Daria KRZEWNIAK
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach[1]
Wydział Nauk Społecznych
Instytut Nauk o Bezpieczeństwie
daria.krzewniak@uph.edu.pl
ORCID 0000-0003-1085-8361
https://doi.org/10.34739/dsd.2021.01.11

NADZÓR I KONTROLA INTERNETU JAKO INSTRUMENT POLITYKI BEZPIECZEŃSTWA INFORMACYJNEGO WSPÓŁCZESNYCH PAŃSTW

ABSTRAKT: Informacja we współczesnym świecie stanowi zasób strategiczny, decydujący o przewadze konkurencyjnej państw na arenie międzynarodowej. Dążąc do zapewnienia właściwej jakości posiadanych zasobów informacyjnych oraz procesów i mechanizmów ich pozyskiwania, przetwarzania i ochrony, poszczególne państwa opracowują i wdrażają politykę bezpieczeństwa informacyjnego. Realizacji tej polityki służą różnorodne instrumenty, wśród których na uwagę zasługują nadzór i kontrola Internetu. Celem artykułu jest omówienie nadzoru i kontroli Internetu jako instrumentu polityki bezpieczeństwa informacyjnego, z uwzględnieniem specyfiki państw demokratycznych oraz totalitarnych i autorytarnych. Na potrzeby badań posłużono się metodą analizy literatury przedmiotu oraz metodą syntezy. Dowiedziono, że niezależnie od reżimu politycznego podmioty państwowe wykorzystują nadzór i kontrolę Internetu, zasadnicze cele tych działań są natomiast odmienne. W państwach demokratycznych chodzi przede wszystkim o ochronę i obronę cenionych społecznie wartości i dóbr, w państwach totalitarnych i autorytarnych zaś o realizację partykularnych interesów osób sprawujących władzę.

SŁOWA KLUCZOWE: informacja, bezpieczeństwo informacyjne, polityka bezpieczeństwa informacyjnego, nadzór, kontrola, cenzura

SUPERVISION AND CONTROL OF THE INTERNET AS AN INSTRUMENT OF THE INFORMATION SECURITY POLICY IN CONTEMPORARY STATES

ABSTRACT: Information in the modern world is a strategic resource that determines the competitive advantage of countries on the international arena. To ensure the appropriate quality of the information resources held as well as the processes and mechanisms of their acquisition, processing, and protection, individual countries develop and implement an information security policy. The implementation of this policy is supported by various instruments, among which the supervision and control of the Internet deserve attention. The aim of the article is to discuss the supervision and control of the Internet as an instrument of information security policy, considering the specificity of democratic, totalitarian, and authoritarian states. For the purposes of the research, the method of analyzing the literature and the method of synthesis were used. It has been proven that, regardless of the political regime, state-owned entities use Internet supervision and control, while the main

[1] Siedlce University of Natural Sciences and Humanities; Poland.

objectives of these activities are different. In democratic countries, it is primarily for the protection and defense of cherished social values and goods, in totalitarian and authoritarian countries for the realization of the particular interests of those in power.

KEYWORDS: information, information security, information security policy, supervision, control, censorship

WPROWADZENIE

Rozwój technologii informacyjno-komunikacyjnych stał jednym z najważniejszych czynników rozwoju społeczeństwa XXI wieku. Nowe technologie umożliwiają gromadzenie, przetwarzanie i przechowywanie olbrzymiej ilości informacji o zróżnicowanym charakterze. Wymaga to stworzenia właściwe prosperującego systemu bezpieczeństwa informacyjnego, które współcześnie traktowane jest jako jeden z najistotniejszych wymiarów bezpieczeństwa narodowego.

Informacja zawsze stanowiła istotny element życia człowieka – jej posiadanie było warunkiem koniecznym dla utrzymania egzystencji. Zdobycie pożywienia musiało być przecież poprzedzone informacją, gdzie i w jaki sposób można je pozyskać, uniknięcie zagrożenia było bardziej prawdopodobne, jeśli człowiek dysponował informacją o możliwości jego wystąpienia itd. Wraz z rozwojem naukowo-technologicznym i rozwojem intelektualnym człowieka katalog zapotrzebowań na informację znacząco się powiększał. Jak podaje W. Krztoń, „Człowiek zawsze poszukiwał informacji o warunkach i sposobach stwarzania i ułatwiania sobie lepszego życia oraz zaspokajania potrzeb duchowych. W miarę intelektualnego rozwoju i politechnizacji życia informacje zaczęły nabierać coraz większej wartości. Ich posiadanie stało się warunkiem lepszej i bezpieczniejszej egzystencji”[2].

Znaczenie informacji znacząco wzrosło w latach 70. XX wieku, kiedy zaliczono ją do zasobów – obok ziemi, środków finansowych oraz pracy[3]. Dodatkowo, w gospodarce rynkowej okazało się, że informacja stanowi jeden z najważniejszych towarów – dobro ekonomiczne będące źródłem przewagi konkurencyjnej. Aktualnie każdy wymiar państwa w coraz większym stopniu opiera się na obiegu informacji. W głównej mierze uzależnione są od niego gospodarka, energetyka, system finansowy, transport, środki masowego przekazu oraz wojsko[4]. Informacja jest także postrzegana jako produkt, wyrób czy usługa[5]. W związku z tym współczesne państwa dużą wagę przykładają do zapewnienia właściwej ochrony informacji pozostających w ich dyspozycji, jak również zagwarantowania odpowiednich standardów ich generowania, gromadzenia, przekazywania, przetwarzania, udostępniania, interpretacji czy wykorzystywania. Szczegółowy opis środków i procedur w tym względzie zawiera polityka bezpieczeństwa informacyjnego, która w perspektywie długoterminowej ukierunkowana jest na budowanie autorytetu, przewagi

[2] W. Krztoń, *Walka o informację w cyberprzestrzeni w XXI wieku*, Warszawa 2017, s. 33.
[3] B. Stefanowicz, *Informacja*, Warszawa 2004, s. 78.
[4] W. Krztoń, *Walka o informację…*, op. cit.
[5] Vide: J. Oleński, *Ekonomika informacji*, Warszawa 2001, s. 246–284.

i konkurencyjności kraju na arenie międzynarodowej. Informacja bowiem stanowi obecnie istotny czynnik decydujący o supremacji państwa.

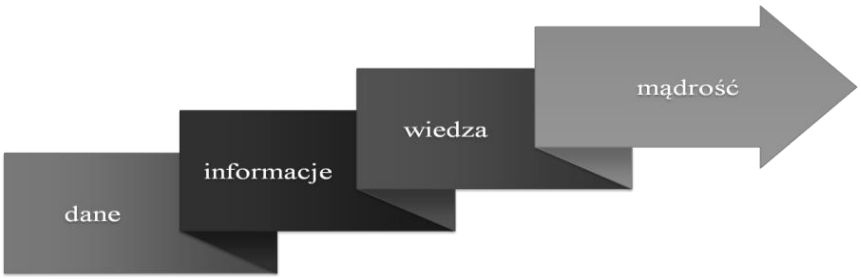
W kontekście powyższego zakłada się, że ważny instrument polityki bezpieczeństwa informacyjnego stanowi nadzór i kontrola. Celem artykułu jest zatem omówienie nadzoru i kontroli Internetu jako instrumentu polityki bezpieczeństwa informacyjnego, z uwzględnieniem specyfiki państw demokratycznych oraz totalitarnych i autorytarnych. Na potrzeby badań posłużono się metodą analizy literatury przedmiotu oraz metodą syntezy.

INFORMACJA, BEZPIECZEŃSTWO INFORMACYJNE I POLITYKA BEZPIECZEŃSTWA INFORMACYJNEGO W UJĘCIU TEORETYCZNYM

Wielość wymiarów i kontekstów, w których analizowana może być informacja, utrudnia uchwycenie istoty tego zagadnienia. W ujęciu etymologicznym termin „informacja" z łac. „informatio" znaczy tyle, co wyobrażenie, wyjaśnienie, zawiadomienie[6], w ujęciu słownikowym zaś – „powiadomienie o czymś, zakomunikowanie czegoś; wiadomość, wskazówka, pouczenie […]"[7] lub „wiadomość, wieść, nowinę, rzecz zakomunikowaną, zawiadomienie, komunikat; pouczenie, zakomunikowanie o czymś, dane […]"[8]. Pojęcie to należy do terminów bardzo często używanych zarówno w mowie potocznej, jak i na gruncie naukowym. W języku codziennym słowo „informacja" pojawia się zamiennie z takimi pojęciami jak: dane, wiadomość, wieść, wiedza, zawiadomienie, nowina, pouczenie itp., co wynika m.in. z faktu, że dotychczas na gruncie naukowym nie wypracowano jednoznacznej definicji omawianego terminu, ujmującej całość form i sposobów jego występowania. Informacja stanowi bowiem obiekt dociekań naukowych specjalistów wielu różnych dziedzin i dyscyplin, stąd też konstruowane są liczne ujęcia definicyjne tego pojęcia oraz rozwijane różnorodne teorie podejmujące próbę wyjaśnienia jego istoty.

Na potrzeby niniejszego artykułu przyjęto rozumienie informacji, zgodnie z którym jest to „każdy czynnik zmniejszający stopień niewiedzy (nieokreśloności) o badanym zjawisku, umożliwiający człowiekowi, organizmowi żywemu lub urządzeniu automatycznemu polepszenie znajomości otoczenia i sprawniejszy sposób przeprowadzenia celowego działania"[9]. Dodatkowo, za M. Wrzoskiem przyjęto założenie, że informacja stanowi etap pośredni pomiędzy danymi a wiedzą, nad którą dominuje mądrość (rysunek 1).

[6] W. Doroszewski (red.), *Słownik języka polskiego*, t. 3, Warszawa 1964, s. 203.
[7] M. Szymczak (red.), *Słownik języka polskiego*, t. 1., Warszawa 1978, s. 788.
[8] W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Warszawa 1989, s. 229.
[9] *Encyklopedia powszechna PWN*, t. 2, Warszawa 1974, s. 281.



Rysunek 1. Hierarchia informacji,
Źródło: opracowanie własne na podstawie: M. Wrzosek, *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, Warszawa 2010, s. 30.

Wspomniany autor mianem danych określa uporządkowany zbiór nazw i wartości liczbowych charakteryzujących określony obiekt (system, proces, zdarzenie). W jego opinii informacje zaś to zbiór danych uporządkowanych adekwatnie do potrzeb użytkownika, wyrażających jego potencjalne bądź realne działanie. Wiedza natomiast – według M. Wrzoska – to zbiór informacji wykorzystywanych przez tegoż użytkownika stosowanie do wymogów wynikających z podejmowanych aktywności, podczas gdy mądrość jest wiedzą umożliwiającą użytkownikowi realizację założonych celów zgodnie z przyjętym systemem wartości[10]. W tym rozumieniu dane, zapisywane w postaci symboli i sygnałów, uzewnętrzniają właściwości systemów, procesów i zdarzeń w celu uchwycenia stanu rzeczywistego. Pochodną danych jest natomiast informacja, pochodną informacji – wiedza. Istota tej ostatniej sprowadza się do syntezy doświadczenia i informacji, zweryfikowanej przez dyskusje, eksperymenty, krytykę przy wsparciu odpowiednich instytucji (np. szkoły). Celem wiedzy jest nabycie i kształtowanie umiejętności, zdobycie doświadczenia, uczenie się i samodoskonalenie ukierunkowane na podnoszenie poziomu i jakości życia ludzi oraz kreowanie lub zwiększanie wartości, np. organizacji. Informacja jest zatem wynikiem ludzkiej interpretacji, podczas gdy wiedza wykracza poza informację, ponieważ zawiera elementy uczenia się. Poziomem najwyższym jest natomiast mądrość rozumiana jako obszerna wiedza i doświadczenie w określonej kwestii. Powstaje wtedy, gdy człowiek poznał oraz zrozumiał zasadnicze wzorce wiedzy i potrafi je wykorzystać w różnorodnych sytuacjach.

Informacja stanowi niewyczerpalny zasób o zróżnicowanym charakterze i postaci. Może być powielana i przenoszona w czasie oraz przestrzeni, jej przetwarzanie zaś nie powoduje zużycia czy zniszczenia. Przy łącznym rozpatrywaniu kilku informacji osiąga się większy efekt aniżeli przy rozpatrywaniu pojedynczych kwestii (tzw. efekt synergii). Ta sama informacja ma różne znaczenie dla różnych użytkowników, a ponadto uzależniona jest od kontekstu, czyli słów poprzedzających ją i następujących po niej[11].

Informacja, jak każdy zasób, posiada pewne cechy, które pozwalają na optymalne jej wykorzystanie. Do cech umożliwiających określenie jakości i przydatności informacji zalicza się: aktualność, powiązanie z czasem przyszłym bez jednoczesnej utraty związku z teraźniejszością,

[10] M. Wrzosek, *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, Warszawa 2010, s. 30.
[11] J. Kisielnicki, H. Sroka, *Systemy informacyjne biznesu*, Warszawa 2005, s. 14.

zrozumiałość dla odbiorcy, operatywność, dokładność oraz wiarygodność. Rzetelna, zgodna z prawdą, dostarczona terminowo informacja stanowi często zasób strategiczny, decydujący o przewadze nad innymi podmiotami (ludźmi, grupami społecznymi, państwami itd.). Obok dostarczania danych na określony temat spełnia szereg innych funkcji. Do najważniejszych należą:

- funkcja modelowania – stanowi model rzeczywistości, jest miarą jej złożoności i różnorodności,
- funkcja decyzyjna – motywuje do osiągania założonych celów, uruchamia i wspiera proces decyzyjny,
- funkcja sterująca – wyznacza kierunek zachowania i działania podmiotu otrzymującego informacje,
- funkcja kapitałotwórcza – obok ziemi, kapitału oraz pracy,
- funkcja konsumpcyjna – jest towarem, który podlega transakcjom kupna-sprzedaży,
- funkcja kulturotwórcza – stanowi istotny czynnik rozwoju kulturalnego społeczeństwa,
- funkcja demokratyzująca – umożliwia podejmowanie decyzji o charakterze politycznym i prawnym,
- funkcja rozwoju wiedzy – jest elementem procesu prowadzącego do osiągnięcia przez podmiot mądrości[12].

Aby informacja spełniała należycie swoje funkcje, musi cechować się wysoką jakością. Za K. Lidermanem można przyjąć, że jakość informacji uzależniona jest przede wszystkim od następujących kryteriów:

- dokładność – precyzyjność informacji, dopasowanie do poziomu wiedzy jej użytkownika,
- aktualność – zmiana informacji następująca równolegle ze zmianą przedmiotu opisu,
- kompletność – ilość i stopień szczegółowości informacji odpowiadające wymogom postawionym przez jej użytkownika,
- spójność – odniesienie informacji do jednego obszaru tematycznego, jednolita forma prezentacji i przedstawiania ich, a także brak sprzeczności pomiędzy poszczególnymi fragmentami informacji,
- odpowiedniość formy – sposób prezentacji informacji, która minimalizuje jej błędną interpretację,
- wiarygodność – informacja w sposób rzetelny odzwierciedlająca niesiony przez siebie przekaz[13].

Z kolei K. Kolegowicz stoi na stanowisku, że informacja, która jest użyteczna i wartościowa, pozwala przede wszystkim analizować i oceniać stan teraźniejszy lub stan w przyszłości. Umożliwia również dokonanie prawidłowej oceny związków i zależności pomiędzy czynnikami wewnętrznymi i zewnętrznymi a efektywnością działań podmiotu,

[12] W. Krztoń, *Walka o informację…*, op. cit., s. 46–47; K. Kolegowicz, *Wartość informacji a koszty jej przechowywania i ochrony*, [w:] R. Borowiecki, M. Kwieciński (red.), *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystywanie i ochrona (wybrane problemy teorii i praktyki)*, Zamykacze 2003, s. 60.
[13] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 18.

w rezultacie zaś sprzyja podejmowaniu trafnych decyzji oraz projektowaniu i wdrażaniu potencjalnych zmian kierunków działania[14]. Informacja wartościowa wspiera zatem procesy decyzyjne podmiotu, wzbogaca indywidualną wiedzę, a jednocześnie pozwala na budowanie więzi z otoczeniem i komunikowanie się z nim.

Tak ważna rola informacji w funkcjonowaniu człowieka i zbiorowości sprawia, że wszelkie procesy informacyjne (generowanie, gromadzenie, przechowywanie, przekazywanie, przetwarzanie, udostępnianie, interpretacja, wykorzystywanie) z jej udziałem powinny podlegać odpowiedniemu zabezpieczeniu. Równie istotne jest także właściwe zorganizowanie:

- systemów, w których realizowane są procesy informacyjne,
- środowiska, w którym systemy te działają,
- personelu, który korzysta z systemów informacyjnych,
- otoczenia formalno-prawnego kształtującego technologie informacyjne i procesy użytkowania informacji[15].

Wszystkie wymienione kwestie stanowią bowiem przedmiot bezpieczeństwa informacyjnego. Termin ten często stosowany jest zamiennie z pojęciami: „bezpieczeństwo informacji", „bezpieczeństwo komputerowe", „bezpieczeństwo sieciowe", „bezpieczeństwo telekomunikacyjne" czy „bezpieczeństwo danych". Przyjmuje się jednak, że pojęcie „bezpieczeństwo informacyjne" ma najszerszy zakres znaczeniowy z uwagi na fakt, iż obejmuje całokształt procesów od gromadzenia przez przetwarzanie, przesyłanie aż po wykorzystywanie i przechowywanie informacji w systemach informacyjnych.

Istota omawianego wymiaru bezpieczeństwa jest różnorodnie ujmowana w literaturze. W potocznym rozumieniu, często błędnie zawężanym, odnosi się wyłącznie do ochrony informacji niejawnych. Tak rozumiane pojęcie nie obejmuje wszystkich kwestii dotyczących znaczenia informacji w systemie bezpieczeństwa narodowego. Ogranicza się wyłącznie do aspektów funkcjonalnych wynikających z zapisów ustawy o ochronie informacji niejawnych. Natomiast „wzrost znaczenia informacji powoduje, że wąskie, jednoaspektowe ujęcie bezpieczeństwa informacyjnego jest niewystarczające dla zapewnienia bezpieczeństwa narodowego"[16].

Przykładem wąskiego rozumienia tego pojęcia jest definicja zaproponowana przez P. Potejko. Jego zdaniem istota bezpieczeństwa informacyjnego sprawdza się do przekonania o konieczności ochrony wszelkiego rodzaju informacji treściowych oraz parametrów technicznych, jak kody dostępu, konfiguracji komputerów itp., mających znaczenie dla właściwego funkcjonowania poszczególnych sektorów gospodarek narodowych[17]. W szerokim zaś ujęciu, przedstawionym przez W. Fehlera, bezpieczeństwo to należy rozumieć jako „proces i stan, w ramach których zapewniana jest swoboda dostępu, gromadzenia, przetwarzania i przepływu

[14] K. Kolegowicz, *Wartość informacji...*, op. cit., s. 61.
[15] S. Jarmoszko, *Bezpieczeństwo informacyjne a casus infosfery bezpieczeństwa,* [w:] M. Kubiak, R. Białoskórski (red.), *Informacyjne uwarunkowania współczesnego bezpieczeństwa*, Siedlce-Warszawa 2016, s. 42–43.
[16] P. Potejko, *Bezpieczeństwo informacyjne,* [w:] K. A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa. Wybrane problemy*, Warszawa 2009, s. 209.
[17] Ibidem, s. 194.

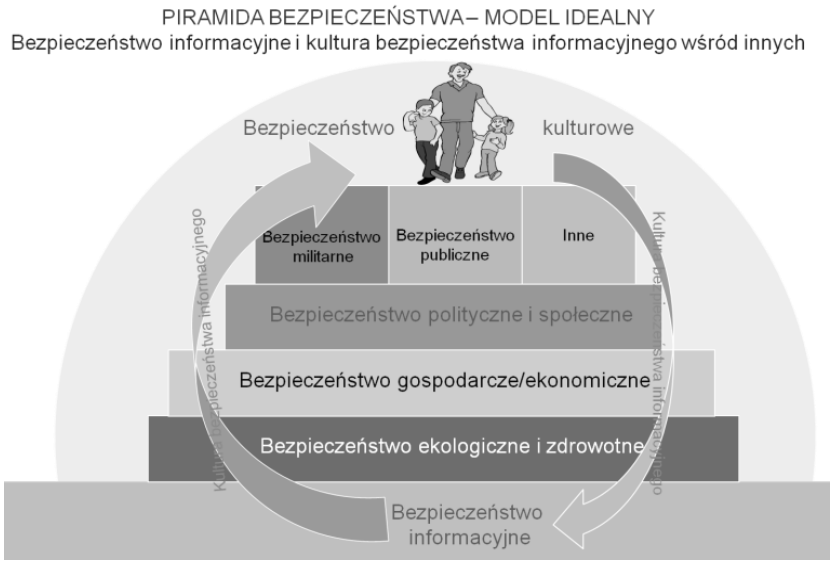
wysokiej jakości informacji (osiąganej przez merytoryczną selekcję) połączone z racjonalnym, prawnym i zwyczajowym wyodrębnieniem kategorii podlegających ochronie lub reglamentacji, ze względu na bezpieczeństwo podmiotów, których one dotyczą”[18]. Ten sposób rozumienia omawianego terminu przyjęto na potrzeby niniejszego artykułu.

Bezpieczeństwo informacyjne charakteryzuje się określonymi atrybutami, wśród których istotne wydają się następujące:

- dostępność – zapewnienie możliwości autoryzowanego wykorzystania danych w określonym czasie, a także zapewnienie prawa dostępu do informacji publicznej oraz swobody obrotu informacją, dla której istotny jest zakaz stosowania cenzury prewencyjnej,
- poufność – zapewnienie, że informacja nie jest udostępniona lub ujawniona nieuprawnionym podmiotom lub procesom,
- użyteczność – zapewnienie możliwości wykorzystania informacji przez podmiot, który nią dysponuje,
- integralność danych – zapewnienie, że dane nie zostały w sposób nieautoryzowany zmienione lub zniszczone,
- integralność systemu – zapewnienie, że system urzeczywistnia swoje funkcje w sposób nienaruszony, wolny od przypadkowej lub celowej manipulacji,
- integralność – zapewnienie integralności danych i systemu,
- autentyczność – zapewnienie, że tożsamość podmiotu/zasobu jest zgodna z deklarowaną,
- rozliczalność – zapewnienie, że działania podmiotu mogą być w sposób jednoznaczny przypisane jedynie temu podmiotowi,
- niezawodność – zapewnienie o spójnych, zamierzonych zachowaniach i skutkach[19].

W odniesieniu do innych przedmiotowych wymiarów bezpieczeństwa, bezpieczeństwo informacyjne stanowi obszar bazowy, a w rezultacie – strategiczny. Uwagę na ten fakt zwraca m.in. M. Cieślaczyk, przedstawiając tę kwestię w sposób graficzny w postaci piramidy bezpieczeństwa (rysunek 2).

[18] W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*, [w:] M. Kubiak, S. Topolewski (red.), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce–Warszawa 2016, s. 29–30.
[19] Vide: PN-ISO/IEC 27001:2007, *Technika informatyczna – Technika bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, Warszawa 2007, s. 9; W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*, op. cit., s. 30–32; W. Krztoń, *Walka o informację…*, op. cit., s. 76.



Rysunek 2. Piramida bezpieczeństwa,
Źródło: M. Cieślarczyk, referat pt. „Między teorią a praktyką bezpieczeństwa i obronności" wygłoszony podczas VII Ogólnopolskich Warsztatów Metodologiczno-Dydaktycznych w Naukach o Bezpieczeństwie i w Naukach o Obronności nt. *Teoria oraz praktyka bezpieczeństwa i obronności*, Siedlce, 26–27 kwietnia 2018 r.

O bezpieczeństwie informacyjnym jako strategicznym elemencie systemu bezpieczeństwa narodowego można mówić wtedy, kiedy kluczowe zasoby informacyjne kraju nie są zagrożone, władze natomiast podejmują decyzje dotyczące spraw wewnętrznych i zewnętrznych państwa bazując na prawdziwych, sprawdzonych, wiarygodnych i aktualnych informacjach, proces ich przepływu zaś jest niezakłócony[20]. Ważną kwestią jest także prawne zagwarantowanie przez państwo bezpieczeństwa publicznych sieci teleinformatycznych, systemu ochrony informacji oraz ochrony danych osobowych obywateli, jak również przyznanie obywatelom prawa do prywatności. Istotny element bezpieczeństwa informacyjnego państwa stanowi zapewnienie, że w trakcie zbierania informacji o obywatelach i ich aktywnościach, instytucje państwowe i prywatne działają w granicach prawa, obywatele i ich przedstawiciele zaś (np. parlamentarzyści, media) mają możliwość dostępu do informacji na temat działalności władz.

Bezpieczeństwo informacyjne nie jest stanem stałym, ma charakter procesualny, w związku z czym utrzymanie pożądanego jego poziomu wiąże się z koniecznością permanentnego monitorowania, planowania i podejmowania odpowiednich działań zaradczych oraz sprzyjających rozwojowi podmiotu, którego dotyczy. W związku z tym konieczne jest zarządzanie bezpieczeństwem informacyjnym, obejmujące szereg uzupełniających się procesów:

- opracowanie polityki bezpieczeństwa informacyjnego,
- identyfikacja i analiza zagrożeń dla posiadanych zasobów,
- dobór odpowiednich zabezpieczeń minimalizujących ryzyko,
- monitorowanie procesu wdrożenia zabezpieczeń oraz ich ewaluacja,

[20] Vide: P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006, s. 74.

- opracowanie i wprowadzenie programu szkoleń w zakresie wdrożonych zabezpieczeń,
- wykrywanie i reagowanie na incydenty[21].

Jednym z istotnych elementów zarządzania bezpieczeństwem w wymiarze informacyjnym jest sporządzenie i wdrożenie polityki bezpieczeństwa informacyjnego. W. Krztoń podaje, że terminem tym określa się zbiór reguł i zasad obowiązujących podczas zbierania, przetwarzania, gromadzenia i wykorzystywania informacji[22]. Natomiast P. Potejko podkreśla, że polityka ta odnosi się do procesu korzystania z informacji, bez względu na metodykę ich przetwarzania, jak również do wszystkich systemów przetwarzania danych i informacji prowadzonych zarówno w sposób tradycyjny, jak i za pośrednictwem systemów teleinformatycznych. Ponadto, przywołany autor wskazuje, że dotyczy ona również zabezpieczenia technicznego i organizacyjnego pozwalającego utrzymać założony poziom ryzyka informacyjnego[23]. Na potrzeby niniejszego opracowania przyjęto natomiast definicję W. Fehlera, zgodnie z którą polityka bezpieczeństwa informacyjnego to „celowa i zorganizowana działalność danego podmiotu (państwa, korporacji, organizacji, instytucji itp.) ukierunkowana na tworzenie i utrzymywanie w optymalnym jakościowo kształcie własnych zasobów informacyjnych i mechanizmów ich użytkowania połączona z efektywną ochroną przed destrukcyjnym oddziaływaniem podmiotów konkurencyjnych, nieprzyjaznych czy wrogich”[24].

Realizacji polityki bezpieczeństwa informacyjnego służą różne instrumenty, wśród których wskazać można m.in. nadzór i kontrolę. Pojęcia te często stosowane są zamiennie, choć ich zakres treściowy znacząco się różni. J. Boć wskazuje, że kontrola stanowi proces przynależny do wszystkich dziedzin życia człowieka, a – co za tym idzie – jest także właściwa dla wszystkich przejawów działań zorganizowanych niezależnie od tego, czy „organizatorem objętych kontrolą stosunków społecznych, gospodarczych i politycznych, jest podmiot samorządowy, podmiot państwowy, podmiot społeczny czy obywatel jako człowiek prywatny”[25]. W ogólnym rozumieniu zaproponowanym przez E. Iserzona istota kontroli sprowadza się do sprawdzenia czegoś, zestawienia stanu faktycznego ze stanem wymaganym[26]. Nieco szerszą perspektywę przedstawia J. Starościak. Zgodnie z jego stanowiskiem „kontrola polega na obserwowaniu, ustalaniu czy wykrywaniu stanu faktycznego, porównywaniu rzeczywistości z zamierzeniami, występowaniu przeciw zjawiskom niekorzystnym i sygnalizowaniu jednostkom kompetentnym dokonanych spostrzeżeń – bez decydowania jednak o zmianie kierunku działania jednostki skontrolowanej”[27]. Według W. Dawidowicza natomiast „kontrolę można scharakteryzować jako działanie obejmujące zbadanie istniejącego stanu rzeczy, zestawienie tego, co istnieje, z tym, co być powinno, co przewidują odpowiednie wzorce czy normy postępowania, i sformułowanie na tej podstawie odpowiedniej oceny, w przypadku istnienia rozbieżności między stanem istniejącym a stanem

[21] W. Krztoń, *Walka o informację…*, op. cit., s. 86-87.
[22] Ibidem, s. 81.
[23] P. Potejko, *Bezpieczeństwo informacyjne*, op. cit., s. 206.
[24] W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*, op. cit., s. 33.
[25] J. Boć, *Kontrola prawna administracji*, [w:] J. Boć (red.), *Prawo administracyjne*, Wrocław 2010, s. 357.
[26] E. Iserzon, *Prawo administracyjne. Podstawowe instytucje*, Warszawa 1968, s. 174.
[27] J. Starościak, *Zarys nauki administracji*, Warszawa 1971, s. 356.

pożądanym, ustalenie przyczyn tych rozbieżności i sformułowanie zaleceń mających na celu wskazanie sposobów usunięcia niepożądanych zjawisk ujawnionych przez kontrolę"[28]. W przytoczonych definicjach omawiana kategoria w znacznej mierze została ujęta w sposób zbliżony. Bazując na powyższych treściach należy zatem stwierdzić, że kontrola odnosi się do następujących kwestii:

- ustalania stanu faktycznego określonej działalności/stanu w konkretnym czasie,
- oceny tej działalności/stanu poprzez zestawienie rzeczywistego obrazu z pierwotnymi, wyjściowymi założeniami odnoszącymi się do całości podejmowanej aktywności, procesu itp., jak również do poszczególnych ich fragmentów, etapów, pozwalających stwierdzić ich prawidłowość lub nieprawidłowość,
- rozpoznania w zakresie ewentualnych nieprawidłowości ze wskazaniem na podmiotowe (personalne) i przedmiotowe ich aspekty,
- sformułowania wniosków w zakresie możliwości podejmowania działań prewencyjnych ukierunkowanych na minimalizowanie wystąpienia nieprawidłowości w przyszłości.

Tak ujmowana kontrola nie wiąże się z podejmowaniem czynności władczych, których celem jest skorygowanie i naprawienie kontrolowanej działalności/stanu. Inaczej rzecz ma się w przypadku nadzoru, w którym kontrola łączy się z kompetencjami w zakresie władczej ingerencji wobec podmiotu nadzorowanego. Organ nadzorujący dokonuje nie tylko spostrzeżeń i oceny, lecz także współadministruje, jest odpowiedzialny za wyniki działalności organizatorskiej podmiotów poddanych oddziaływaniu nadzorczemu. Wskazuje na to chociażby stanowisko J. Starościaka, zgodnie z którym „tam, gdzie w grę wchodzi prawo obserwacji plus prawo wydawania poleceń będziemy mówili o nadzorze […]"[29], czy definicja zaproponowana przez W. Dawidowicza mówiąca, że „nadzór oznacza prawną możliwość wpływania na działalność podporządkowanych organów lub instytucji"[30].

Wiele podmiotów prywatnych[31] oraz instytucji państwowych (tj. administracja, służby specjalne, organy ścigania) sprawuje nadzór i kontrolę w Internecie, za jego pośrednictwem zdobywając wiedzę o obywatelach[32]. Zadaniem M. Juzy, „każdy z tych podmiotów wykorzystuje zgromadzoną wiedzę w realizacji swojej władzy, nawet jeśli nie wszystkie wyrażają wprost zamiar jej sprawowania"[33]. Na ogół mniejsze emocje pojawiają się w przypadku zbierania danych obywateli przez podmioty państwowe, np. w postaci spisów powszechnych, statystyk publicznych, rejestrów służby zdrowia czy ubezpieczalni, niż wtedy, kiedy czynią to podmioty prywatne. Państwa w zasadzie od zawsze gromadziły dane o członkach swoich społeczeństw, co służyło sprawowaniu

[28] W. Dawidowicz, *Zagadnienia ustroju administracji państwowej w Polsce*, Warszawa 1970, s. 34.
[29] J. Starościak, *Zarys nauki administracji*, op. cit., s. 357.
[30] W. Dawidowicz, *Zagadnienia ustroju…*, op. cit.
[31] Vide: Z. Bederna, T. Szadeczky, *Cyber espionage through Botnets*, „Security Journal" Vol. 33, 2020, s. 43–44.
[32] Vide: H. Abelson i in., *Keys under doormats: mandating insecurity by requiring government access to all data and communications*, „Journal of Cybersecurity", Vol. 1, Issue 1, 2015, s. 69.
[33] M. Juza, *Między wolnością a nadzorem. Internet w zmieniającym się społeczeństwie*, Warszawa 2019, s. 265.

władzy nad nimi albo dyscyplinie, czyli zarządzaniu obywatelami poprzez rozlokowywanie ich w określonych placówkach (np. w wojsku, w więzieniu) i regulowanie ich aktywności[34].

Przyczyn, dla których nadzór i kontrola podmiotów państwowych nie spotykają się zazwyczaj z ożywionymi protestami społecznymi, jest wiele, jednak najważniejsze są dwie. Po pierwsze, nadzór i kontrola, przynajmniej w krajach demokratycznych, mają charakter jawny, transparentny, uregulowany prawnie. Wiadomym jest, jaka instytucja ma uprawnienia do zbierania danych, jakie dane może zbierać i w jaki sposób je chroni. Po drugie zaś, obywatele domagają się często od podmiotów państwowych efektywnego zarządzania, udzielania różnego rodzaju świadczeń, wsparcia, sprawnej i adekwatnej reakcji w sytuacjach trudnych, a przede wszystkim – zapewnienia odpowiedniego poziomu bezpieczeństwa. Aby udźwignąć ciężar społecznych oczekiwań, państwa muszą dysponować danymi obywateli. Zapewnienie prawidłowego funkcjonowania społeczeństwa i państwa wymaga jednak tworzenia zrównoważonych środków bezpieczeństwa informacyjnego.

NADZÓR I KONTROLA INTERNETU W PAŃSTWACH DEMOKRATYCZNYCH

Człowiek jako istota społeczna, funkcjonująca w różnych zbiorowościach, szczególnie silnie ceni sobie przynależne prawa i wolności, zwłaszcza zaś prawo do prywatności, do ochrony swoich danych osobowych, ważna jest dla niego wolność i tajemnica komunikowania się czy dostęp do wiarygodnych, rzetelnych informacji. Są to fundamenty demokratycznego państwa, gwarantowane przez akty prawa międzynarodowego i uregulowania prawne na poziomie krajowym.

Kwestie dotyczące szeroko rozumianego nadzoru i kontroli obywateli, w tym zbierania danych czy inwigilacji, istniały znacznie wcześniej, jednak wraz z upowszechnieniem Internetu materia ta nabrała szczególnej wagi. Zapisy odnoszące się m.in. do konieczności poszanowania ww. praw i wolności odnaleźć można chociażby w Powszechnej Deklaracji Praw Człowieka z 10 grudnia 1948 r., Międzynarodowym Pakcie Praw Obywatelskich i Politycznych z dnia 16 grudnia 1966 r., Europejskiej Konwencji Praw Człowieka i Podstawowych wolności z dnia 4 listopada 1950 r., Traktacie o funkcjonowaniu Unii Europejskiej z dnia 25 marca 1957 r., Karcie Praw Podstawowych Unii Europejskiej z dnia 7 grudnia 2000 r. czy rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w spawie swobodnego przepływu takich danych.

W państwach demokratycznych ograniczanie praw i wolności człowieka i obywatela, ingerencja w określone sfery życia osobistego i publicznego członków społeczeństwa są dopuszczalne jedynie w określonych przypadkach[35]. Muszą wówczas zostać spełnione trzy zasadnicze warunki:

[34] Ibidem, s. 268.
[35] R. Połeć, *Podsłuch operacyjny a ochrona tajemnicy i wolności komunikowania się*, [w:] M. Borkowski, M. Stańczyk-Minkiewicz, I. Ziemkiewicz-Gawlik (red.), *Edukacja dla bezpieczeństwa. Wyzwania i zagrożenia XXI wieku. Cyberprzestrzeń a bezpieczeństwo jednostki*, Poznań 2013, s. 270. Vide np. Konstytucja Rzeczypospolitej Polskiej

- legalności – w postaci właściwej ustawowej podstawy prawnej na poziomie prawa krajowego,
- celowości – ze względu na ochronę bezpieczeństwa narodowego, dobrobytu gospodarczego kraju, ochronę porządku publicznego, ochronę środowiska, zdrowia i moralności lub ochronę praw i wolności innych osób itp.,
- konieczności ochrony celów w demokratycznym społeczeństwie, uwzględniająca zasadę proporcjonalności pomiędzy chronionym celem a zastosowanym do tej ochrony środkiem.

Podmioty państwowe, realizując przyjętą politykę bezpieczeństwa informacyjnego, mogą działać jedynie w granicach i na podstawie prawa, czyli realizować wyłącznie te aktywności, na które przepisy prawne im wyraźnie zezwalają. Obywatelom natomiast przysługuje prawo do posiadania wiedzy na temat zakresu i sposobu działania tych podmiotów, udzielonych im uprawnień władczych, szczególnie w kontekście granic dopuszczalnej ingerencji w sferę prywatności poszczególnych członków społeczeństwa. Kiedy na szali zostają postawione ważne dla ludzi wartości, jak zdrowie, bezpieczeństwo czy moralność, są oni skłonni oddać państwu część przysługujących im praw i wolności, o ile intencje państwa są czyste i jawne. Legitymizacja praktyk nadzorczych i kontrolnych, a także ich częsta akceptacja przez społeczeństwo, jest związana przede wszystkim ze zwiększającym się naciskiem na bezpieczeństwo, co w znacznej mierze jest reakcją m.in. na zamachy terrorystyczne z 11 września 2001 r. i kolejne.

Pewne formy nadzoru i kontroli, w tym m.in. w postaci cenzury, także prewencyjnej, są obecne w krajach powszechnie uważanych za nowoczesne i demokratyczne. Zapewnienie bezpieczeństwa obywatelom wymaga monitorowania Internetu przez organy państwowe. Jest to konieczne chociażby ze względu na występujące tam przestępstwa przeciwko porządkowi publicznemu (np. publiczne propagowanie faszyzmu, nawoływanie do nienawiści, rozpowszechnianie lub publiczne prezentowanie treści mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym[36]), obyczajowości[37] czy moralności. Co więcej, w Internecie działa szara strefa sieciowa, w której swobodnie funkcjonują wszyscy ci, których celem jest ukrycie się przed czujnym okiem policji i innych służb odpowiedzialnych za bezpieczeństwo[38]. W tzw. darkwebie istnieją pewne niepisane, trudne do zaakceptowania zasady, sprzeczne z obowiązującymi normami społecznymi. Ta część wirtualnej przestrzeni – z uwagi na dużo większą anonimowość – wykorzystywana jest w znacznej mierze do działań niezgodnych w prawem. Wielu kryminalistów traktuje ją jako źródło zarobkowania. Znajdują się w niej oferty sprzedaży nielegalnych produktów (np. broni, narkotyków) i usług (np. fałszowanie paszportów, prawa jazdy). Znaczna część ofert w darkwebie to oszustwa – przestępcy czują się bezkarni, ponieważ istnieje niewielkie prawdopodobieństwo, że oszukana przez nich osoba zgłosi fakt wyłudzenia na policji. Darkweb jest także strefą, w której zrzeszają się i dyskutują na forach

z 2 kwietnia 1997 roku (Dz. U. z 1997 r., nr 78, poz. 483), Międzynarodowym Pakcie Praw Obywatelskich i Politycznych z dnia 16 grudnia 1966 r. (Dz. U. z 1977 r., nr 38, poz. 167).

[36] W Polsce: art. 256-264A ustawy z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. 1997 Nr 88 poz. 553 z późn. zm.).

[37] W Polsce: Ibidem, art. 200.

[38] Vide: M. Mirea, V. Wang, J. Jung, *The not so dark side of the darknet: a qualitative study*, „Security Journal" vol. 32/2019, s. 104–106.

hakerzy czy pedofile, a nawet terroryści (darkwebu używało Państwo Islamskie). Nie uwzględniają przy tym, że wszystkie najważniejsze służby wywiadowcze na świecie uważnie przyglądają się funkcjonowaniu tej sieci. Wynikiem ich działania było m.in. ujęcie Rossa Ulibrichta, znanego jako Dread Pirate Roberts, twórcy Silk Road – internetowej platformy aukcyjnej działającej w sieci Tor, zamkniętej w 2013 roku przez amerykańskie organy ścigania, zajmującej się handlem narkotykami. W przekazach medialnych głośno było również o schwytaniu szeregu pedofilów, w tym Matthew Grahama, ukrywającego się pod pseudonimem Lux, założyciela PedoEmpire – serwisu dla pedofilów, na którym nie tylko dyskutowano i wymieniano się wiedzą i doświadczeniami o tym, w jaki sposób obezwładniać dzieci, żeby poddawały się czynnościom seksualnym, lecz także przesyłano amatorskie filmy pornograficzne z udziałem nieletnich, nagrywane przez użytkowników serwisu[39].

Współczesne państwa często wykorzystują nowinki techniczne i technologiczne, które z jednej strony przyczyniają się do zapewnienia społeczeństwu bezpieczeństwa, dobrobytu, odpowiednio wysokiego poziomu zdrowia itd., z drugiej zaś ingerują w prywatność obywateli. Przykładem może być Echelon – najpotężniejszy system podsłuchowy na świecie. „To amerykański superszpieg, który analizuje rozmowy telefoniczne, smsy, maile, bilingi, wypłaty z bankomatów, cały ruch internetowy, wszystko, co przeglądamy w sieci. Prawdopodobnie Echelon analizuje około 3 miliardów tego typu komunikatów na dobę! Superwydajne komputery mają zainstalowane słowniki, by na bieżąco tłumaczyć podsłuchiwane wiadomości, dokonywać selekcji i wyłapywać to, co wydaje się najciekawsze. Wyłapują komunikaty, które mogą być powiązane z organizacją zamachów terrorystycznych, politycznych morderstw, wielkoskalowej korupcji, działań karteli narkotykowych itp.”[40]. W pracach Echelonu uczestniczą także Wielka Brytania, Kanada, Australia i Nowa Zelandia[41]. System ten miał prawdopodobnie przyczynić się bezpośrednio do rozwiązania kontraktu pomiędzy europejskim Airbusem a Arabią Saudyjską, wartego 6 mln dolarów. Dzięki niemu przechwycono informacje, z których wynikało, że pracownicy Airbusa proponowali łapówki saudyjskim urzędnikom w zamian za wygranie przetargu[42].

Wszelka aktywność podmiotów państwowych jest pożądana, gdy koncentruje się na zapewnieniu właściwych warunków do bezpiecznego funkcjonowania obywateli – wówczas państwowy nadzór i kontrola nad obywatelami nie budzą żadnych wątpliwości. Obiekcje i zastrzeżenia pojawiają się zazwyczaj wtedy, gdy podmioty państwowe gromadzą informacje w niejasnych celach, wykraczając poza prawnie określone ramy oraz nie informując, jakie dane, o kim i po co gromadzą. Tymczasem rządy zbierają dziś olbrzymie ilości danych o członkach

[39] Ibidem, s. 106.
[40] K. Pyzia, *Ile oni wiedzą o tobie? Szpiedzy i podsłuchy w Polsce. Bruno Kowalsky w rozmowie z Krzysztofem Pyzią*, Warszawa 2019, s. 21–22.
[41] European Parliament, Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), s. 11, https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN (13.02.2021).
[42] K. Pyzia, Ile *oni wiedzą o tobie?...*, op. cit., 28.

swoich i obcych społeczeństw, nawet jeżeli w konkretnym czasie nie są w stanie ich wykorzystać czy chociażby przetworzyć, poniekąd „na wszelki wypadek", by mieć możliwość przeanalizowania aktywności poszczególnych osób, gdy padnie na nie jakieś podejrzenie. M. Juza wyraźnie zaznacza, że „wraz z zastosowaniem do analizy tych danych narzędzi *Big Data* otwiera to możliwość faktycznego karania pewnych osób za posiadanie określonych skłonności, zanim jeszcze zdążą one popełnić jakiekolwiek przestępstwo"[43].

Dane, które gromadzą i udostępniają serwisy internetowe na temat swoich użytkowników, są niezwykle cenne dla władzy państwowej, z różnych innych względów niż te, na które przyzwala prawo. Wyraźnie dowiodła tego tzw. afera PRISM, ujawniona w połowie 2013 r. przez Edwarda Snowdena – informatyka, byłego pracownika CIA i współpracownika amerykańskiego wywiadu. Stał się on tzw. sygnalistą (demaskatorem), który pomimo grożących mu konsekwencji, ujawnił opinii publicznej informacje na temat ogromnej skali inwigilacji elektronicznej prowadzonej przez służby specjalne. Wyjawił on, że PRISM to tajny program szpiegowski umożliwiający wywiadowi amerykańskiemu dostęp do danych użytkowników zgromadzonych na serwerach największych przedsiębiorstw internetowych, jak Google, Apple, Facebook, Microsoft, Yahoo, oraz wykorzystywanie ich na własnych użytek. W związku z tym, że wymienione serwisy funkcjonują na całym świecie, a prowadzone są przez amerykańskie przedsiębiorstwa, zbierano dane dotyczące obywateli różnych krajów[44]. Po ujawnieniu tego incydentu amerykański wywiad utrzymywał, że jego działania mieściły się w granicach prawa, ich celem zaś było zminimalizowanie ryzyka potencjalnych aktów terroru po wydarzeniach z września 2011 roku. Szeroko zakrojona inwigilacja nie przyczyniła się jednak do udaremnienia jakiegokolwiek zamachu terrorystycznego.

Tego rodzaju działania niewątpliwie zmniejszają zaufanie obywateli do państwa i jego organów, w tym zwłaszcza do posiadanych i realizowanych uprawnień władczych i kontrolnych. Podmioty państwowe mają obowiązek działać na rzecz i dla dobra obywateli, wszelkie aktywności przez nie podejmowane muszą być transparentne, zgodne zarówno z prawem naturalnym, jak i prawem stanowionym.

NADZÓR I KONTROLA INTERNETU W PAŃSTWACH TOTALITARNYCH I AUTORYTARNYCH

Kwestie praw człowieka, swobód obywatelskich w kontekście nadzoru i kontroli w Internecie zupełnie inaczej przedstawiają się w państwach totalitarnych i autorytarnych. Podczas gdy w Europie czy Stanach Zjednoczonych ograniczanie prawa do prywatności, swobody wypowiedzi w sieci czy prawa dostępu do aktualnej, wiarygodnej i rzetelnej informacji postrzegane są jako pogwałcenie podstawowych praw człowieka, równolegle funkcjonuje system, któremu pojęcia te są całkowicie

[43] M. Juza, *Między wolnością a nadzorem…*, op. cit., s. 268.
[44] Vide: Ibidem, s. 261–262; G. Greenwald, E. MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, „The Guardian" 7 czerwca 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (14.02.2021); S. Mainwaring, *Always in control? Sovereign states in cyberspaces*, „European Journal of International Security", Vol. 5(2)/2020, s. 216–217.

obce. Swobody obywatelskie i prawa człowieka, z których słyną i z których są dumne państwa demokratyczne, przez państwa totalitarne i autorytarne traktowane są jako źródło degrengolady moralnej.

Filozofia Wschodu na piedestale stawia dobru ogółu, często kosztem dobra jednostki. „Chiny, w imię zapewnienia bezpieczeństwa wewnętrznego, bezpieczeństwa narodowego czy ochrony wartości społecznych dysponują zoczonym systemem regulacji, które mają na celu zapobieganie publikowania w Internecie materiałów i treści uznawanych za nielegalne. Treści zamieszczane w sieci są filtrowane wielopłaszczyznowo, dzięki wykorzystaniu bardzo zaawansowanej i rozbudowanej infrastruktury technologicznej”[45]. Szczegółowe cele w tym zakresie przedstawiają zapisy Nakazu Rady Państwa nr 147, które stanowią: „zakaz używania Internetu przez osoby fizyczne w sposób:

- zagrażający bezpieczeństwu narodowemu,
- ujawniający tajemnice państwowe,
- szkodzący interesom państwa, społeczeństwa lub grupy społecznej,
- konstytuujący działalność przestępczą,
- zakazuje się również tworzenia, powielania, przekazywania informacji, które:
  a) prowokują nieposłuszeństwo wobec konstytucji, ustawy lub regulacji administracyjnych,
  b) nawołują do obalenia rządu lub systemu socjalistycznego,
  c) prowokują podziały kraju lub
  d) godzą w poczucie solidarności narodowej,
  e) nawołują do dyskryminacji pomiędzy tożsamościami regionalnymi lub naruszają ich jedność,
  f) przekłamują prawdę,
  g) szerzą plotki,
  h) zaburzają porządek społeczny,
  i) godzą w reputację kraju,
  j) gloryfikują przesądy feudalne,
  k) materiały o treściach wyraźnie seksualnych (pornografia), reklamujące hazard, przemoc lub morderstwo,
  l) rozpowszechniające terroryzm,
  m) nawołujące do działań przestępczych,
  n) obrażające, pomawiające innych ludzi”[46].

Niedostosowanie się do tych przepisów wiąże się z karą grzywny lub blokadą dostępu do Internetu przez określony czas. Równocześnie inne uregulowania prawne nakazują wszystkim internautom w Chinach przekazanie informacji na temat dostępu do sieci miejscowej jednostce policji w ciągu 30 dni od daty podpisania umowy o świadczenie usług internetowych

[45] J. Przyjemska, *Granice wolności słowa w Internecie w wybranych systemach prawnych*, [w:] A. Biłgorajski (red.), *Wolność wypowiedzi i jej granice. Analiza wybranych zagadnień*, Katowice 2014, s. 116.
[46] Ibidem, s. 116–177, za: J. Kulesza, *Międzynarodowe Prawo Internetu*, Poznań 2010, s. 258.

z dostawcą. Co więcej, powołano specjalne jednostki policji ds. przestępstw internetowych, do których zadań należy śledzenie zachowań użytkowników sieci celem badania naruszeń przepisów prawnych.

W państwach totalitarnych i autorytarnych często dochodzi do cenzurowania przez władzę treści zawartych w Internecie. Cenzura państwowa przybiera postać ingerencji bezpośredniej lub pośredniej – z wykorzystaniem różnorodnych sankcji, może mieć charakter prewencyjny lub post facto. Najczęściej przejawia się w następujących formach:

- techniczne utrudnianie dostępu do sieci polegające na całkowitym bądź częściowym jej zablokowaniu,
- penalizowanie korzystania z określonych internetowych kanałów przekazu bądź usług i/lub wprowadzanie zakazu udostępniania pewnych treści,
- tworzenie administracyjnych, finansowych oraz polityczno-społecznych barier dostępu do Internetu, np. poprzez wymóg rejestracji treści zamieszczanych w sieci, zawyżanie cen dostępu do Internetu czy hakowanie stron internetowych, a następnie blokowanie/ kasowanie ich zawartości oraz zastraszanie aktywnych użytkowników[47].

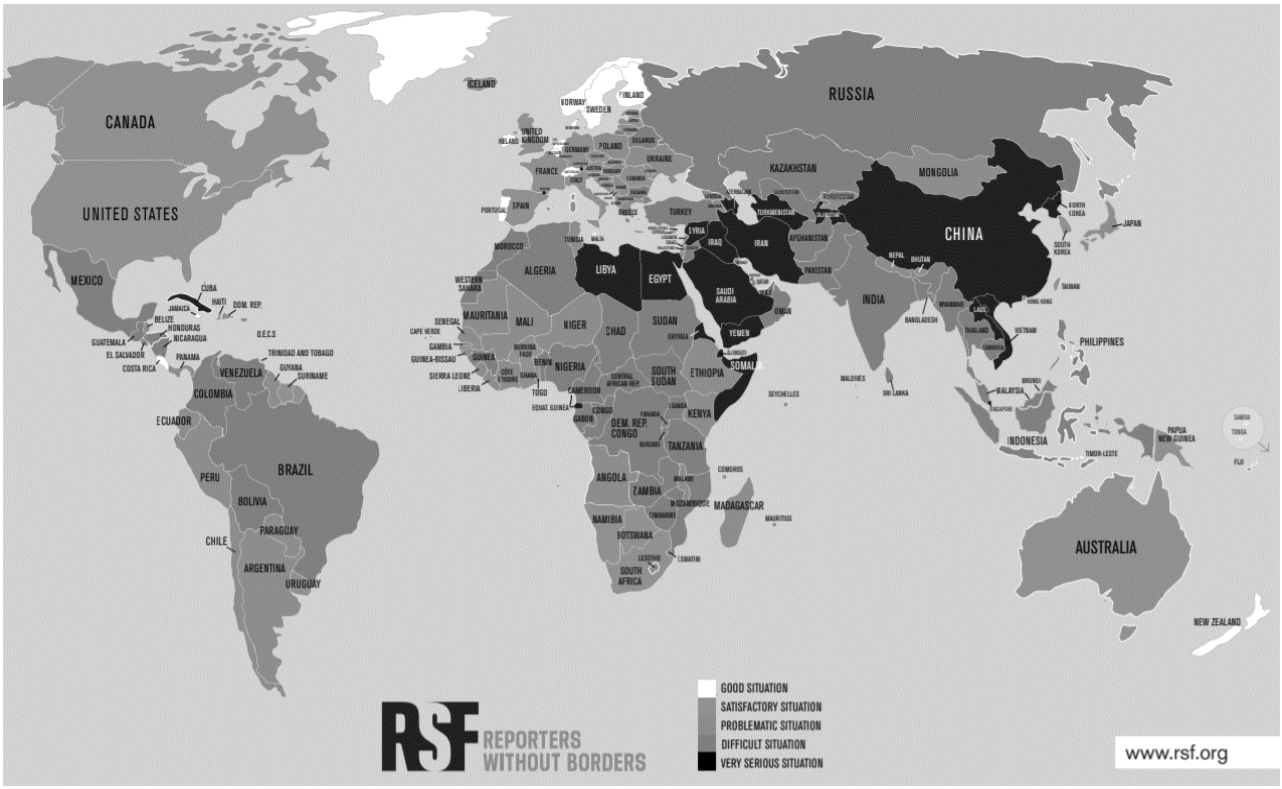
Istotnym wymiarem oceny aktywności internautów staje się nie tylko bezpieczeństwo kraju, utrzymanie tajemnic państwowych, lecz także zgodność z założeniami polityki państwa. Szczególnego znaczenia nabierają często kwestie gospodarcze. Blokowanie dostępu do pewnych treści ukierunkowane jest na dyskryminowanie produktów i usług świadczonych przez zagraniczne podmioty i umożliwienie rozwoju rodzimych przedsiębiorstw. Ma to miejsce m.in. w przypadku Chińskiej Republiki Ludowej. United States Trade Representative oponowała przeciwko chińskim restrykcjom w tym zakresie, wskazując, że stanowią one niedozwolone bariery w handlu. Do oskarżeń tych odniosła się Cyberspace Administration of China (CAC) – agencja rządowa odpowiedzialna za kontrolę sieci w Chinach. Stwierdziła ona, że: „Celem [chińskiego] systemu kontroli Internetu jest zagwarantowanie bezpieczeństwa i możliwości monitorowania produktów oraz usług informatycznych, zabezpieczenie informacji użytkowników, a także umocnienie ich poczucia bezpieczeństwa”[48]. Przedstawiciele tej instytucji podali również, że: „Chiny skrupulatnie przestrzegają zasad WTO [Światowej Organizacji Handlu – podkr. D.K.], oraz protokołów akcesyjnych, chronią interesy uczciwych przedsiębiorstw zagranicznych zgodnie z prawem, i tworzą dla nich uczciwe otoczenie rynkowe”[49].

Podobnie sytuacja wygląda w Korei Północnej. Mniej więcej co dwudziesty piąty obywatel tego kraju ma dostęp do Kwangmyong, czyli krajowej sieci internetowej, oferującej jedynie podstawowe usługi, jak poczta elektroniczna, wyszukiwarka internetowa oraz grupy dyskusyjne. Dostęp do globalnego Internetu ma wyłącznie najwęższe grono elity rządzącej.

[47] D. Mider, *Formy przemocy politycznej w Internecie – próba klasyfikacji*, „Annales Universitatis Mariae Curie-Skłodowska”, vol. XXII, 2 (2015), s. 37.
[48] E. Miranda, *Chinese Internet Regulator: The Great Firewall Not a ‘Trade Barrier’*, „Yibada”, 2016, http://en.yibada.com/articles/115714/20160412/chinese-internet--regulator-the-great-firewall-not-a-trade-barier.htm#ixzz49tAdiJPV (16.02.2021).
[49] Ibidem.

Iran jest kolejnym przykładem państwa, w którym władze dążą do wprowadzenia krajowej sieci. Dostęp do części usług i serwisów internetowych na terenie tego państwa jest zablokowany. Każda aktywność obywateli w sieci jest rejestrowana, krytyka władzy zaś spotyka się z jednoznaczną jej reakcją w postaci represji. Podobnie dzieje się w Wietnamie, gdzie odcięto użytkownikom dostęp m.in. do Google'a i Facebooka[50].

Chiny, Korea Północna czy Wietnam nie są jedynymi państwami, w których polityka bezpieczeństwo informacyjnego kreowana przez władzę sprowadza się do ograniczania aktywności użytkowników sieci i blokowania określonych usług. Poniższa ilustracja (rysunek 3) przedstawia światowy indeks wolności prasy w 2021 roku. Wolność prasy, dostęp do informacji jest oczywiście jedynie elementem bezpieczeństwa informacyjnego w ogóle, niemniej jednak rzuca pewne światło na podjętą problematykę.



Rysunek 3. Wolność prasy na świecie w 2021 roku według Reporterów bez Granic, Źródło: https://rsf.org/en/ranking/2020# (16.02.2021).

W wielu krajach na świecie polityka bezpieczeństwa informacyjnego sprzyjać ma realizacji partykularnych interesów podmiotów państwowych. Władze często przejmują i powielają schematy działań wdrożonych w Chinach, zwłaszcza w zakresie cenzury Internetu. Mowa tu chociażby o Filipinach, Kambodży i Indonezji. W Malezji czy Birmie funkcjonuje zakaz publikowania materiałów, które godziłyby w partię sprawującą władzę. Liberia blokuje

[50] P. Ładny**,** *Neutralność sieci – dogmat czy postulat*, „Nierówności Społeczne a Wzrost Gospodarczy", nr 1/2015, s. 335 i in.

treści o bliżej nieokreślonym antyliberyjskim wydźwięku. Władze Zimbabwe odcinają dostęp do zagranicznych serwisów internetowych, które „mogłyby budzić niepokój lub smutek”[51].

Trudno nie zgodzić się z J. Angwin, która pisze, że „rządy krajów na całym świecie – od Afganistanu po Zimbabwe – skwapliwie korzystają z technologii nadzoru, począwszy od sprzętu do masowego przechwytywania [*massive intercept*] po narzędzia, które pozwalają im zdalnie przejmować telefony i komputery ludzi”[52]. Do momentu, kiedy dostęp do komputerów nie był powszechny, sprawowanie nadzoru i kontroli nad aktywnością obywateli w sieci było kosztowne i trudne. Władze gromadziły dane wyłącznie w pewnych określonych okolicznościach, jak narodziny, śmierć, zawarcie związku małżeńskiego czy zakup nieruchomości. Rozwój nowych technik i technologii sprawił, że gromadzenie różnorodnych danych i informacji o członkach społeczeństwa stało się stosunkowo tanie i łatwe. Państwa zaś – głownie totalitarne i autorytarne, ale w pewnym zakresie również demokratyczne – skwapliwie wykorzystują ten fakt w celu realizacji nie tyle racji stanu, ile pozyskiwania korzyści przez osoby sprawujące władzę.

PODSUMOWANIE

Szybki dostęp do wielu informacji oraz wolność słowa nigdy nie były tak powszechne i możliwe do praktycznego zastosowania na szeroką skalę, jak z chwilą rozpowszechnienia Internetu. Rządy państw starają się tę swobodną wymianę danych i informacji nadzorować i kontrolować, uzasadniając koniecznością ochrony dobra wspólnego w postaci bezpieczeństwa, wartości demokratycznych, moralności czy prawa własności intelektualnej. Ponadto, władza – w różnorodnych okolicznościach i ze względu na liczne uwarunkowania – gromadzi i przechowuje rozmaite informacje na temat swoich obywateli. Może to prowadzić do nadużyć, na co wskazuje m.in. D. Mider, pisząc: „Groźba ujawnienia lub wykorzystania naszych prywatnych, często intymnych spraw, w tym korespondencji z najbliższymi, aktywności, w których chcielibyśmy pozostawać anonimowi, jawi się jako potężne narzędzie władzy w rękach instytucji państwa posiadających takie informacje na temat jednostek. Utrzymywanie takiej asymetrii może być rozpatrywane w kategoriach krzywdy – nadmierna, nieuzasadniona wiedza państwa o obywatelu to potencjalne narzędzie represji i wymuszania posłuszeństwa”[53]. Historia dostarcza wielu przykładów niewłaściwego, niezgodnego z prawem wykorzystania przeciwko obywatelom newralgicznych informacji pozostających w dyspozycji władz państwowych. Każdy przejaw tego rodzaju aktywności należy traktować jako ważny sygnał ostrzegawczy dotyczący naruszenia praw i wolności człowieka i obywatela. Jednocześnie warto mieć na uwadze fakt, iż władza, dążąc do wypełniania przypisanych jej zadań, ról i funkcji, musi posiadać szereg informacji o swoich obywatelach.

[51] J. Przyjemska, *Granice wolności słowa w Internecie…*, op. cit., s. 118.
[52] J. Angwin, *Społeczeństwo nadzorowane. W poszukiwaniu prywatności, bezpieczeństwa i wolności w świecie permanentnej inwigilacji*, Warszawa 2019, s. 11.
[53] D. Mider, *Formy przemocy politycznej w Internecie…*, op. cit.

W państwach demokratycznych obywatele mają zagwarantowane prawo do ochrony danych osobowych, prawo dostępu do wiarygodnych, rzetelnych informacji czy wolność słowa. Polityka bezpieczeństwa informacyjnego w państwach demokratycznych z założenia ma służyć suwerenowi, państwu i jego bezpieczeństwu we wszystkich wymiarach, w krajach autorytarnych oraz totalitarnych natomiast koncentruje się na realizacji i ochronie interesów osób będących u władzy, na utrzymaniu „w ryzach" społeczeństwa i zapobieganiu wszelkiej kontestacji władzy i niezadowoleniu społecznemu. Dobro wspólne schodzi na drugi plan, kwestią najistotniejszą jest realizacja partykularnych interesów elit rządzących. Wydaje się zatem, że większość działań podmiotów państwowych podejmowanych wobec użytkowników sieci w państwach demokratycznych ma charakter kontrolny ukierunkowany na zapewnienie m.in. bezpieczeństwa personalnego i strukturalnego, w państwach autorytarnych i totalitarnych natomiast – nadzorczy, ingerujący bezpośrednio lub pośrednio w aktywność obywateli w sieci oraz przynależne im prawa i wolności.

BIBLIOGRAFIA

MONOGRAFIE I OPRACOWANIA

Angwin Julia. 2019. Społeczeństwo nadzorowane. W poszukiwaniu prywatności, bezpieczeństwa i wolności w świecie permanentnej inwigilacji. Warszawa: PWN.

Bączek Piotr. 2006. Zagrożenia informacyjne a bezpieczeństwo państwa polskiego. Toruń: Wydawnictwo Adam Marszałek,

Dawidowicz Wacław. 1970. Zagadnienia ustroju administracji państwowej w Polsce. Warszawa: PWN.

Doroszewski Witold Red. 1964. Słownik języka polskiego. Tom 3.Warszawa: PWN.

Encyklopedia powszechna PWN. 1974. Tom 2. Warszawa: PWN.

Iserzon Emanuel. 1968. Prawo administracyjne. Podstawowe instytucje. Warszawa: Wydawnictwo Prawnicze.

Juza Marta. 2019. Między wolnością a nadzorem. Internet w zmieniającym się społeczeństwie. Warszawa: Wydawnictwo Naukowe SCHOLAR.

Kisielnicki Jerzy, Sroka Henryk. 2005. Systemy informacyjne biznesu. Warszawa: Agencja Wydawnicza „Placet".

Kopaliński Władysław 1989. Słownik wyrazów obcych i zwrotów obcojęzycznych. Warszawa: Wiedza Powszechna.

Krztoń Waldemar. 2017. Walka o informację w cyberprzestrzeni w XXI wieku. Warszawa: Wydawnictwo Rambler.

Kulesza Joanna. 2010. Międzynarodowe Prawo Internetu. Poznań: ARS BONI ET AEQUI.

Liderman Krzysztof. 2012. Bezpieczeństwo informacyjne. Warszawa: PWN.

Oleński Józef. 2001 Ekonomika informacji. Warszawa: PWE.

Pyzia Krzysztof. 2019. Ile oni wiedzą o tobie? Szpiedzy i podsłuchy w Polsce. Bruno Kowalsky w rozmowie z Krzysztofem Pyzią. Warszawa: Prószyński i S-ka.

Starościak Jerzy. 1971. Zarys nauki administracji. Warszawa: PWN.

Stefanowicz Bogdan. 2004. Informacja. Warszawa: Oficyna Wydawnicza SGH.

Szymczak Mieczysław Red. 1978. Słownik języka polskiego Tom 1. Warszawa: PWN.
Wrzosek Marek. 2010. Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną. Warszawa: AON.

ROZDZIAŁY W MONOGRAFIACH

Boć Jan. 2010. Kontrola prawna administracji. W Prawo administracyjne, s. 355–412. Kolonia Lomited.
Fehler Włodzimierz. 2016. O pojęciu bezpieczeństwa informacyjnego. W Bezpieczeństwo informacyjne w XXI wieku. Siedlce–Warszawa: Wydawnictwo UPH w Siedlcach, s. 25–44.
Jarmoszko Stanisław. 2016. Bezpieczeństwo informacyjne a casus infosfery bezpieczeństwa. W Informacyjne uwarunkowania współczesnego bezpieczeństwa, s. 36–64. Wydawnictwo UPH w Siedlcach.
Kolegowicz Krzysztof. 2016. Wartość informacji a koszty jej przechowywania i ochrony. W Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystywanie i ochrona (wybrane problemy teorii i praktyki), s. 54–69. Kantor Wydawniczy Zamykacze.
Połeć Rafał. 2013. Podsłuch operacyjny a ochrona tajemnicy i wolności komunikowania się. W Edukacja dla bezpieczeństwa. Wyzwania i zagrożenia XXI wieku. Cyberprzestrzeń a bezpieczeństwo jednostki, s. 269–282. Wydawnictwo Wyższej Szkoły Bezpieczeństwa.
Potejko Piotr. 2009. Bezpieczeństwo informacyjne. W Bezpieczeństwo państwa. Wybrane problemy, s. 208–215. Oficyna Wydawnicza ASPRA-JR.
Przyjemska Joanna. 2014. Granice wolności słowa w Internecie w wybranych systemach prawnych. W Wolność wypowiedzi i jej granice. Analiza wybranych zagadnień, s. 106–119. Wydawnictwo Uniwersytetu Śląskiego.

ARTYKUŁY W CZASOPISMACH

Abelson Harold et al. 2015. „Keys under doormats: mandating insecurity by requiring government access to all data and communications". Journal of Cybersecurity Vol. 1, Issue 1, 2015: s. 69–79.
Bederna Zsolt, Szadeczky Tomas. 2020. „Cyber espionage through Botnets". Security Journal vol. 33: s. 43–62.
Ładny Piotr. 2015. „Neutralność sieci – dogmat czy postulat". „Nierówności Społeczne a Wzrost Gospodarczy" Nr 1/2015: s. 333–349.
Mainwaring Sarah. 2020. „Always in control? Sovereign states in cyberspaces". European Journal of International Security vol. 5(2)/2020: s. 215–232.
Mider Daniel. 2015. „Formy przemocy politycznej w Internecie – próba klasyfikacji". Annales Universitatis Mariae Curie-Skłodowska Vol. XXII, 2 (2015): s. 23–42.
Mirea Mihnea, Wang Victoria, Jung Jeyong. 2019. „The not so dark side of the darknet: a qualitative study". Security Journal Vol. 32: s. 102–118.

ŹRÓDŁA INTERNETOWE

European Parliament. 2001. Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system). W https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN.

Greenwald Glenn, MacAskill Ewen. 2013. „NSA Prism program taps in to user data of Apple, Google and others", The Guardian, W https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Miranda Erika. 2016. „Chinese Internet Regulator: The Great Firewall Not a 'Trade Barrier'". Yibada. W http://en.yibada.com/articles/115714/20160412/chinese-internet--regulator-the-great-firewall-not-a-trade-barier.htm#ixzz49tAdiJPV (16.02.2021).

World Press Freedom Index. 2021. W https://rsf.org/en/ranking/2020#.

AKTY PRAWNE

Międzynarodowym Pakt Praw Obywatelskich i Politycznych z dnia 16 grudnia 1966 r. (Dz. U. z 1977 r., nr 38, poz. 167).

Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 roku (Dz. U. z 1997 r., nr 78, poz. 483).

Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. 1997 Nr 88 poz. 553 z późn. zm.).

PN-ISO/IEC 27001:2007. Technika informatyczna – Technika bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania. Warszawa: Polski Komitet Normalizacyjny.