Magdalena Sitek
Wyższa Szkoła Gospodarki Euroregionalnej
im. Alcide De Gasperi w Józefowie
ms@wsge.edu.pl

DOI: 10.13166/JMS/91855
JOURNAL OF MODERN SCIENCE TOM 2/37/2018, S. 177–189

The legal framework for the security of the individual in cyberspace

Prawne ramy bezpieczeństwa jednostki w cyberprzestrzeni

Abstract

The subject of the study is to present legal frameworks of the security of the individual in cyberspace. As a research hypothesis, it should be assumed that the level of this security depends primarily on the appropriate regulations and institutions that will deal with active forms of protection of the individual's security in cyberspace. To achieve this goal, the method of description of advantages and disadvantages of cyberspace and showing its characteristics was used in the work. Then, the analysis of legal provisions in Poland was carried out in terms of their applicability in policy which could guarantee the security of the individual in cyberspace.

Streszczenie

Przedmiotem opracowania jest ukazanie prawnych ram bezpieczeństwa jednostki w cyberprzestrzeni. Jako hipotezę badawczą należy przyjąć, że poziom tego bezpieczeństwa zależy przede wszystkim od odpowiednich uregulowań oraz instytucji, które będą zajmowały się aktywnymi formami ochrony bezpieczeństwa jednostki w cyberprzestrzeni. W celu realizacji tego zamierzenia w pracy posłużono się metodą opisu zalet i wad cyberprzestrzeni oraz ukazania jej cech charakterystycznych. Następnie w opracowaniu przeprowadzono analizę przepisów prawa w Polsce pod kątem możliwości ich zastosowania w polityce mającej gwarantować bezpieczeństwo jednostki w cyberprzestrzeni.

Keywords: *cybersecurity, cybersecurity threats, security, hacking, data theft, manipulation, legal framework of safety*

Słowa kluczowe: *cyberbezpieczeństwo, zagrożenia cyberbezpieczeństwa, bezpieczeństwo, hakerstwo, kradzież danych, manipulacja, prawne ramy bezpieczeństwa*

Wprowadzenie

Bezpieczeństwo – zarówno indywidualne, jak i jednostkowe – jest jedną z wartości najbardziej pożądanych przez współczesnego człowieka. Wartość bezpieczeństwa mierzona jest proporcjonalną odwrotnością istniejących zagrożeń. Współczesna skala zagrożeń oraz ich rodzaj są czynnikami determinującymi zachowania jednostki w poszukiwania bezpieczeństwa. Z teoretycznego punktu widzenia jednostka może czuć się bezpieczna wówczas, gdy zostanie stworzona przestrzeń wolna od zagrożeń lub też potencjalne zagrożenia zostaną znacząco zminimalizowane dzięki możliwości szybkiego reagowania na pojawiające się nieporządne zjawiska (Nowacki, 2004, s. 4; Sitek, 2016, s. 385).

Bezpieczeństwo jest przede wszystkim stanem psychicznym, a w dalszej kolejności prawnym. Stąd z psychologicznego punktu widzenia można mówić o poczuciu bezpieczeństwa, które jest wymierną emanacją warunków, w których żyje człowiek. Jego znaczenie uwidacznia się w hierarchii Abrahama Maslowa, wg którego potrzeba bezpieczeństwa jest na drugim miejscu po potrzebach fizjologicznych. W doktrynie można spotkać się z poglądami, zgodnie z którymi potrzeba bezpieczeństwa wyprzedza wszystkie inne, nawet te fizjologiczne. Wpływa na wartościowanie przez człowieka jego otoczenia oraz determinuje jego konkretne decyzje i działania (Klamut, 2012, s. 43).

Otoczenie człowieka stanowi zatem tło dla psychicznego, czyli wewnętrznego poczucia bezpieczeństwa. Każdy człowiek może zatem inaczej szacować swoje bezpieczeństwo w tych samych warunkach zewnętrznych. Taki stan rzeczy jest niewątpliwe powiązany ze zróżnicowaną wrażliwością każdej osoby, ale nie tylko. Kształt oszacowanego przez człowieka poziomu bezpieczeństwa zależy bowiem od zdolności percepcji i przetwarzania dostarczanych z zewnątrz informacji, oceny ich autentyczności (tutaj potrzebne jest doświadczenie, które w praktyce jest znacznie zróżnicowane) (Klamut, 2012, s. 47). Dlatego jednostka poszukuje bezpieczeństwa w ramach większych grup społecznych.

Dzięki rozwojowi technologii termin „cyberprzestrzeń" przestał być ograniczany tylko do sieci komputerowych. Od strony technicznej obejmuje on szeroki wachlarz urządzeń elektronicznych, sieci i współtowarzyszącej im

fizycznej infrastruktury. Pojęcie cyberprzestrzeni zostało zastosowane w założeniach do Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009–2011. Według tego dokumentu cyberprzestrzeń jest rozumiana jako przestrzeń komunikacyjna tworzona przez system powiązań internetowych. W uaktualnionym dokumencie na lata 2011–2016 pojęcie to zostało opisane jako cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami (Kosiński, 2015, s. 33).

Współczesna sytuacja zmienia się wraz z dynamicznym rozwojem nowych technik i technologii informatycznych, na bazie których powstała cyberprzestrzeń. Od dość dawna podejmowane są próby zdefiniowania tego pojęcia, ale głównie w oparciu o koncepcję komunikowania się za pomocą komunikatorów. Ta definicja oddaje tylko w niewielkiej części to, czym jest cyberprzestrzeń (Kosiński, 2015, s. 33). Można również zadać pytanie, czy jest możliwe jej zdefiniowanie. Czy raczej, ze względu na dynamiczny rozwój technik i technologii informatycznych, nie należałoby wymienić obszarów życia człowieka, które stały się częścią nowej przestrzeni aktywności człowieka? Taki właśnie paradygmat-definicja jest bardziej prawdziwy i otwarty na dalsze zmiany oraz obejmowanie tym pojęciem coraz to nowszych obszarów życia (Wasilewski, 2013, s. 225–234).

Można powiedzieć, że cyberprzestrzeń to taki obszar życia, do którego człowiek przeniósł większą część swojej aktywności z dawnego świata realnego. Cyberprzestrzeń to nie tylko możliwość właściwie nieograniczonej komunikacji. Tam właśnie współczesny człowiek dokonuje zakupów, pobiera porady finansowe, medyczne czy korepetycje. Wnosi opłaty związane z codziennym życiem. Świat polityki obecnie funkcjonuje coraz bardziej w cyberprzestrzeni, czego przykładem były wygrane w 2008 r. wybory prezydenckie przez Baracka Obamę w Stanach Zjednoczonych, czy – jak sugeruje Maria Nowina Konopka – również przez Andrzeja Dudę w Polsce w 2015 r. (Nowina Konopka, 2015, s. 89).

Tak szerokie rozumienie cyberprzestrzeni, która obecnie jest dla człowieka światem jak najbardziej realnym, obejmuje również zagrożenia, o których w rzeczywistym świecie nie było mowy. To one wpływają na poczucie współczesnego bezpieczeństwa.

Zagrożenia w cyberprzestrzeni

Zagrożenia, jakie czyhają na człowieka w cyberprzestrzeni i są jednocześnie źródłem zagrożenia, można zgrupować wokół takich problemów jak:

- wykluczenie i uzależnienie,
- cyberprzestępczość.

Wykluczenie i uzależnienie

Cyberprzestrzeń jest dzisiaj sposobem na życie. Już nie w kawiarni czy pod romantycznym drzewem przy zachodzie słońca młodzi ludzie wyznają swoje uczucia. Dobierają się nie na podstawie cech fizycznych czy psychicznych. Portale randkowe oferują partnerów sprofilowanych pod potrzeby, a nawet konkretne zamówienie czy zapotrzebowanie. Tak zwana chemia nie jest już potrzebna do bycia razem.

Ogromnemu przeobrażaniu uległ też stosunek do pracy. Dzięki cyberprzestrzeni wzrosła liczba miejsc pracy, otworzyły się możliwości zwiększenia zarobków. Człowiek może się pełniej realizować.

Dzięki cyberprzestrzeni wzrosła możliwość edukacji, zdobywania nowych kwalifikacji. Uczeń czy student pobierający naukę online zaoszczędza pieniądze na podróż, hotele, materiały dydaktyczne itp. Podnosi się świadomość społeczeństwa, ogólna wiedza. Wprowadzona została koncepcja uczenia się przez całe życie. Tak przynajmniej twierdzą koryfeusze cyberprzestrzeni (Badźmirowska-Masłowska, 2013, s. 59–100; Chodak, 2016, s. 189).

Wymienione przykładowo pozytywne strony realnej cyberprzestrzeni niosą również liczne zagrożenia (Goban-Klas, Sienkiewicz, 1999, s. 64 i n.). Uwidaczniają się one przede wszystkim w wykluczeniu wielu osób z komunikacji. Przyczyn takiego stanu rzeczy należy upatrywać nie tylko w braku dostępu do Internetu (GUS, dane za 2016). Problemem nadal jest brak umiejętności posługiwania się współczesnymi narzędziami informatycznymi. Edukacja techniczna i technologiczna nadal pozostawia wiele do życzenia, zwłaszcza w pokoleniu starszym, poczynając od osób w wieku 50+. Osoby te albo w ogóle nie korzystają z cyberprzestrzeni, albo czynią to w niewielkim stopniu.

Chyba najwięcej zagrożeń ze społecznego punktu widzenia jest w obszarze pracy. Kompleksowa przebudowa procesów gospodarczych wyznacza nowe

kierunki rozwoju różnych form organizacji pracy w instytucjach społeczno-gospodarczych. Jest to konsekwencją wdrażania najnowszych technologii informacyjnych. Coraz więcej osób podejmuje pracę w systemie telepracy, ale też z wykorzystaniem Internetu (tak pracują m.in. księgowe), portalów i witryn internetowych (np. osoby trudniące się reklamą czy pozycjonowaniem postów). Te zmiany w sposobie zatrudniania zawieszają jednak regulacje kodeksowe co do ograniczenia godzin pracy, wypoczynku, urlopu. Osoby pracujące z wykorzystaniem Internetu często wykonują swoją pracę w domu, nie zmieniając swojego środowiska życia, co negatywnie wpływa na człowieka. Taki model pracy nie tylko powoduje lekceważenie zdobyczy XIX i XX w. w zakresie praw pracowniczych, ale wprowadza niewątpliwie dehumanizację relacji pracodawca–pracownik (Pańkowska, 2002, s. 78–98).

Kolejnym obszarem zmian, jakie wprowadza cyberprzestrzeń do życia człowieka, to nauka. Z jednej strony jest łatwiejszy dostęp do nauki, z drugiej jednak dokonuje się dehumanizacja relacji nauczyciel–uczeń czy student. Internet stwarza okazję do wielu nieuczciwych zachowań, jak rozwiązywanie testów przez inne osoby, kupowanie prac dyplomowych czy – coraz częstsza – kradzież praw autorskich lub majątkowych. Tym samym można raczej wątpić, czy ułatwienie dostępu do nauki przyniosło jednocześnie podniesienie jej poziomu.

Zagrożenia cyberprzestępczością

Wszelkie udogodnienia, jakie niesie cyberprzestrzeń, zawierają również zagrożenia, analogicznie jak nóż, który może być pomocny człowiekowi, ale też może stać się narzędziem zbrodni (Roman, 2015, s. 224; Sienkiewicz, 2009, s. 583–592).

Pierwszym rodzajem zagrożeń dla człowieka jest kradzież lub użycie w niedozwolony sposób informacji gromadzonych przez różne instytucje publiczne i prywatne, a nawet przez osoby fizyczne. Mnogość podmiotów gromadzących informacje jest ogromna. Powstał też legalny (za zgodą danej osoby) i nielegalny rynek obrotu informacjami. Człowiek, za sprawą sprzedaży informacji o jego danych osobowych, stał się jakąś jednostką, którą można wycenić tak jak np. akcje czy udziały w spółce z o.o. Najgorsze jednak jest to, że gromadzone informacje mogą być i bardzo często są wykorzystywane do działalności przestępczej w różnych obszarach. Brak kontroli nad bazami da-

nych ułatwia m.in. kradzież tożsamości w celu wysyłania spamu, uzyskania dostępu do cudzego konta bankowego czy podrobienia karty płatniczej, zaciągnięcia niechcianych zobowiązań (np. kredytu) (Lach, 2012, s. 583–592).

Szczególne znaczenie mają informacje dotyczące stanu zdrowia człowieka, które mogą być nielegalnie wykorzystywane przez firmy farmaceutyczne lub dla celów przestępczych, np. szantażu.

Cyberprzestrzeń umożliwia nawiązywanie znajomości. Ta możliwość może być jednak przyczyną licznych nadużyć. Jednym z nich jest grooming, czyli zaprzyjaźnianie się z dziećmi w celach pedofilskich. Takie działanie jest możliwe, bowiem przestępca może ukryć swoją prawdziwą twarz i wykreować fałszywy obraz człowieka miłego czy przyjaciela dzieci (Kozak, 2011, s. 186). Ten sam mechanizm wykorzystywany jest również w odniesieniu do osób dorosłych, lecz mało doświadczonych. W konsekwencji osoby takie zostają wciągnięte mimowolnie w świat pornografii.

Kolejnym rodzajem zagrożenia, jakie niesie cyberprzestrzeń, jest możliwość kradzieży już nie tylko danych osobowych, ale również zasobów zgromadzonych na komputerach prywatnych i jednostek publicznych. Cracking, bo o tym zjawisku jest tu mowa, to sposób łamania zabezpieczeń systemu poprzez kradzież haseł, za pomocą znalezionej luki w zabezpieczeniach systemów komputerowych. W ten sposób tracone się opracowania, opinie, a także zdjęcia zapisywane na komputerach (Białoskórski 2011, s. 81). Zjawiskiem prawie tożsamym z crakingiem jest hakerstwo (ang. *hacking*). Jest z kolei celowe działanie zmierzające do zdobycia konkretnych informacji, często na czyjeś zlecenie.

Kradzież danych z komputerów przez hakerów może służyć do szantażowania, nękania, publikowania i rozpowszechniania kompromitujących zdjęć czy filmów, wyłudzania okupu. Takie działania podejmowane są również w sferze polityki podczas kampanii wyborczych, np. podczas wyborów ostatniego prezydenta USA w 2016 r., którym został Donald Trump. Jak donoszą media, podejrzewa się nawet, że służby rosyjskie wykradły wiele informacji ze sztabu jego kontrkandydatki Hilary Clinton, co mogło przechylić szalę zwycięstwa (Herb, Raju, 2016; *Rosyjscy hakerzy…*, 2017).

Zagrożeń, jakie niesie cyberprzestrzeń, jest bardzo wiele. Konieczna wydaje się jednak choć krótka wzmianka o wykorzystywaniu Internetu czy cyberprzestrzeni przez terrorystów. Terroryści wykorzystują Internet do pro-

mowania i szerzenia swoich idei, do werbowania nowych zwolenników, do komunikacji między sobą. Ale też Internet w ich ręku staje się narzędziem do cyberataków na urządzenia przemysłowe, szpitale, umożliwia przejęcie kontroli nad samolotem, elektrownią czy sygnalizacją świetlną w mieście (Wejkszner, 2010, s. 38–39).

Ramy prawne mające gwarantować bezpieczeństwo w cyberprzestrzeni

Mówiąc o prawnych ramach bezpieczeństwa w cyberprzestrzeni, można wskazać na regulacje międzynarodowe państw wiodących w tym obszarze i wreszcie na systemy prawne poszczególnych krajów. Ze względu na ograniczony wymogami redakcyjnymi rozmiar pracy zmuszona jestem do ograniczenia się do analizy prawa polskiego, zarówno *soft law* jak i *hard law*. Podsumowanie dotychczasowych działań władz polskich znalazło odzwierciedlenie w dokumencie zawierającym informacje o wynikach kontroli NIK-u pt. *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP* (dalej: Informacja NIK-u).

Na postawie analizy Informacji NIK-u można stwierdzić, że władze państwowe w Polsce raczej nie dostrzegają potrzeby zapewniania bezpieczeństwa w cyberprzestrzeni. Podejmowane od 2008 r. działania w tej sferze mają raczej charakter pozorny. Brakuje spójnej wizji systemowej, zaś podejmowane działania miały charakter doraźny, np. w przypadku ataku ACTA. Dostrzega się również bierne oczekiwanie na to, co zaproponuje Unia Europejska (Informacja NIK-u, 2016).

W latach 2008–2011 powstało siedem projektów strategii przeciwdziałania zagrożeniom płynącym z cyberprzestrzeni. Żaden z nich nie został przyjęty przez Radę Ministrów i wdrożony do realizacji. Dokumenty te miały niską jakość merytoryczną. Jedną z istotnych przyczyn takiego stanu rzeczy były sprzeczne interesy poszczególnych resortów na etapie tworzenia projektów strategii (Informacja NIK-u, 2016, s. 34). Zamiast stworzyć prawne ramy dla bezpieczeństwa w cyberprzestrzeni koncertowano się na budowie kompromisu. Była to ślepa uliczka (Zawisza, 2015, s. 408).

W 2012 r. Ministerstwo Administracji i Cyfryzacji przygotowało projekt dokumentu pt. *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*.

Polityka ta została przyjęta uchwałą nr 111/2013 Rady Ministrów w dniu 23 czerwca 2013 r. Przeprowadzona kontrola tego dokumentu wykazała, że również on nie był rzetelnie przygotowany. Nie zostały przeprowadzone niezbędne analizy (Infromacja NIK-u, 2016, s. 36). W konsekwencji jest to „dokument wadliwy, pozbawiony podstawowych cech dokumentu strategicznego i ma jedynie charakter propagandowy" (Informacja NIK-u, 2016, s. 38).

Z kolei Biuro Bezpieczeństwa Narodowego w styczniu 2015 r. przygotowało dokument pt. *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*. Według protokołu NIK-u (https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html) dokument ten stanowi znaczny wkład w zwiększenie świadomości zagrożeń w cyberprzestrzeni. Dalej jest to jednak dokument bardzo ogólny, którego nie można uznać za pełną strategię. Brakuje w nim wskazania konkretnych zadań, podmiotów odpowiedzialnych za ich realizację oraz ich kosztów i źródeł finansowania (Infromacja NIK-u, 2016, s. 38).

W Informacji NIK-u wskazano na brak koordynacji działań pomiędzy poszczególnymi resortami. W konsekwencji wiele z nich się powielało, a centralne organy państwa nie informowały się o podejmowanych działaniach.

Po wygranych przez PiS wyborach parlamentarnych na mocy rozporządzenia Rady Ministrów z dnia 7 grudnia 2015 r. zostało utworzone Ministerstwo Cyfryzacji poprzez przekształcenie dotychczasowego Ministerstwa Administracji i Cyfryzacji. Niestety, do zadań tego Ministerstwa nie zostały *explicite* przypisane zadania z zakresu zapewniania cyberbezpieczeństwa.

Cyberbezpieczeństwo pojawia się w art. 27 Ustawy z dnia 14 grudnia 2016 r. prawo oświatowe (Dz.U. z 2017 r. poz. 59). W artykule tym stwierdzono, że szkoły i placówki oświatowe muszą zabezpieczyć uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju. Chodzi tutaj o ochronę dzieci i młodzieży przed: działaniem złośliwych użytkowników z wnętrza sieci, atakiem ze strony sieci Internet (przypadkowego lub intencjonalnego), dostępem do nieodpowiednich treści (narkotyki, przemoc, pornografia, hazard), naruszaniem praw autorskich (Balicki, Pyter, 2017, Legalis). Szkoły mają stworzyć i wdrożyć politykę bezpieczeństwa internetowego.

Ważnym działaniem obecnego rządu jest wydanie Rozporządzenia Rady Ministrów z dnia 7 czerwca 2017 r. w sprawie Nadania Naukowej i Akade-

mickiej Sieci Komputerowej Statusu państwowego instytutu badawczego. W § 2 pkt. 1d stwierdzono, że jednym ze zdań Naukowej i Akademickiej Sieci Komputerowej (dalej: NASK) jest prowadzenie prac badawczych rozwojowych z zakresu cyberbezpieczeństwa. Z kolei w § 3 pkt. 2 normodawca postanowił, że NASK zapewnienia „cyberbezpieczeństwo podmiotom publicznym w zakresie zlecanym i wskazywanym przez ministra nadzorującego". Zadanie to NASK ma realizować „przez utrzymanie operacyjnego centrum zarządzania cyberbezpieczeństwem sfery cywilnej oraz przez rozwój Narodowego Centrum Cyberbezpieczeństwa (NC Cyber)".

Takie rozwiązanie jest niewątpliwie zdecydowanym krokiem naprzód w kierunku zbudowania systemu bezpieczeństwa w cyberprzestrzeni, chroniącego zwłaszcza przed działaniami złośliwymi, a więc działaniami hakerskimi, cyberatakami itp. (Worona, 2016, s. 466). Działania NASK-u są elementem budowy megasystemu bezpieczeństwa narodowego w Polsce (Rydlewski, 2017, 59). Słabością tego rozwiązania jest jednak ograniczenie tej inicjatywy wyłącznie do sfery publicznej. Pominięcie prywatnego biznesu, a także osób prywatnych może okazać się błędem. Działania władzy publicznej finansowane są przecież ze środków wnoszonych przez podatnika, któremu państwo w zamian za otrzymane środki finansowe winno zapewnić również bezpieczeństwo w cyberprzestrzeni.

Powyższa uwaga jest zasadna także z tego względu, że definicję cyberbezpieczeństwa Polski sformułowano we wspomnianej już wcześniej opracowanej przez Biuro Bezpieczeństwa Narodowego *Doktrynie cyberbezpieczeństwa Rzeczypospolitej Polskiej* z 2015 r. jako „proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni".

Pewną szansą na stworzenie podstaw prawnych i organizacyjnych dla cyberbezpieczeństwa będzie implementowanie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia

Dyrektywy 95/46/WE (Dz.U. U.E. L 119/1). Rozporządzenie potocznie określa się mianem RODO i weszło w życie 17 maja 2016 r. Ma ono obowiązywać bezpośrednio w krajowych porządkach prawnych od 25 maja 2018 r. Zgodnie z art. 1 pkt. 1 tego rozporządzenia przedmiotem regulacji jest ochrona „osób fizycznych w związku z przetwarzaniem danych osobowych". Materialny zakres stosowania Rozporządzenia został określony w art. 2 pkt. 1, w który postanowiono, że ma ono „zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych".

W art. 3 bardzo szeroko zostali zdefiniowani adresaci obowiązków określonych Rozporządzeniem. Praktycznie każdy podmiot, publiczny i prywatny, który posiada lub w jakiekolwiek sposób przetwarza dane osobowe zobowiązany jest do stosowania przepisów tego aktu prawnego. Przede wszystkim jednak Rozporządzenie wiązać będzie wszystkich, którzy przetwarzają dane osobowe w związku z prowadzoną działalnością gospodarczą. Tym samym ciężar ochrony, w tym finansowy, został przerzucony na barki podmiotów prywatnych. Miernikiem nowej filozofii ochrony danych osobowych są kary przewidziane za naruszenie postanowień Rozporządzenia, tj. nawet 10 mln euro lub 2% całkowitego rocznego światowego obrotu przedsiębiorcy z roku obrotowego poprzedzającego naruszenie (art. 83 pkt. 5 Rozporządzenia). Wysokość tych kar ma charakter wyłącznie represyjny.

Wprowadzenie do polskiego systemu prawnego Rozporządzenia 2016/679 nie rozwiązuje sprawy regulacji prawnych, których celem byłoby zagwarantowanie cyberbezpieczeństwa. Rozporządzenie dotyczy bardzo wąskiego kręgu problemów bezpieczeństwa w cyberprzestrzeni.

Zakończenie – wnioski końcowe

Przedstawione w pracy bardzo pobieżnie problemy związane z cyberprzestrzenią, korzyści, ale też i wszelkie zagrożenia z nią związane pokazują wagę i potrzebę prowadzenia dyskusji naukowej o cyberbezpieczeństwie. Jednym z podstawowych elementów stworzenia cyberbezpieczeństwa jest skontrowanie jego ram prawnych.

Przedstawiona analiza dotychczasowych działań władz publicznych w Polsce pokazuje, że kwestią zapewnienia cyberbezpieczeństwa w Polsce zaczęto zajmować się dopiero pod koniec pierwszej dekady obecnego stulecia. Przygotowane wówczas dokumenty, zawierające wyłącznie strategie, są zaliczane co najwyżej do *soft law*. Infromacja NIK-u z 2015 r. pokazała, że strategie te zostały bardzo słabo przygotowane i nie mogą stanowić podstawy działań władzy publicznej na rzecz cyberbezpieczeństwa w Polsce.

Dopiero w 2016 r. stworzono instytut badawczy na bazie NASK-u, którego celem jest budowanie systemu bezpieczeństwa w cyberprzestrzeni. Instytucja ta jednak nie została wyposażona w instrumenty, chociażby takie jak inicjatywa ustawodawcza.

Wobec tych faktów należy stwierdzić, że w Polsce mamy do czynienia zasadniczo z pustynią prawną w obszarze cyberprzestrzeni. Nie zapewnia jej wejście życie do polskiego porządku prawnego unijnego rozporządzenia w maju 2018 r. Konieczne jest podjęcie działań legislacyjnych, chociażby zmian w Kodeksie karnym, w którym winny znajdować się kary przewidziane za wszelkiego rodzaju negatywne działania w Internecie. Należy stworzyć w warstwie normatywnej konkretne formy przestępczego działania i przypisać im odpowiednie sankcje.

Literatura

Badźmirowska-Masłowska, K. (2013). *Ochrona małoletnich w środowisku mediów audiowizualnych, Internetu i innych usług online przed współczesnymi zagrożeniami w świetle dokumentów Rady Europy. Wybrane aspekty prawne*, „Journal of Modern Science" 1/16, s. 59–100. ISSN 1734-2031.

Balicki, A. Pyter, M. (2017). *Prawo oświatowe. Komentarz*, Warszawa: C.H. Beck. ISBN 9788325597757. Legalis.

Białoskórski, R. (2011). *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Warszawa: Wydawnictwo Wyższej Szkoły Cła i Logistyki. ISBN 9788389226853.

Chodak, P. (2016). *Czy szkoła jest bezpieczna dla uczniów? Skala przestępczości*, „Journal of Modern Science" 1/28, s. 179–194. ISSN 1734-2031.

Gibuła, P. (2016). *Działania na rzecz bezpieczeństwa teleinformatycznego Polski. Niebezpieczna cyberprzestrzeń*, „Kontrola Państwowa" nr 61, s. 52–64. ISSN 0452-5027.

Goban-Klas, T. Sienkiewicz, P. (1999). *Społeczeństwo informacyjne: szanse zagrożenia, wyzwania*, Kraków: Fundacja Postępu Telekomunikacji. ISBN 8386476192.

Informacja NIK-u o wynikach kontroli *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* z 23 czerwca 2015 r. Nr ewid. P/14/043.

Klamut, R. (2012). *Bezpieczeństwo jako pojęcie psychologiczne*, „Zeszyty Naukowe Politechniki Rzeszowskiej", Ekonomia i nauki Humanistyczne, z. 19(4), s. 41–51. ISSN 1234-3684.

Kosiński, J. (2015). *Paradygmaty cyberprzestępczości*, Warszawa: Difin, ISBN 978837930666.

Kozak, S. (2011). *Patologie komunikowania w Internecie. Zagrożenia i skutki dla dzieci i młodzieży*, Warszawa: Difin. ISBN 9788376413884.

Lach, A. (2012). *Kradzież tożsamości*, „Prokuratura i Prawo" nr 3, s. 29–40. ISSN 1233-2577.

Nowacki, G. (2004). *Psychologia bezpieczeństwa*, Warszawa: Akademia Obrony Narodowej.

Nowina Konopka, M. (2015). *Czy Andrzej Duda wygrał dzięki internetowi?*, „Przegląd Polityczny" nr 2, s. 89 (87–100). ISSN 1232-6488.

Pańkowska, M. (2002). *Nowe formy organizacji pracy w cyberprzestrzeni*, Prace Naukowe/Akademia Ekonomiczna w Katowicach, Katowice: Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, s. 78–98. ISSN 2083-8611.

Roman, Ł. (2015). *Istota współczesnych wyzwań i zagrożeń bezpieczeństwa*, „Journal of Modern Science" 4/27, s. 209–226. ISSN 1734-2031.

Rydlewski, G. (2017). *Megasystem bezpieczeństwa narodowego w Polsce. Ujęcie procesowe i funkcjonalno-decyzyjne*, Toruń: Adam Marszałek. ISBN 9788380197756.

Sienkiewicz, P. (2009). *Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni*, „Automatyka/Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie" t. 13, z. 2, s. 583–592. ISSN 1429-3447.

Sitek, B. (2016). *Zasady etyczne stosowane w cyberprzestrzeni*. W: B. Sitek, J. Knap, S. Sagan, Ł. Roman, *Nowoczesne narzędzia informatyczne w przeciwdziałaniu zagrożeniom bezpieczeństwa*, Józefów: Wydawnictwo WSGE, s. 71–84. ISBN 9788362753789.

Wasilewski, J. (2013). *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" nr 9, t. 5, s. 225–234. ISSN 2080-1335.

Wejkszner, A. (2010). *Ewolucja terroryzmu motywowanego ideologią religijną na przykładnie salafickiego ruchu globalnego dżihadu*, Poznań: Uniwersytet im. Adama Mickiewicza. ISBN/ISSN: 9788360677858.

Worona, J. (2016). *Prace naczelnych organów administracji państwowej a cyberbezpieczeństwo Polski*, „Białostockie Studia Prawnicze" nr 20B, s. 465–474. ISSN 1689-7404.

Zawisza, J. (2015). *Cyberprzestrzeń jako zagrożenie bezpieczeństwa państwa*, „Journal of Modern Science" 4/27, s. 403–416. ISSN 1734-2031.

Źródła internetowe

GUS, *Społeczeństwo informacyjne w Polsce w 2016 r.*, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2016-roku,2,6.html (dostęp: 2.11.2017).

Herb, J. Raju, M. (2017). *Russia investigators probe GOP operative who sought Clinton emails*, CNN Politics z 16 października 2016 r., http://edition.cnn.com/2017/10/16/politics/peter-w-smith-house-intelligence-committee/index.html (dostęp: 4.11.2017).

Rosyjscy hakerzy, którzy przejęli korespondencję sztabu Clinton, zaatakowali polskie MSZ!, „Dziennik Narodowy" z 31 stycznia 2017 r., http://www.dzienniknarodowy.pl/5114/rosyjscy-hakerzy-ktorzy-przejeli-korespondencje-sz/ (dostęp: 4.11.2017).