Cyberbezpieczeństwo – w kierunku redefinicji odpowiedzialności w cyberprzestrzeni

*dr hab. prof. ALK Katarzyna Chałubińska-Jentkiewicz**

W ostatnim czasie, poza aspektem technologicznym zmian społecznych dotyczących nowoczesnych technologii, w szczególności związanym z tak powszechnie dyskutowaną Sztuczną Inteligencją, istotna staje się kwestia wzmocnienia bezpieczeństwa w cyberprzestrzeni. Celem działań regulacyjnych staje się dostęp do wiarygodnych źródeł informacji, zapewnienie porządku publicznego i poszanowania praw podstawowych w działalności e-commerce, wzmocnienie zadań podmiotów odpowiedzialnych za infrastrukturę kluczową dla prawidłowego funkcjonowania państwa i jego obywateli. Ta zmiana stanowi podstawę nowej odpowiedzialności za treści nielegalne i treści szkodliwe. Jednak to państwo odgrywa ważną rolę regulatora rzeczywistości opartej na danych. W artykule podjęto próbę ustalenia jak te uwarunkowania wpływają na redefinicję pojęcia cyberbezpieczeństwa, a w konsekwencji na nowe reguły cyber odpowiedzialności w kręgu nowych podmiotów zobowiązanych do aktywności na rzecz cyberbezpieczeństwa.

Od redefinicji bezpieczeństwa do definicji cyberbezpieczeństwa

Jednym z podstawowych obszarów, który obecnie wymaga redefiniowania, jest bezpieczeństwo. W teorii nauk o bezpieczeństwie przyjmuje się, że pojęcie bezpieczeństwa (od łacińskiego *sine cura* – „bez pieczy") jest interpretowane przede wszystkim jako stan braku zagrożenia[1]. Równocześnie „bezpieczeństwo" to proces, ponieważ bezpieczeństwo i jego organizacja stale podlegają zmianom, a co za tym idzie nie można uznać, że jest ono trwale ustanowione i zorganizowane[2]. W tym ujęciu **bezpieczeństwo** oznacza „ciągłą działalność jednostek, społeczności lokalnych, państw czy organizacji międzynarodowych w tworzeniu pożądanego stanu bezpieczeństwa"[3]. Szczególna odmiana bezpieczeństwa, czyli cyberbezpieczeństwo, może być definiowana zarówno poprzez odniesienie do pożądanego stanu, jak i jako stale realizowany proces prowadzący do takiego stanu. W wyniku zmian technologicznych pojęcie bezpieczeństwa Państwa coraz silniej wiąże się z bezpieczeństwem cyberprzestrzeni i jej użytkowników. **Cyberbezpieczeństwo** staje się głównym celem nowych rozwiązań, których na bieżąco wymaga zmieniająca się cyberprzestrzeń. Należy zaznaczyć, że jednocześnie bezpieczeństwo w cyberprzestrzeni jest niezbędnym elementem prawidłowego postępu naukowo-technicznego i jako takie określa potrzeby ochrony tego obszaru nie tylko z punktu widzenia użyteczności, ale również ze względu na przeciwdziałanie zupełnie nieznanym dotąd zagrożeniom. W dobie globalnej informatyzacji, także sfery publicznej, w warunkach rozwoju portali społecznościowych, wszechobecnego mailingu często dochodzi do nieuprawnionych działań, które mogą stanowić naruszenie dóbr osobistych, prawa własności czy praw konsumenckich. Jednak coraz częściej pojawiają się także innego typu cyber-zagrożenia, które dotykają struktur władzy publicznej i samego Państwa, zwłaszcza jego infrastruktury krytycznej. I właśnie to ostatnie pojęcie najczęściej wiązane jest z definicją cyberbezpieczeństwa. Współcześnie, kiedy strefa prywatności człowieka wolna od ingerencji osób trzecich stopniowo się kurczy, w jednakowym, a może nawet większym stopniu proces ten dotyka obszaru prawidłowego działania administracji publicznej oraz jej służb, także służb specjalnych, których zadania wyznaczają zagrożenia związane z nowymi technologiami. Jak podkreśla *W. Kitler* działanie systemu bezpieczeństwa narodowego w cyberprzestrzeni ma swoje dwa wymiary: cyberbezpieczeństwa i bezpieczeństwa cyberprzestrzeni, co dotyczy odpowiednio: bezpiecznego (wolnego od zakłóceń) funkcjonowania systemu i jego elementów w cyberprzestrzeni oraz niezakłóconej pracy przestrzeni wirtualnej, tj. sieci współpracujących lub komunikujących się ze sobą komputerów, telefonów, telewizorów tabletów i innych urządzeń z ich użytkownikami włącznie[4].

Dotychczasowe podejście regulatorów do zagadnienia cyberbezpieczeństwa wynikało z utożsamiania tego rodzaju ochrony z potrzebą przeciwdziałania atakom nakierowanym na same sieci, co wydaje się nieuzasadnione, zwłaszcza w kontekście analizy pojęcia cyberprzestrzeni. *J. Wasilewski* stwierdzał, że: „O ile zatem z definicji domeny cyfrowej wyłącza się jej użytkowników, bezpieczeństwo tak ujętej cyberprzestrzeni będzie skupiać się na zapewnieniu ochrony elementów infrastrukturalnych. Z kolei dodanie do przedmiotowej definicji relacji pomiędzy użytkownikami a podbudowującym cyberprzestrzeń sprzętem oraz relacji pomiędzy samymi użytkownikami (użytkownik – cyberprzestrzeń jako medium – użytkownik) narzuca konieczność pojmowania bezpieczeństwa tego obszaru w sposób zdecydowanie bardziej dynamiczny, zwłaszcza, że jest on pełny ludzkich

* Autorka jest dr. hab. profesorem Akademii Leona Koźmińskiego, dyrektorem Rejestru Domen Internetowych w NASK PIB; ORCID: 0000-0003-0188-5704.

[1] *Z. Ściborek, B. Wiśniewski, R.B. Kuc, A. Dawidczyk*, Bezpieczeństwo wewnętrzne. Podręcznik akademicki, Toruń 2015, s. 26.

[2] *J. Marczak*, Bezpieczeństwo narodowe [w:] *R. Jakubczak, J. Marczak*, Bezpieczeństwo narodowe Polski w XXI wieku, Warszawa 2011, s. 15.

[3] *Ibidem*, s. 15.

[4] Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne pod red. *W. Kitlera, J. Taczkowskiej-Olszewskiej*, Warszawa 2017, s. 19.

działań o najróżniejszych konotacjach prawnych"[5]. Takie dynamiczne ujęcie cyberbezpieczeństwa przyjęto w Doktrynie Cyberbezpieczeństwa Rzeczypospolitej Polskiej[6] stwierdzając, że jest to „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.

Zdaniem *C. Banasińskiego*, cyberbezpieczeństwo można sprowadzić do „sposobu wolnego od zakłóceń gromadzenia, przetwarzania i wymiany informacji utrwalonych i przetwarzanych w sposób cyfrowy"[7]. W państwach zaangażowanych w budowę społeczeństwa informacyjnego, bezpieczeństwo cyberprzestrzeni uznawane jest za jedno z najpoważniejszych wyzwań w systemie bezpieczeństwa narodowego. Odnosi się ono zarówno do bezpieczeństwa całej instytucji państwa, jak i poszczególnych obywateli. Istotne znaczenie dla zapewnienia cyberbezpieczeństwa ma prawidłowe funkcjonowanie administracji publicznej. W ostatnich latach dokonała się także ewolucja w rozumieniu pojęcia bezpieczeństwa narodowego pod względem przedmiotowym. Przy definiowaniu cyberbezpieczeństwa zauważono znaczenie nie tylko aspektów militarnych czy politycznych, ale także m.in. ekonomicznych, kulturowych, ekologicznych i ideologicznych. Należy zatem przyjąć, że cyberbezpieczeństwo jest zjawiskiem interdyscyplinarnym, korzystającym z dorobku wielu innych dziedzin (w tym z różnych dziedzin prawa). Aby jednak wyodrębnić je z całego systemu prawa i administracji publicznej (w tym drugim przypadku przede wszystkim organizacyjnie i podmiotowo), konieczne jest określenie zakresu działania, jakiego sfera ta dotyczy (zarówno w sensie przedmiotowym, podmiotowym, organizacyjnym, jak i funkcjonalnym). Dopiero wówczas możliwe będzie usystematyzowanie tego pojęcia. Obecnie, w dobie regulacji związanych ze środowiskiem cyfrowym, zabieg ten staje się niezbędny.

Określenie definicji bezpieczeństwa cyberprzestrzeni związane jest z potrzebami przywołanej już Doktryny Cyberbezpieczeństwa RP, zgodnie z którą ,,część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych". Przywołane określenie podkreśla aspekt funkcjonalny bezpieczeństwa cyberprzestrzeni, czyli działania mającego na celu ochronę tego środowiska oraz jego użytkowników. Postępująca cyfryzacja i automatyzacja kolejnych dziedzin życia sprawiają, że z każdym dniem coraz większa liczba procesów pozbawionych cyfrowego wsparcia stałaby się niemożliwa do realizacji. Skutkami tych zmian, które są coraz bardziej widoczne, jest uzależnienie się społeczeństwa od cyberprzestrzeni i procesów cyfrowych.

Definiowanie cyberbezpieczeństwa w dokumentach strategicznych

Do sieci przenosi się także coraz większa część ludzkiej aktywności, a łatwość dostępu do informacji, a także do technologii umożliwiających jej generowanie i rozpowszechnianie, wpływa jednocześnie na stały wzrost podaży danych. Skokowo rośnie też globalna sieć agregująca wiedzę, informacje oraz dostęp do rozrywki i platform komunikacyjnych. W ciągu każdej sekundy internauci dokonują setek tysięcy operacji w różnego rodzaju serwisach społecznościowych czy transakcyjnych. Jak podaje *J. Surma*: „Dzienna średnia liczba użyć przeglądarki Google wynosi około 3,5 miliarda. Zakładając, że każde użycie pochodzi od innej osoby, to niemal co drugi człowiek na kuli ziemskiej dokonuje jednego wyszukiwania dziennie! Liczba użytkowników Facebooka to 25% populacji całego świata. W przypadku Polski prawie 70% całej populacji używa Google i niemal 60% jest użytkownikami Facebooka"[8]. Równocześnie niezwykle intensywnie rozwija się koncepcja Internetu rzeczy (*Internet of Things* – IoT), w której otaczające nas urządzenia codziennego użytku stają się częścią transgranicznego systemu wymiany informacji. Nowy wymiar cyberbezpieczeństwa pojawia się w związku z rozwojem mediów cyfrowych, jednolitego rynku cyfrowego oraz sztucznej inteligencji. Świat cyfrowy to także przestrzeń, w której aktywnie i kreatywnie korzystając z nowych narzędzi, działają zorganizowane grupy przestępcze, udoskonalając nowe metody popełniania znanych przestępstw, a także tworząc ich całkiem nowe kategorie. W wymiarze geopolitycznym i instytucjonalnym to jednocześnie dla wielu krajów atrakcyjne miejsce do realizowania celów politycznych, zadań wywiadowczych czy swoistej projekcji siły z wykorzystaniem instrumentów marketingowych oraz informacji – w ramach tzw. dezinformacji.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej[9] określa cyberbezpieczeństwo jako ,,(…) Każde znaczące zakłócenie funkcjonowania cyberprzestrzeni, czy to o charakterze globalnym, czy lokalnym, będzie miało wpływ na bezpieczeństwo obrotu gospodarczego, poczucie bezpieczeństwa obywateli, sprawność funkcjonowania instytucji sektora publicznego, przebieg procesów produkcyjnych i usługowych, a w rezultacie na ogólnie pojmowane bezpieczeństwo narodowe (…)"[10]. Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę podkreśla, że: „Cyberbezpieczeństwo stanowi integralny element bezpieczeństwa Europejczyków. (…) Poprawa cyberbezpieczeństwa jest zatem niezbędna, aby ludzie ufali innowacjom, łączności i automatyzacji, używali ich i czerpali z nich korzyści, a także aby zapewnić ochronę podstawowych praw i wolności, w tym prawa do prywatności i ochrony danych osobowych

[5] *J. Wasilewski*, Zarys definicyjny cyberprzestrzeni, ,,Przegląd Bezpieczeństwa Wewnętrznego" Nr 9/2013, s. 232.

[6] Doktryna Cyberbezpieczeństwa RP, https://en.bbn.gov.pl/ftp/dok/01/DCB.pdf (dostęp: 28.10.2024 r.).

[7] *C. Banasiński*, Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni [w:] Cyberbezpieczeństwo. Zarys wykładu, pod red. *C. Banasińskiego*, Warszawa 2018, s. 33.

[8] *J. Surma*, Cyfryzacja życia w erze Big Data, Warszawa 2017, s. 74; autor wskazuje jednocześnie, że: „Tak powszechne wykorzystanie Google'a, Facebooka i innych podobnych firm globalnej gospodarki ma niebagatelne znaczenie dla bezpieczeństwa poszczególnych państw i całego świata" (s. 74).

[9] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 zastąpiła Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 przyjęte uchwałą nr 52/2017 Rady Ministrów z 27.4.2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Uchwała nr 125 Rady Ministrów z 22.10.2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, „Monitor Polski" 2019, poz. 1037.

[10] *Ibidem*, s. 23.