestępczość – próba diagnozy zjawiska*, „Kwartalnik Policyjny" 2017, nr 4.

Świeboda H., *Percepcja społecznych konsekwencji rozwoju społeczeństwa informacyjnego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2011, nr 67.

Świerczek M., *„System matrioszek", czyli dezinformacja doskonała. Wstęp do zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 10.

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

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

Vego M.N., *Effect-Based Operations: A Critique*, „Joint Forces Quarterly" 2006, no. 41.

Wachowicz M.J., *Ujęcie teoretyczne pojęcia dezinformacji*, „Wiedza Obronna" 2019, nr 1–2.

Wasiuta O., Wasiuta S., *Wojna informacyjna zagrożeniem dla bezpieczeństwa ludzkości*, [w:] *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania*, H. Batorowska (red.), Kraków 2017.

Werner J., Szczepaniuk E., *Bezpieczeństwo informacyjne organizacji*, „Zeszyty Naukowe AON" 2016, nr 4.

Wędrowska E., *Ilościowe i jakościowe koncepcje informacji,* „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2010, nr 57.

Wilson T., *Information behaviour an interdisciplinary perspective*, „Information Processing &Management" 1997, vol. 33, no. 4.

Włodarczyk J., *Informacja i jej znaczenie dla konsumentów – wybrane aspekty*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2006, nr 38.

Wojnowski M., *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w*., „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12.

Wojnowski M., *Terroryzm w służbie geopolityki. Konflikt rosyjsko-ukraiński jako przykład realizacji doktryny geopolitycznej Aleksandra Dugina i koncepcji „wojny buntowniczej" Jewgienija Messnera*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 11.

Wróblewski R., *O definiowaniu wojny*, [w:] *Oblicza współczesnych wojen*, M. Kubiak, R. Wróblewski (red.), Warszawa-Siedlce 2018.

Wrzosek M., *Dezinformacja – skuteczny element walki informacyjnej*, „Zeszyty Naukowe AON" 2012, nr 2.

Wrzosek M., *Zmagania o informacje we współczesnych organizacjach*, „Zeszyty Naukowe AON" 2010, nr 4.

Zacharski J.R., *Wojna informacyjna*, [w:] *Zagrożenia i wyzwania bezpieczeństwa współczesnego świata*, I. Oleksiewicz, K. Stępień (red.), Warszawa 2016.

Zalewski T., *Definicja sztucznej inteligencji*, [w:] *Prawo sztucznej inteligencji*, L. Lai, M. Świerczyński (red.), Warszawa 2020.

Zaskórski P., Szwarc K., *Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2013, nr 9.

Zieliński J.S., *Zarys badań nad sztuczną inteligencją*, [w:] *Inteligentne systemy w zarządzaniu. Teoria i praktyka*, J.S. Zieliński (red.), Warszawa 2000.

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

Żebrowski A., *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Roczniki Kolegium Analiz Ekonomicznych" 2013, nr 29.

Żebrowski A., *Determinanty walki informacyjnej*, [w:] *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania*, H. Batorowska (red.), Kraków 2017.

IV. Raporty, ekspertyzy i opracowania

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2013.

Doktryna bezpieczeństwa informacyjnego. Projekt, Biuro Bezpieczeństwa Narodowego, Warszawa 2015.

Inspiracja i aktywność jako metody nowoczesnego wywiadu, Ministerstwo Spraw Wojskowych Sztab Generalny, Warszawa 1926.

Księga komunikacji kryzysowej 2017. Podstawy zarządzania informacją w kryzysie, Rządowe Centrum Bezpieczeństwa, Warszawa 2017.

New estimates of benefits of crash avoidance features on passenger vehicles, „Status Report", Insurance Institute for Highway Safety, 2010.

Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001––2006, Ministerstwo Łączności, Warszawa 2001.

Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, Wspólny komunikat do Parlamentu Europejskiego, Rada Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, 2013.

Sztuczna inteligencja dla Europy (*COM/2018/237 final)*, Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-społecznego i Komitetu Regionów.

Wytyczne dla dostępności informacji. Technologie informacyjno-komunikacyjne (TIK) w zapewnianiu dostępności informacji w procesie uczenia się (ICT4IAL), European Agency for Special Needs and Inclusive Education, 2015.

Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji, Komisja Europejska, Bruksela 2019.

Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego. Informacja o wynikach kontroli, KAP.430.020.2018 Nr ewid. 187/2018/P/18/006/KAP, Najwyższa Izba Kontroli, Departament Administracji Publicznej, Warszawa 2018.

V. Inne źródła

A. Berger, *Sztuczna inteligencja Google'a tworzy własne systemy szyfrowania*, [online] https://trybawaryjny.pl/sztuczna-inteligencja-googlea-tworzy-wlasne-systemy szyfrowania.

Bralczyk J., *Słownik 100 tysięcy potrzebnych słów*, Warszawa 2005.

Brzeski R., *Dezinformacja. Skrypt*, Warszawa 2011, [online] https://forumemjot.wordpress.com/2012/06/04/dezinformacja-skrypt-warszawa-2011-rafal-brzeski/.

Cypryjański J., *Możliwości szacowania wartości informacji ex ante a funkcje informacji w organizacji*, „Prace Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2005, [online] http://www.swo.ue.katowice.pl/swo-2005/zarzadzanie-wiedza-i-rozwiazania-bi/mozliwosci-szacowania-wartosci-informacji-ex-ante-a-funkcje-informacji-w-organizacji.html.

Darczewska J., *Dezinformacja – rosyjska broń strategiczna*, [online] https://rcb.gov.pl/dezinformacja-rosyjska-bron-strategiczna/.

Dictionary for Library and Information Science, [online] https://products.abc-clio.com/ODLIS/odlis_w.aspx.

Domagała K., Domagała T., *Tajemnice prawnie chronione po wejściu w życie ustawy z dnia 05.08.2010 r. o ochronie informacji niejawnych*, [online] http://www.zielona-gora.po.gov.pl/magazyn/upload/lektury_elektroniczne/tajemnice1.pdf.

Encyklopedia bezpieczeństwa, O. Wasiuta, S. Wasiuta (red.), Kraków 2021.

Encyklopedia politologii. Pojęcia, teorie i metody, M. Żmigrodzki, M. Sokół (red.), t. 1, Warszawa 2016.

Encyklopedia PWN, [online] https://encyklopedia.pwn.pl/haslo/;3957879.

Encyklopedia zarządzania, [online] https://mfiles.pl/pl/index.php/Zas%C3%B3b.

Europa na miarę ery cyfrowej. Zapewnienie ludziom dostępu do technologii najnowszej generacji, [online] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_pl#policy-areas.

Europejska agenda cyfrowa, [online] https://www.europarl.europa.eu/factsheets/pl/sheet/64/europejska-agenda-cyfrowa.

S. Gliwa, *AI vs AI. Jakie trendy bezpieczeństwa i zagrożeń czekają nas w 2020 roku*?, [online], https://www.cyberdefence24.pl/ai-vs-ai-jakie-trendy-bezpieczenstwa-i-zagrozen-czekaja-nas-w-2020-roku.

Godbold N, *Beyond information seeking: towards a general model of information behaviour*, „Information Research" 2006, no. 4, [online] https://files.eric.ed.gov/fulltext/EJ1104640.pdf.

Grabowski M., Zając A., *Dane, informacja, wiedza – próba definicji*, [online] https://www.cri.agh.edu.pl/uczelnia/tad/PSI11/art/Dane_informacje_wiedza.pdf.

Inny słownik języka polskiego, t.1, M. Bańko (red.), Warszawa 2000.

Kaczmarek S., *Integralność danych, czyli imperatyw kategoryczny bezpieczeństwa IT*, [online] http://it-filolog.pl/integralnosc-danych-czyli-imperatyw-kategoryczny-bezpieczenstwa-it/.

Klasyfikacja informacji, „Bezpieczeństwo Informacji. Biuletyn Tematyczny" 2006, nr 1, [online] http://security.dga.pl/biuletyn/dga_biuletyn_tematyczny_01_06.pdf.

Komunikat (KOM (2010) 2020 wersja ostateczna) – *Europa 2020: Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu*, [online] https://eur-lex.europa.eu/legal-content/pl/txt/html/?uri=legissum:em0028.

Korolov M., *AI isn't just for the good guys anymore*, [online] http://www.csoonline.com/article/3163022/advanced-persistent-threats/ai-isnt-just-for-the-good-guys-anymore.html.

Kosztowne podróbki – raport EUIPO, [online] https://europarlament.pap.pl/kosztowne-podrobki-raport-euipo.

Kościelniak P., *Sztuczna inteligencja robi się agresywna*, [online] http://www.rp.pl/Nowe-technologie/302149906-Sztuczna-inteligencja-robi-sie-agresywna.html.

Kubera G., *Ochrona punktów końcowych – co trzeba o niej wiedzieć*, „Computer World" z dn. 27.12.2018, [online] https://www.computerworld.pl/news/Ochrona-punktow-koncowych-co-trzeba-o-niej-wiedziec,411609.html.

Kumaniecki K., *Słownik łacińsko-polski*, Warszawa 1957.

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

Leksykon wiedzy wojskowej, Warszawa 1979.

Małkowski J., *Społeczeństwo informacyjne w Unii Europejskiej*, [online] https://alebank.pl/wp-content/uploads/2010/04/eds.2008.k4.007-013.pdf.

Materska K., *Rozwój koncepcji, informacji i wiedzy jako zasobu organizacji*, [online] https://www.academia.edu/2269216/Rozw%C3%B3j_koncepcji_informacji_i_wiedzy_jako_zasobu_organizacji?auto=download.

Merriam-Webster Dictionary, [online] https://qlf3cqm6hbj4jyqwnggyhohzia-adv7ofecxzh2qqi-merriam-webster-com.translate.goog/dictionary/war?show=0&t=1347910895.

Nowak P.A., *Rozwój społeczeństwa informacyjnego na świecie*, [online] https://si.lodzkie.pl/rozwoj-spoleczenstwa-informacyjnego-na-swiecie/.

Olender-Skorek M., Wydro K.B., *Wartość informacji*, [online] http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-article-BAT8-0008-0023.

Oszustwa publikacyjne i naruszenia praw autorskich, [online] https://www.biblos.pk.edu.pl/nauka/publikowanie-wybrane-aspekty/oszustwa-publikacyjne-i-naruszenia-praw-autorskich.

Pac B., *Wojna informacyjna jako skuteczne narzędzie destabilizacji państw i rządów*. Raport z 2 lutego 2016 r., [online] https://www.defence24.pl/wojna-informacyjna-jako-skuteczne-narzedzie-destabilizacji-panstw-i-rzadow-raport.

Palczewski S., *Etyczna sztuczna inteligencja na polu bitwy? Amerykańskie wojsko uważa, że to możliwe*, [online] https://cyberdefence24.pl/etyczna-sztuczna-inteligencja-na-polu-bitwy-amerykanskie-wojsko-uwaza-ze-to-możliwe.

Ploski Z., *Słownik encyklopedyczny – informatyka*, Wrocław 1999.

PN ISO/IECI 17799:2007, *Technika informatyczna – Techniki bezpieczeństwa –Praktyczne zasady zarządzania bezpieczeństwem*, Warszawa 2007.

PN-I-02000:2002, *Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia*, Warszawa 2002.

PN-ISO/IEC 27000:2007, *Technika informatyczna – Techniki bezpieczeństwa. – Praktyczne zasady zarządzania bezpieczeństwem informacji – Wymagania*, Warszawa 2007.

PN-ISO/IEC 27000:2012, *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji. – Przegląd i terminologia,* Warszawa 2012.

Policja sięga po niezwykłe rozwiązanie. Sztuczna inteligencja już namierza kierowców w Polsce, [online] https://auto.dziennik.pl/aktualnosci/artykuly/613953,policja-swiatla-samochod-mandat-akcja-ekran-warszawa-screen-network.html.

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa 2013, [online] https://jakubow.pl/wp-content/uploads/2015/06/Polityka-Ochrony-Cyberprzestrzeni-RP_148x210_wersja-pl.768174_715482.pdf.

Salecki M., *Perspektywy rozwojowe reklamy online: sprzedaż w dobie sztucznej inteligencji*, [online] https://iab.org.pl/aktualnosci/perspektywy-rozwojowe-reklamy-online-sprzedaz-w-dobie-sztucznej-inteligencji/.

Sewerynik A., *Plagiat ukryty a wzorowanie się na cudzej twórczości*, [online] https://www.rp.pl/Prawo-autorskie/302289997-Plagiat-ukryty-a-wzorowanie-sie-na-cudzej-tworczosci.html.

Sienkiewicz P., *Wizje i modele wojny informacyjnej*, [online] https://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf.

Skowroński M., Gugała A., Jurkiewicz S. i in., *Sztuczna inteligencja. Dobre praktyki, aspekty prawne i zastosowania w sektorze finansowym. Raport*, [online] http://fintechpoland.com/wp-content/uploads/2020/01/AI_raport_FIN.pdf.

Słownik język polskiego PWN, [online] https://sjp.pwn.pl/slowniki.

Słownik języka polskiego PWN, M. Szymczak (red.), t. I, Warszawa 1978.

Słownik terminologiczny informacji naukowej, M. Dembowska i in. (red.), Wrocław––Warszawa 1979.

Słownik terminów z zakresu bezpieczeństwa narodowego, Warszawa 2002.

Słownik wyrazów obcych PWN, J. Tokarski (red.), Warszawa 1980.

Streszczenie – Raport z 2019 r. na temat statusu ochrony praw własności intelektualnej. Dlaczego prawa własności intelektualnej są ważne, naruszenia praw własności intelektualnej oraz walka z podrabianiem i piractwem, [online] https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Status_Report_on_IPR_infringement/2019_Status_Report_on_IPR_infringement_exec_pl.pdf.

Szewc A., *Przestępstwa i wykroczenia przeciwko prawom własności przemysłowej*, [online] https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/3824/1/BSP%2019_A_Szewc.pdf.

Szpor G., *Prawo informacyjne*, [online] http://wikiprawna.com.pl/index.php?title=prawo_informacyjne.

Tadeusiewicz R., *Czy test Turinga mierzy inteligencję komputera*, [online] http://ryszardtadeusiewicz.natemat.pl/106415,czy-test-turinga-mierzy-inteligencje-komputera.

The Chairman of the Joint Chiefs of Staff Instruction, CJCSI S-3210.01, 02 January 1996.

The Stanford Encyclopedia of Philosophy, [online] https://quxcmx7hq3makbek7gukfbclza-adv7ofecxzh2qqi-plato-stanford-edu.translate.goog/archives/fall2008/entries/war/.

Turek A., *Sztuczna inteligencja – realne zagrożenie? Gates: „Nie rozumiem, czemu niektórzy się nie przejmują"*, [online] http://innpoland.pl/115221,sztuczna-inteligencja-realne-zagrozenie-gates-nie-rozumiem-czemu-niektorzy-sie-nie-przejmuja.

Vademecum bezpieczeństwa informacyjnego, O. Wasiuta, R. Klepka (red.), t. I, Kraków 2019.

War, [online] https://www.britannica.com/topic/war.

Wielka encyklopedia radziecka, t. XII, Moskwa 1952.

Włodarski A., *Sztuczna inteligencja. Nasze niebo i piekło*, [online] http://wyborcza.pl/magazyn/7,124059,20870967,sztuczna-inteligencja-bog-juz-istnieje.html.

Wydro K.B., *Badania nad istotą informacji, jej właściwościami i stosowanymi technikami informacyjnymi – próba systematyzacji w obszarze wiedzy o informacji*, Warszawa 2007, [online] https://docplayer.pl/17644783-Badania-nad-istota-informacji-jej-wlasciwosciami-i-stosowanymi-technikami-informacyjnymi-proba-systematyzacji-w-obszarze-wiedzy-o-informacji.html.

Spis tabel i rysunków

Streszczenie

Podstawy bezpieczeństwa informacyjnego

Monografia stanowi rezultat badań dotyczących teoretycznych kwestii bezpieczeństwa informacyjnego. Ich głównym celem była weryfikacja istniejących ustaleń co do fundamentalnych pojęć odnoszących się do istoty tego wymiaru bezpieczeństwa oraz przedstawienie propozycji autorskich w tym zakresie.

Pierwsza część publikacji poświęcona została sposobom pojmowania informacji i ukazaniu jej znaczenia. W jej obrębie, na tle charakterystyki przedmiotu zainteresowań nauki o informacji, dokonano przeglądu sposobów definiowania informacji. Następnie scharakteryzowano główne teorie informacji, ukazano klasyfikacje informacji, jej cechy i funkcje oraz odniesiono się do traktowania informacji jako zasobu.

Część druga zawiera analizy dotyczące społeczeństwa informacyjnego. Są one skupione wokół jego genezy i etapów rozwoju, sposobów definiowania, cech i funkcji oraz zagrożeń i wyzwań towarzyszących temu społeczeństwu. Istotnym elementem są także rozważania poświęcone sztucznej inteligencji.

Trzecia część dotyczy zagrożeń i barier informacyjnych. Otwiera ją ogólna charakterystyka zagrożeń dla bezpieczeństwa informacyjnego. Następnie ukazano – jako szczególne kategorie zagrożeń – przestępstwa informacyjne i dezinformację. W końcowych partiach tej części monografii zawarto rozważania dotyczące walki oraz wojny informacyjnej, a także analizy poświęcone barierom informacyjnym.

Monografię zamykają rozważania dotyczące pojmowania bezpieczeństwa informacyjnego i bezpieczeństwa informacji oraz towarzyszących im polityk (polityki bezpieczeństwa informacyjnego oraz polityki bezpieczeństwa informacji).

Słowa kluczowe: *bezpieczeństwo informacyjne, zagrożenia bezpieczeństwa informacyjnego, polityka bezpieczeństwa informacyjnego, społeczeństwo informacyjne*

Abstract

Fundamentals of information security

The monograph is the result of research on theoretical issues of information security. Their main goal was to verify the existing arrangements in relation to fundamental concepts relating to the essence of this security dimension and to present author's proposals in this regard.

The first part of the book is devoted to the ways of understanding information and showing its meaning. Within it, the methods of defining information were reviewed against the background of the characteristics of the subject of interest of information science.

Then, the main theories of information were characterized, the classification of information, its features and functions were presented, and the treatment of information as a resource was referred to.

The second part contains analyzes of the information society. They are focused on its origins and stages of development, ways of defining, features and functions, as well as threats and challenges accompanying this society. An important element is also consideration on artificial intelligence.

The third part deals with threats and information barriers. It opens with a general description of threats to information security. Then, it was shown as specific categories of threats: information crimes and disinformation.

The final parts of this part of the monograph contain considerations on fight and information warfare, as well as analyzes devoted to information barriers. The monograph ends with considerations on the understanding of information security and information security and the accompanying policies (information security policy and security policy of information).

Keywords: *information security, information security threats, information security policy, information society*

– Notatki –

– Notatki –