UNIWERSYTET JANA DŁUGOSZA W CZĘSTOCHOWIE
Res Politicae 2023, t. 15, s. 183–197

http://dx.doi.org/10.16926/rp.2023.15.10

Ryszard NIEDŹWIECKI
https://orcid.org/0000-0003-1025-3602
Uniwersytet Jana Kochanowskiego w Kielcach

Bezpieczeństwo jako kryterium oceny prawa do informacji

Streszczenie

Niniejszy artykuł bazuje na założeniu, że kluczową rolę w ustalaniu priorytetów między bezpieczeństwem a dostępem do informacji i jej rozpowszechnianiem odgrywają prawo i etyka. W większości państw, a z całą pewnością w każdym państwie demokratycznym, istnieją przepisy prawa gwarantujące obywatelom dostęp do informacji publicznej. Przepisy te uznają znaczenie transparentności i przejrzystości w działaniach rządu i instytucji publicznych.

Z drugiej strony, informacja ma ogromny wpływ na różne obszary bezpieczeństwa, istnieje zatem potrzeba zarządzania informacją, jej ochrony i monitorowania.

Słowa kluczowe: bezpieczeństwo, informacja, prawo do informacji.

> Naukowcy raptem zaczynają rozumieć potęgę informacji jako przyczyny, która może w istotny sposób zmieniać świat[1].
>
> Paul Davies

Wprowadzenie

Bezpieczeństwo i informacja tworzą na przestrzeni dziejów nierozłączną, aczkolwiek nie zawsze zgodną parę. Współcześnie ten związek jest coraz silniejszy, a jednocześnie napotyka na coraz bardziej złożone problemy. Z jednej strony państwowe i międzynarodowe systemy bezpieczeństwa nie mogą sprawnie funkcjonować bez chronienia cennych zasobów informacji przed nieuprawnionym dostępem, z drugiej ludzie zamieszkujący globalną wioskę mają prawo do-

[1] P. Davies, *Demon w maszynie*, Kraków 2020, s. 9.

stępu do informacji i jej rozpowszechniania oraz coraz skuteczniej z tego prawa korzystają. Zatem związek między bezpieczeństwem a informacją stanowi subtelny i złożony balans między dwiema ważnymi wartościami. Równowaga między tymi wartościami i potrzebami bieżącej polityki jest fundamentalna dla zachowania zdrowej i demokratycznej społeczności, ale trudna do osiągnięcia.

Informacja a bezpieczeństwo

Informacja ma ogromną moc i wpływ na różne aspekty funkcjonowania społeczeństwa, gospodarki i polityki. W dzisiejszym świecie łatwo dostępne i błyskawicznie rozpowszechniane informacje mogą wywierać wpływ na różne procesy i zjawiska zachodzące w sferze bezpieczeństwa narodowego i międzynarodowego. Ujawnienie lub wyciek informacji wrażliwych, dotyczących systemów bezpieczeństwa, działań rządów, polityki zagranicznej, operacji militarnych, infrastruktury krytycznej, może prowadzić do poważnych negatywnych konsekwencji w postaci destabilizacji instytucji państwa. Wycieki informacji dyplomatycznych mających wpływ na stosunki międzynarodowe i bezpieczeństwo międzynarodowe mogą prowadzić do kryzysów dyplomatycznych lub eskalacji konfliktów. Manipulacja informacjami może wpływać na bezpieczeństwo społeczne, tworząc napięcia, dezinformację lub siejąc panikę w społeczeństwie. Nielegalne ujawnienie kluczowych dla bezpieczeństwa gospodarczego informacji handlowych, tajemnic przemysłowych i danych ekonomicznych może szkodzić interesom gospodarki narodowej i przedsiębiorstw. W bezpieczeństwie cybernetycznym (cyberbezpieczeństwie) informacja jest kluczowym aktywem, bowiem ataki w cyberprzestrzeni opierają się na zdobywaniu informacji, w tym poufnych danych, które mogą być wykorzystane w celach szantażu, kradzieży tożsamości lub naruszenia systemów infrastruktury krytycznej. Naukowcy i eksperci w dziedzinie bezpieczeństwa stale badają i analizują wpływ informacji na bezpieczeństwo, aby lepiej zrozumieć te zależności i opracować skuteczniejsze strategie zapobiegania zagrożeniom związanym z informacjami.

Bezpieczeństwo i informacja jako wartości

Nie ma stałych, jednoznacznych odpowiedzi na pytanie, co jest ważniejsze: prawo do informacji i jej rozpowszechniania czy bezpieczeństwo? W każdej konkretnej sytuacji priorytet może zależeć od kontekstu, celu i skali zagrożenia. Istnieje kilka czynników, które wpływają na to, jakie wartości mogą być brane pod uwagę. Przede wszystkim ważny jest kontekst, bowiem każda sytuacja jest inna, a priorytety w zakresie bezpieczeństwa i informacji mogą się zmieniać. Na przykład w sytuacji kryzysowej priorytetem może być zapewnienie bezpieczeństwa

narodowego, podczas gdy w normalnych warunkach większy nacisk może być kładziony na prawo do informacji. Istotna jest również wartość konkretnej informacji i jakie są potencjalne konsekwencje jej ujawnienia lub zatajenia. Niektóre informacje ważne dla bezpieczeństwa narodowego lub publicznego mogą wymagać szczególnej ochrony.

W przypadku prawa dostępu do informacji istnieją klauzule, które pozwalają na ograniczenie dostępu do niej w sytuacjach, gdy bezpieczeństwo narodowe lub inne ważne interesy publiczne są zagrożone. Te klauzule są niezbędne, ale zawsze wymagają stosowania ostrożnego i proporcjonalnego do zagrożeń bezpieczeństwa. Niektóre środowiska zawodowe, jak na przykład dziennikarze, mają swoje własne zasady etyczne, które odnoszą się do zbierania, przechowywania i publikowania informacji. Etyka dziennikarska wymaga uwzględnienia potencjalnych skutków publikacji danej informacji, zwłaszcza jeśli może ona naruszyć bezpieczeństwo lub prywatność osób. Dziennikarze starają się chronić źródła, które dostarczają im informacje, co niekiedy prowadzi do konfliktów z prawem lub interesami bezpieczeństwa.

W każdej konkretnej sytuacji może zostać poddane ocenie co jest ważniejsze: prawo do ochrony informacji czy prawo do jej posiadania i rozpowszechniania? Zgodnie z Powszechną Deklaracją Praw Człowieka ONZ (z 1948), a w szczególności jej artykułem 19. „każdy ma prawo do…poszukiwania, otrzymywania i rozpowszechniania informacji i poglądów wszelkimi środkami i bez względu na granice”[2]. Jednakże w wydanej już dwa lata później Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (z 1950 roku)[3] w art. 10. uwzględniono niezbędne w społeczeństwie demokratycznym: ograniczenia, warunki, wymogi i sankcje do powyższego prawa. Uczyniono to z uwagi na potrzeby państw w zakresie zapobiegania ujawnieniu informacji poufnych. Można skonstatować, że obie konwencje oddają w ręce instytucji państw kompetencje oceny w jakich okolicznościach fundamentalne prawa człowieka dotyczące również wolności wypowiedzi i prawa do informacji, mogą zostać ograniczone. Ograniczanie dostępu do informacji przez nadawanie im klauzuli tajności jest standardową procedurą instytucji państwowych i międzynarodowych odpowiedzialnych za zapewnianie bezpieczeństwa.

Sytuacja, w której państwo, podmioty publiczne i prywatne korzystają z możliwości ograniczania praw innych podmiotów zbiorowych i indywidualnych do informacji z uwagi na interes własny jest powszechnie akceptowana, jednakże przyczyny i sposoby egzekwowania togo prawa mogą niekiedy budzić wątpliwości zarówno ze strony instytucji odpowiedzialnych za tworzenie i egzekwowanie

[2] Powszechna Deklaracja Praw Człowieka, wydana w Paryżu 10 XII 1948 r. [źródło: https://isap.sejm.gov.pl/].

[3] *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*, [źródło: https://isap.sejm.gov.pl/].

przestrzegania obowiązujących norm prawnych, jak też tych instytucji, które mają za zadanie monitorowanie przestrzegania prawa do informacji.

Przykładem, który obrazuje problem ograniczania prawa do informacji może być pandemia COVID–19. W początkowej fazie pandemii rządy wielu państw zaczęły wprowadzać ograniczenia w dostępie do informacji. W tej sytuacji w marcu 2020 r. przewodnicząca Komisji Europejskiej Ursula von der Leyen wydała oświadczenie informujące państwa członkowskie Unii Europejskiej, że Komisja Europejska będzie ściśle monitorować stosowanie przez państwa środków nadzwyczajnych, sprawdzając w duchu współpracy, czy nie są one wprowadzane kosztem wolności słowa. W sytuacji kryzysowej wywołanej przez pandemię Komisja uznała za ważniejsze niż kiedykolwiek przeciwdziałanie dezinformacji oraz zapewnienie swobody dziennikarzom, dostępu do informacji obywatelom[4].

W kwietniu 2020 r. Rada Europy wystosowała do 47 państw członkowskich dokument informacyjny, w którym zwrócono uwagę na ograniczanie prawa do wyrażania opinii, w tym swobodnego i szybkiego przepływu informacji[5]. W dokumencie zauważono, że w niektórych krajach europejskich (bez wskazywania, w których) osobom rozpowszechniającym informacje niepozostające w pełnej zgodzie ze źródłami oficjalnymi grozi kara więzienia, a dostęp do informacji uznanych przez władze za fałszywe może być blokowany bez wyjaśnień powodów ograniczeń[6].

Według Katarzyny Dunaj[7] bezpieczeństwo jednostki jako wartość uniwersalna od zarania dziejów ludzkości było związane z procesami państwowotwórczymi, a państwo zgodnie z koncepcją umowy społecznej Thomasa Hobbesa[8] może ograniczyć ograniczać niektóre wolności jednostek, aby zapewnić porządek i bezpieczeństwo. To podejście jest widoczne w wielu współczesnych systemach prawnych i konstytucjach, gdzie państwo posiada uprawnienia do regulowania i ograniczania niektórych praw jednostek w imię ochrony bezpieczeństwa narodowego i społecznego. Niejednokrotnie może dochodzić do kolizji wartości, jakimi są wolności i prawa człowieka i obywatela, które państwo ma chronić, z wartościami takimi jak bezpieczeństwo i porządek publiczny[9]. Z tej przyczyny w demokratycznym państwie prawnym istnieją odpowiednie mechanizmy w po-

---

[4] *Ograniczenia nie mogą naruszać zasad, Oświadczenie przewodniczącej Komisji Europejskiej Ursuli von der Leyen na temat środków nadzwyczajnych podjętych przez państwa członkowskie*, Komisja Europejska Bruksela 31 marca 2020, https://poland.representation.ec.europa.eu/news/

[5] *Przestrzeganie praw człowieka w dobie pandemii COVID-19. Stanowisko Rady Europy.* Opracowania tematyczne OT–684, Kancelaria Senatu, Warszawa 2020, s. 19.

[6] Ibidem, s. 21.

[7] M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Bezpieczeństwo państwa Zagadnienia prawne i administracyjne,* Olsztyn 2016, s. 17–18

[8] T. Hobbes, *Lewiatan, czyli materia, forma i władza państwa kościelnego i świeckiego*, Warszawa 2005, s. 353.

[9] M. Karpiuk, *Państwo sprawne, skuteczne i przyjazne obywatelom*, „Problemy Prawa i Administracji" 2011, nr 1, s. 7.

staci zasad prawa, trójpodziału władzy i niezależności sądownictwa, które mają na celu ochronę przed nadmiernym ograniczaniem przez państwo wolności człowieka. Równowaga między bezpieczeństwem a wolnościami jednostek jest współcześnie jednym z kluczowych wyzwań stojących przed demokratycznymi społeczeństwami i mimo nieustannie podejmowanych prób równoważenia potrzeb bezpieczeństwa i prawa do informacji, otwarta pozostaje kwestia rozstrzygnięcia zakresu kompetencji instytucji demokratycznego państwa oraz mnogości służb, uprawnionych do ingerencji w podstawowe wolności i prawa człowieka[10]. Przy czym, ciągle zmienia się podległość, organizacja oraz zakres przekazywanych, a niekiedy dublujących się kompetencji podmiotów (służb) właściwych w sprawach bezpieczeństwa. W permanentnie zmieniających się okolicznościach funkcjonowania poszczególnych służb trudno nie zgodzić się z tezą, że taka sytuacja nie sprzyja zachowaniu standardów bezpieczeństwa demokratycznego państwa prawnego[11].

Zapewnianie bezpieczeństwa i prawa do informacji

Ciągłego rozwiązywania wymaga złożony i wielowątkowy problem wyrażający się w pytaniu: w jaki sposób oraz jakimi dopuszczalnymi środkami państwo może i powinno zapewniać swoim obywatelom bezpieczeństwo, nie naruszając przy tym nadrzędnego, przynależnego każdemu człowiekowi prawa do wolności opinii i wypowiedzi oraz poszukiwania, otrzymywania i rozpowszechniania informacji i poglądów wszelkimi środkami i bez względu na granice?

Od czasu, kiedy powstała Konwencja o Ochronie Praw Człowieka w środowisku bezpieczeństwa zmieniło się prawie wszystko. Zasady pozostały nie zmienione, ale okoliczności, w jakich obowiązują są dziś inne. Podobnie ochrona bezpieczeństwa obywateli rozumiana jako zbiór państwowych gwarancji bezpieczeństwa jest wytworem epoki nowożytnej, w której stopniowo umacniał się instytucjonalny system bezpieczeństwa, kreowany w celu utrzymania porządku międzynarodowego i państwowego. W tym wymiarze państwo stało się gwarantem bezpieczeństwa ludzi, integralności terytorialnej, stabilności władzy, porządku publicznego.

Procesowi globalizacji towarzyszy erozja suwerennych państw, a regulacja i kontrola zastępują lub uzupełniają ochronę bezpieczeństwa. Rozwój technologii komunikacyjnych i internetu przyczynił się do zwiększenia dostępu do informacji. Globalizacja sprzyja wymianie informacji między krajami i kulturami. To może pomagać w zrozumieniu różnic kulturowych i politycznych oraz w promowaniu dialogu między narodami. Ludzie na całym świecie mogą teraz uzyskiwać informacje z różnych odległych geograficznie źródeł i komunikować się w bardzo

[10] M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, op. cit., s. 305.

[11] Ibidem, s. 306.

krótkim czasie, bez względu na granice naturalne stworzone przez przyrodę oraz polityczne i ideologiczne będące dziełem ludzi. W kontekście globalizacji niektóre państwa, jedne oficjalnie, a inne skrycie, wykorzystują nowoczesne technologie do kontroli przepływu informacji i monitorowania działań swoich obywateli, co może stanowić realne zagrożenie dla praw człowieka, w tym prawa do informacji. Z drugiej strony, w związku z globalizacją wzrosło również zainteresowanie ochroną prywatności i danych osobowych. Wiele krajów wprowadziło przepisy dotyczące ochrony danych, które regulują, jak informacje są gromadzone, przetwarzane i udostępniane. Warto zaznaczyć, że proces globalizacji wprowadza nowe wyzwania dla ochrony praw człowieka i równocześnie stwarza nowe możliwości w zakresie dostępu do informacji i komunikacji. Rządy i społeczeństwa muszą dążyć do zachowania równowagi między potrzebą ochrony bezpieczeństwa narodowego a ochroną praw jednostek, w tym prawa do informacji na skalę międzynarodową. W kontekście globalizacji kluczową rolę w tym procesie odgrywają międzynarodowe standardy praw człowieka i międzynarodowa współpraca.

Informacja a bezpieczeństwo

Spróbujmy spojrzeć na problem roli i znaczenia informacji od strony bezpieczeństwa, albowiem to właśnie bezpieczeństwo, mimo swojej wieloznaczności, jest nadal źródłem tworzenia wielu zasad regulacyjnych w wymiarze globalnym, państwowym (narodowym) oraz indywidualnym. Jednocześnie może ono oznaczać: poczucie braku zagrożeń, program polityczny, źródło legitymizacji, niezbędne siły materialne, służbę publiczną oraz dobro handlowe. Natomiast informacja, jak to zauważył Tomasz Aleksandrowicz, stanowi strategiczny zasób państwa, który jest krytyczny dla jego funkcjonowania, dlatego powinna być odpowiednio chroniona[12]. Zgodnie z projektem Doktryny Bezpieczeństwa Informacyjnego RP z 2016 r. bezpieczeństwo informacyjne jest transsektorowym obszarem, a jednocześnie procesem, którego celem jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej[13].

Na całym świecie było już wiele przykładów ograniczania prawa do informacji z powodu interesów bezpieczeństwa. Przytoczę tylko kilka z nich w celu zasygnalizowania przyczyn i skali tego zjawiska. Wielka Zapora Ogniowa (Great Firewall[14]) jest systemem kontroli internetowej, który jest używany w Chinach do

[12] T.R. Aleksandrowicz, *Bezpieczeństwo informacyjne państwa,* „Studia Politologiczne" 2018, vol. 49, s. 33–34.

[13] *Doktryna Bezpieczeństwa Informacyjnego RP* (*projekt*), BBN, Warszawa 2015, s. 3.

[14] The Great Firewall of China (GFW) – „termin używany do opisania kombinacji działań legislacyjnych i technologii narzuconych przez chiński rząd w celu regulowania i kontrolowania internetu w kraju. GFW jest uważany za najbardziej wyrafinowany system cenzury na świecie i ma

blokowania dostępu do wielu stron internetowych i treści uważanych przez rząd chiński za niebezpieczne lub niepożądane. Jest to przykład znacznego ograniczenia dostępu do informacji w imię utrzymania kontroli i bezpieczeństwa. W Korei Północnej rząd ściśle kontroluje dostęp do informacji i mediów. Obywatele mają ograniczony dostęp do informacji z zewnątrz kraju, a treści medialne są silnie cenzurowane w celu utrzymania kontroli nad narracją[15]. Po zamachach z 11 września 2001 roku Stany Zjednoczone przyjęły Ustawę Patriotyczną (Patriot Act[16]), która znacząco rozszerzyła uprawnienia rządu w zakresie monitorowania komunikacji i dostępu do informacji w celu zwalczania terroryzmu. To spowodowało wiele kontrowersji związanych z prywatnością i prawami obywateli.

Niektóre państwa pod pozorem zapewniania bezpieczeństwa jawnie naruszają prawo obywateli do wolności i wypowiedzi. Przykładów, które obrazują łamanie tego prawa jest wiele, ale przejawy tego zjawiska może zobrazować przypadek, który ma miejsce w bliskim sąsiedztwie Polski. W 2023 r. białoruski sąd kierując się wytycznymi politycznymi, skazał Andrzeja Poczobuta – znanego dziennikarza i pasjonata historii – na 8 lat więzienia za rzekome „wzniecanie nienawiści" i „działalność terrorystyczną". Postępowanie władz i sądów Białorusi spotkało się z krytyką polskich instytucji, w tym Ministerstwa Spraw Zagranicznych Rzeczypospolitej Polskiej, które potępiając niesprawiedliwy, domaga się uwolnienia Andrzeja Poczobuta[17].

W wielu krajach istnieją przepisy, które zabraniają publikacji informacji związanych z tajnymi operacjami wojskowymi lub wywiadowczymi. Celem jest ochrona bezpieczeństwa narodowego i zapobieganie ujawnieniu poufnych informacji. W niektórych państwach istnieją przepisy ograniczające rozpowszechnianie informacji na temat technologii podwójnego zastosowania. Ograniczenia te wywołują wiele kontrowersji i nie sprzyjają osiągnięciu równowagi między potrzebą zapewnienia bezpieczeństwa narodowego a prawem obywateli do dostępu do informacji i wolności słowa. W tym kontekście warto zwrócić uwagę na politykę informacyjną władz w Polsce podczas narastania kryzysu migracyjnego na granicy z Białorusią latem 2021 r. w związku z działaniami służb białoruskich.

---

na celu uniemożliwienie obywatelom Chin dostępu do treści uznanych za nieodpowiednie lub szkodliwe dla bezpieczeństwa narodowego lub wartości kulturowych kraju". Źródło: Website Rating – https://www.websiterating.com/pl/vpn/glossary/what-is-great-firewall-china/ [dostęp: 15.04.2023].

[15] Pełny dostęp do internetu w Korei Północnej ma ograniczony krąg władzy, społeczeństwo ma dostęp wyłącznie do krajowego internetu Kwangmyong. Źródło: Raport *North Korea Cyber Activity,* Recorded Future Insikt Group, https://go.recordedfuture.com/hubfs/reports/north-korea-activity.pdf, [dostęp: 15.04.2023].

[16] Patriot Act, „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001". Źródło: https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act [dostęp: 15.04.2023].

[17] Oświadczenie MSZ w sprawie wyroku w procesie Andrzeja Poczobuta, Ministerstwo Spraw Zagranicznych, https://www.gov.pl/web/dyplomacja.

Liczba nielegalnych prób przekroczenia granicy wzrosła wówczas do ok. 3000 w miesiącu. W związku z destabilizacją sytuacji na granicy polsko-białoruskiej Rada Ministrów 31 sierpnia 2021 r. skierowała do Prezydenta RP wniosek o wprowadzenie stanu wyjątkowego na przygranicznych obszarach będących częścią województw lubelskiego i podlaskiego. W rozporządzeniu o wprowadzeniu 30-dniowego stanu wyjątkowego, obowiązującym od 2.09.2021 r., zawarto zapis o ograniczeniu dostępu do informacji publicznej dotyczącej czynności prowadzonych na obszarze objętym stanem wyjątkowym. W tym samym dniu Rada Ministrów wydała Rozporządzenie w sprawie ograniczeń wolności i praw w związku z wprowadzeniem stanu wyjątkowego[18]. W rozporządzeniu RM również znalazł się zapis o ograniczeniu dostępu do informacji publicznej dotyczącej czynności prowadzonych na obszarze objętym stanem wyjątkowym[19]. Do sprawy odniósł się Rzecznik Praw Obywatelskich, dostrzegając ścisły związek ograniczenia prawa dostępu do informacji publicznej z wolnością słowa i wolnością mediów. Zauważył on, że uniemożliwienie dziennikarzom dostępu do informacji o sytuacji w rejonie objętym stanem wyjątkowym zwiększa ryzyko niekontrolowanego rozprzestrzeniania się nieprawdziwych i niezweryfikowanych informacji, co w efekcie może prowadzić do dodatkowego zagrożenia bezpieczeństwa i porządku publicznego. Taka sytuacja w opinii Rzecznika może budzić wątpliwości z punktu widzenia zasady proporcjonalności i prowadzić do wyłączenia spod kontroli społecznej działań organów publicznych i w konsekwencji do obniżenia zaufania obywateli do państwa[20].

Warto zauważyć, że zakres ograniczeń w dostępie do informacji z powodu ochrony ważnych interesów bezpieczeństwa może zależeć od poziomu kultury strategicznej elit politycznych sprawujących władzę w danym kraju. Elity polityczne powinny rozumieć, że zła polityka informacyjna w zakresie ważnych problemów bezpieczeństwa może skutkować spadkiem zaufania społeczeństwa do instytucji państwa i w konsekwencji prowadzić do jego erozji.

Zakładając, że informacja może być bronią, warto wskazać, do jakich celów może być ona wykorzystana:

— informację można wykorzystać do osiągnięcia celów strategicznych, wpływania na opinię publiczną, destabilizowania społeczeństw czy atakowania infrastruktury krytycznej;
— państwa i podmioty niepaństwowe mogą wykorzystywać dezinformację i propagandę jako narzędzie walki hybrydowej do zniekształcania faktów,

[18] Rozporządzenie Rady Ministrów z dnia 2 września 2021 r. w sprawie ograniczeń wolności i praw w związku z wprowadzeniem stanu wyjątkowego, Warszawa, dnia 2 września 2021 r., poz. 1613.

[19] Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 2 września 2021 r. w sprawie wprowadzenia stanu wyjątkowego na obszarze części województwa podlaskiego oraz części województwa lubelskiego, Dziennik Ustaw RP, Warszawa 2.09.2001, poz. 1216.

[20] *RPO ma wątpliwości ws. ograniczeń pracy dziennikarzy oraz dostępu do informacji publicznej*, Biuletyn Informacji Publicznej RPO, https://bip.brpo.gov.pl/pl/content/.

wprowadzania zamętu, manipulowania opinią publiczną i osiągania celów politycznych;
- ataki cybernetyczne, polegające na kradzieży wrażliwych informacji zawierających dane rządowe lub firmowe, mogą być następnie wykorzystane do szantażu lub celów szpiegowskich albo też zakłócać funkcjonowanie infrastruktury krytycznej;
- zaawansowane technologie informacyjne takie jak sztuczna inteligencja i algorytmy służące do analizy wielkich zbiorów danych pozwalają na przetwarzanie ogromnych ilości informacji w celu identyfikowania wzorców i prognozowania zachowań;
- pojedyncze osoby lub grupy mogą wykorzystywać socjotechniki, czyli manipulację ludźmi, w celu uzyskania dostępu do informacji, może to obejmować inżynierię społeczną, wykorzystywanie słabości psychologicznych lub korzystanie z zaufania;
- rządy mogą wykorzystywać zaawansowane systemy śledzenia i inwigilacji do zbierania informacji na temat obywateli, co może naruszać prywatność i wolność jednostki.

Trwa niewypowiedziana powszechna wojna hybrydowa prowadzona przez państwa i podmioty niepaństwowe, które wybierają informację jako broń, gdyż albo nie mają wystarczającej ilości i jakości tradycyjnego uzbrojenia, albo też nie mogą czy nie chcą go używać. W przeciwieństwie do tradycyjnej wojny, wojna hybrydowa nie polega na użyciu konwencjonalnego uzbrojenia, takiego jak broń palna czy wojskowe pojazdy jeżdżące, latające i pływające. Zamiast tego skupia się na atakach w cyberprzestrzeni, dezinformacji, propagandzie i innego rodzaju działań informacyjnych. Celem takich działań jest wywołanie chaosu i spadku zaufania do instytucji publicznych. Niektóre podmioty (państwowe i niepaństwowe) mogą działać poza fizycznymi granicami państw i jurysdykcją prawa krajowego i międzynarodowego. Istotą wojen informacyjnych jest (podobnie jak w każdej innej wojnie) osiągnięcie celów politycznych, a w szczególności takich jak: wpływ na wybory, destabilizacja społeczeństw, szpiegostwo przemysłowe czy dezinformacja w celu osiągnięcia przewagi geopolitycznej.

Wojny informacyjne polegają na wykorzystaniu zaawansowanych technologii komunikacyjnych, w tym komputerów, internetu, mediów społecznościowych oraz algorytmów do manipulowania informacją i opiniami publicznymi. Jednym z wyzwań związanym z wojnami hybrydowymi jest określenie odpowiedzialności za ataki. Często trudno jest dokładnie ustalić, kto jest odpowiedzialny za cyberatak czy dezinformację, co utrudnia podjęcie działań odwetowych lub sankcje. Wojny informacyjne stanowią istotne zagrożenie dla bezpieczeństwa narodowego i międzynarodowego, dlatego wiele krajów i międzynarodowych organizacji pracuje nad strategiami i środkami obrony przed takimi atakami, a także nad zwiększeniem odporności społeczeństw na dezinformację. Jest to także temat licznych debat i dyskusji dotyczących nowych wyzwań w dziedzinie bezpieczeństwa.

Ataki informacyjne na systemy informatyczne państwowe i niepaństwowe mogą mieć na celu kradzież wrażliwych informacji, destabilizację działań, szpiegostwo przemysłowe lub wprowadzenie zamętu. Ataki mogą być wykonywane przy użyciu zaawansowanych technologii (takich jak sztuczna inteligencja), które pozwalają na identyfikację luk w zabezpieczeniach lub analizę ogromnych ilości danych w celu osiągnięcia celów strategicznych. Do rozpowszechniania złośliwego oprogramowania lub kampanii dezinformacyjnych często wykorzystywane są media społecznościowe. Niektóre państwa prowadzą inwigilację i zbierają informacje na temat obywateli oraz innych państw, co może naruszać prywatność i suwerenność narodową.

Manipulowanie informacją

Rzadziej poświęcamy naszą uwagę kwestiom manipulowania informacją, a jak tego dowodzą fakty, zjawisko manipulowania informacją może stanowić istotne wyzwanie dla wszystkich podmiotów funkcjonujących w środowisku bezpieczeństwa oraz implikuje potrzebę weryfikacji dotychczasowych norm i zasad obowiązujących w polityce, relacjach międzynarodowych i stosunkach społecznych w kontekście prawa do informacji. Masowe wycieki informacji często wywołują konflikt potrzeby transparentności i dostępu do informacji z potrzebą ochrony bezpieczeństwa narodowego, prywatności i innych ważnych interesów. To prowadzi do debat na temat granic, które należy wyznaczyć między prawem do informacji a ochroną innych wartości.

Manipulowanie informacją to istotne wyzwanie w kontekście bezpieczeństwa, które może dotyczyć zarówno podmiotów państwowych, jak i publicznych oraz prywatnych. Jest zjawiskiem stanowiącym wyzwanie naszych czasów. Wpływa na różne aspekty funkcjonowania społeczeństwa i bezpieczeństwa, w tym na politykę, relacje międzynarodowe, opinię publiczną i gospodarkę.

Rozwój technologii cyfrowych i mediów społecznościowych umożliwia masowe wycieki informacji i sprawia, że tradycyjne źródła informacji, takie jak gazety i telewizja, tracą monopol na kontrolę nad przepływem informacji. Erozja tradycyjnych źródeł publikacji prowadzi do zmiany sposobów, w jaki informacje są zbierane, rozpowszechniane i kontrolowane. Wreszcie masowe wycieki informacji wywołują debatę nad etyką ujawniania informacji, konsekwencjami takich działań i rolą informatorów w społeczeństwie. Manipulacja jest bagatelizowana, gdyż nie zawsze prowadzi do wymiernych zniszczeń. Jednakże historia konfliktów XX i XXI wieku zna liczne przypadki manipulacji informacjami w celu zastraszania, nękania, a nawet zabijania ludzi.

Dezinformacja, która może przyjmować postać kampanii, może być przyczyną zamętu i konfliktów społecznych, podważać zaufanie do instytucji, prowadzić do dezintegracji społeczeństw, a także wpływać na wyniki wyborów i procesy demo-

kratyczne. Dezinformacja może również destabilizować rynki finansowe, wywołując panikę lub fałszywą wycenę aktywów. Manipulowanie informacją może także kształtować publiczne postrzeganie określonych wydarzeń lub problemów oraz podważać zaufanie do mediów i rzetelnych źródeł informacji, co ma wpływ na zdolność społeczeństwa do uzyskiwania wiarygodnych informacji. Wreszcie kampanie dezinformacyjne mogą być używane do osiągania celów związanych z bezpieczeństwem, takich jak: destabilizacja innych państw, osłabienie sojuszy oraz podejmowanie złych decyzji politycznych przez rządy i organizacje międzynarodowe.

Jednym z najbardziej znanych przykładów manipulacji informacją, szczególnie w kontekście kampanii dezinformacyjnych, jest oskarżenie o ingerencję Rosji w wybory prezydenckie w USA w 2016 roku. Agencje wywiadowcze USA oskarżyły Rosję o próby wpływania na wyniki wyborów poprzez rozpowszechnianie dezinformacji i działania w mediach społecznościowych[21]. Przykłady wpływu na wyniki wyborów za pomocą dezinformacji można znaleźć w wielu innych krajach, w tym w Brazylii, Indiach, Francji. Kampanie dezinformacyjne i manipulacja informacją były i są nadal używane do osłabienia konkurencyjnych kandydatów i podważenia procesów demokratycznych. Kampanie dezinformacyjne mogą być również kierowane przeciwko instytucjom państwowym, rządom i innym organom. Poprzez rozpowszechnianie fałszywych informacji i teorii spiskowych, manipulatorzy starają się podważyć zaufanie obywateli do tych instytucji. Skutkuje to spadkiem zaufania do władzy, co może prowadzić do dezintegracji społeczeństwa. Wprowadzając dezinformację i propagandę, manipulatorzy mogą sprawić, że opinia publiczna będzie podzielona lub zdezorientowana, co wpływa na zdolność społeczeństwa do skonsolidowania się wokół wspólnych celów. Fałszywe informacje lub dezinformacja są wykorzystywane do wprowadzania w błąd wyborców lub dyskredytowania konkurencyjnych kandydatów, co może prowadzić do spadku zaufania do procesów demokratycznych i destabilizacji politycznej. Dlatego manipulowanie informacją w celu dezinformacji jest traktowane jako poważne zagrożenie dla stabilności społeczeństw. W tej sytuacji coraz ważniejsze staje się promowanie krytycznego myślenia o jakości informacji oraz rozwijanie odporności (rezyliencji) społeczeństw na manipulację informacją. Jest to wyzwanie, które wymaga zaangażowania zarówno ze strony rządów, jak i społeczeństwa obywatelskiego oraz sektora prywatnego.

Istnieje wiele inicjatyw i mechanizmów, które zostały wprowadzone w różnych krajach i na poziomie międzynarodowym, aby zwalczać manipulowanie informacją i chronić integralność procesów wyborczych. Organizacje zajmujące się weryfikacją faktów (ang. *fact-checking*) monitorują treści publikowane w mediach i w Internecie oraz weryfikują ich prawdziwość. Ich celem jest ujawnianie fałszywych informacji i dezinformacji, co pomaga w dostępie do rzetelnych da-

[21] A. Kruglashov, S. Shvydiuk, *Hybrydowe zagrożenia dla demokracji. Wybrane przykłady zewnętrznej ingerencji Rosji w wybory,* „Wschód Europy. Studia Humanistyczno-Społeczne" 2022, t. 8, nr 2, s. 84.

nych w sytuacjach, kiedy dezinformacja przesłania prawdę, a użytkownicy mediów nie wiedzą, komu ufać. Podstawową zasadą *fact-checkingu* jest sprawdzanie faktów i publikowanie oryginalnych raportów śledczych opartych na dowodach. W celu zwiększania świadomości w zakresie rozpoznawania dezinformacji i fałszywych informacji oraz promowania krytycznego myślenia konieczna wydaje się również edukacja medialna młodzieży i dorosłych, a zwłaszcza najstarszych, „wychowanych" na tradycyjnych mediach.

Państwa i organizacje międzynarodowe podejmują współpracę w celu zapobiegania ingerencji zewnętrznej w wybory i zwalczania dezinformacji. Przykładem jest Europejski Plany Działań Wsparcia na Rzecz Demokracji[22] (EDPA), którego wdrażanie przyczyniło się między innymi do przyspieszenia działań mających na celu wzmocnienie ochrony osób, które angażują się w debatę publiczną, przed bezpodstawnymi lub stanowiącymi nadużycie postępowaniami sądowymi[23]. Te postępowania będące wynikiem „strategicznych powództw zmierzających do stłumienia debaty publicznej" (ang. *Strategic lawsuits against public participation* – SLAPP) najczęściej są wytaczane przez podmioty „silniejsze" przeciwko podmiotom „słabszym", w celu uciszenia – uzasadnionej skądinąd – krytyki. Warto podkreślić, że walka z dezinformacją jest procesem wieloaspektowym. Działania podejmowane na tym polu często wymagają współpracy wielu podmiotów, w tym rządów, mediów, społeczeństwa obywatelskiego i platform internetowych.

Kolizja wartości

W kontekście ochrony interesów podmiotów państwowych często dochodzi do kolizji między wartościami, jakimi dla społeczeństwa obywatelskiego są wolność i prawa człowieka a potrzebą zapewnienia bezpieczeństwa i porządku publicznego. Złożoność sytuacji mogą zobrazować następujące przykłady konfliktu omawianych wartości:

— *Interesy bezpieczeństwa a prywatność online*: w miarę, jak rozwija się technologia cyfrowa, rządy starają się monitorować komunikację online w celu zapobiegania terroryzmowi i przestępczości internetowej, jednak te działania mogą naruszać prywatność użytkowników internetu i podważać ich prawo do prywatności;

[22] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego komitetu ekonomiczno-społecznego i Komitetu regionów w sprawie Europejskiego Planu Działania na Rzecz Demokracji*, EUR-lex. Baza aktów prawnych Unii Europejskiej, Bruksela dnia 3.12.2020., https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0790 [dostęp: 15.04.2023].

[23] *Proposal for a Directive of the European Parliament and of the Council on protecting persons who engage in public participation from manifestly unfounded or abusive court proceedings* (*„Strategic lawsuits against public participation"*), EUR-lex. Baza aktów prawnych Unii Europejskiej https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0177 [dostęp: 15.04.2023].

— *Walka z terroryzmem a wolność słowa*: państwa podejmują działania w celu zwalczania propagandy terrorystycznej i ekstremizmu online, jednak niekiedy te działania mogą prowadzić do przypadków cenzury i ograniczania wolności słowa;
— *Kontrola granic a prawa uchodźców*: w kontekście kryzysów migracyjnych rządy muszą kontrolować swoje granice, jednak to może stać w sprzeczności z międzynarodowymi zobowiązaniami dotyczącymi praw uchodźców i azylu;
— *Ograniczenia w dostępie do informacji w sytuacjach kryzysowych*: w czasie kryzysów rządy mogą kontrolować przekazywanie informacji, aby zapobiec panice społecznej, jednak równocześnie istnieje potrzeba przejrzystości i dostępu do informacji publicznej, aby umożliwić obywatelom podejmowanie świadomych decyzji;
— *Kwestie zdrowia publicznego a wolność jednostki*: w przypadku pandemii lub różnego rodzaju zagrożeń związanych z chorobami zwierząt i roślin, rządy mogą wprowadzać ograniczenia w przemieszczaniu się i działalności gospodarczej w celu ochrony zdrowia publicznego, jednak te decyzje mogą ograniczać wolność jednostki i jej prawa gospodarcze.

Powyższe przykłady sygnalizują konieczność dokonywania trudnych wyborów przez władze każdego państwa demokratycznego lub instytucje międzynarodowe. Niekiedy decyzje są podejmowane w warunkach, kiedy potrzeba zapewnienia bezpieczeństwa ogółowi koliduje z potrzebą ochrony wolności jednostki.

Podsumowanie

Koncepcja bezpieczeństwa realizowana przez państwo może wydawać się sprzeczna z prawem do swobodnej wypowiedzi oraz nieskrępowanego dostępu do informacji. Należy jednak zauważyć, że prawo do dostępu do informacji nie jest absolutne i może kolidować z potrzebą ochrony innych wartości, chociażby takich jak: ochrona prywatności, ochrona praw autorskich i innych. Ważne jest również, aby państwo działało w sposób odpowiedzialny, gwarantując obywatelom pewność, że wszelkie ograniczania wolności słowa i dostępu do informacji ze względu na konieczność zapewnienia bezpieczeństwa są zgodne z prawem i proporcjonalne do potrzeby zapewnienia bezpieczeństwa.

Bibliografia

Materiały publikowane

Doktryna Bezpieczeństwa Informacyjnego RP (projekt), BBN, Warszawa 2015.
Przestrzeganie praw człowieka w dobie pandemii COVID-19. Stanowisko Rady Europy. Opracowania tematyczne OT–684, Kancelaria Senatu, Warszawa 2020.

Akty prawne

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.

Patriot Act, „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT), Washington 2001.

Powszechna Deklaracja Praw Człowieka, wydana w Paryżu 10 XII 1948 r., Wyd. Biuro Rzecznika Praw Obywatelskich, Warszawa 1998.

Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 2 września 2021 r. w sprawie wprowadzenia stanu wyjątkowego na obszarze części województwa podlaskiego oraz części województwa lubelskiego, Dziennik Ustaw RP, Warszawa 2.09.2001, poz. 1216.

Rozporządzenie Rady Ministrów z dnia 2 września 2021 r. w sprawie ograniczeń wolności i praw w związku z wprowadzeniem stanu wyjątkowego, Dziennik Ustaw RP, Warszawa, dnia 2 września 2021 r., poz. 1613.

Monografie

Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Wydział Prawa i Administracji UWM, Olsztyn 2016.

Davies P., *Demon w maszynie*, Wyd. Copernicus Center Press, Kraków 2020.

Hobbes T., *Lewiatan, czyli materia, forma i władza państwa kościelnego i świeckiego*, Wyd. Aletheia, Warszawa 2005.

Artykuły

Aleksandrowicz T.R., *Bezpieczeństwo informacyjne państwa*, „Studia Politologiczne" 2018, vol. 49.

Karpiuk M., *Państwo sprawne, skuteczne i przyjazne obywatelom*, „Problemy Prawa i Administracji" 2011, nr 1.

Kruglashov A., Shvydiuk S., *Hybrydowe zagrożenia dla demokracji. Wybrane przykłady zewnętrznej ingerencji Rosji w wybory*, „Wschód Europy. Studia Humanistyczno-Społeczne" 2022, t. 8, nr 2.

Źródła internetowe

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego komitetu ekonomiczno-społecznego i Komitetu regionów w sprawie Europejskiego Planu Działania na Rzecz Demokracji, Bruksela dnia 3.12.2020., https://eur-lex.europa.eu/legal-content

Ograniczenia nie mogą naruszać zasad, Oświadczenie przewodniczącej Komisji Europejskiej Ursuli von der Leyen na temat środków nadzwyczajnych podję-

tych przez państwa członkowskie, Komisja Europejska Bruksela 31 marca 2020 https://poland.representation.ec.europa.eu/news

Oświadczenie MSZ w sprawie wyroku w procesie Andrzeja Poczobuta, Ministerstwo Spraw Zagranicznych, https://www.gov.pl/web/dyplomacja

Proposal for a Directive of the European Parliament and of the Council on protecting persons who engage in public participation from manifestly unfounded or abusive court proceedings (*"Strategic lawsuits against public participation"*), Commision Staff Working Document, Bruksela dnia 27.04.2022., https://eur-lex.europa.eu/legal-content

Rapport North Korea Cyber Activity, Recorded Future, www.recordedfuture.com

RPO ma wątpliwości ws. ograniczeń pracy dziennikarzy oraz dostępu do informacji publicznej, Biuletyn Informacji Publicznej RPO, https://bip.brpo.gov.pl/pl/contentWebsite Rating, https://www.websiterating.com

Security as a criterion for assessing the right to information

Summary

This article is based on the premise that law and ethics play a key role in prioritizing security and access to and dissemination of information. In most countries, and certainly in every democratic state, there are laws guaranteeing citizens the right of access to public information. This law recognizes the importance of transparency and transparency in the activities of government and public institutions. On the other hand, information has a huge impact on various areas of security, so there is a need to manage, protect and monitor information.

Keywords: security, information, right to information.