

PIOTR LEBELT, OSKAR RADŁOWSKI¹

Cyberbezpieczeństwo w perspektywie rozwoju e-partycypacji i w obliczu zagrożeń ery cyfrowej

1. Wprowadzenie

Odpowiedzią na nadejście wielkiego rozwoju technologicznego, który nie ominie żadnego aspektu życia, jest e-partycypacja, która wiąże się z zaangażowaniem obywatelskim za pośrednictwem nowych technologii komunikacyjnych. Utworzenie platform służących partycypacji – zespołu działań, który służy do rozwiązywania problemów z inicjatywy społecznej – przeniesie nas obywateli w nowy wymiar postrzegania, ale również rozumienia teraźniejszej instytucji społeczeństwa obywatelskiego. Narzędzia technologii informacyjno-komunikacyjnych (ang. *Information and Communications Technology*, ICT) pozwalają realizować wiele różnych celów związanych z zaangażowaniem obywateli we współdecydowanie o ich sprawach. Przykładowo za pomocą internetowych petycji obywatele mogą w szybkim tempie zebrać wystarczającą liczbę podpisów do osiągnięcia danego celu. Nowe technologie umożliwiają również, z niespotykaną wcześniej łatwością, komunikowanie się na linii obywatele – władze, jak i pomiędzy samymi obywatelami. Za sprawą serwisów mapowych obywatele mogą błyskawicznie zgłaszać urzędnikom problemy, jakie występują w danym miejscu. E-partycypacja w najbliższych latach będzie rozwijać się coraz bardziej, co stworzy nam wiele szans, ale również ściąganie na nas wiele potencjalnych zagrożeń, przed którymi będziemy musieli się zabezpieczyć. W artykule zostaną omówione historia społeczności obywatelskiej oraz zagadnienia e-partycypacji i cyberbezpieczeństwa w kontekście społeczeństwa obywatelskiego. W artykule szczegółowo opisano mechanizmy oraz narzędzia uczestnictwa w dobie elektronicznej partycypacji, skupiono

¹ Piotr Lebelt – Instytut Prawa, Ekonomii i Administracji, Uniwersytet Komisji Edukacji Narodowej w Krakowie, e-mail: piotr.lebelt@student.up.krakow.pl; Oskar Radłowski – Instytut Prawa, Ekonomii i Administracji, Uniwersytet Komisji Edukacji Narodowej w Krakowie, e-mail: oskar.radlowski@student.up.krakow.pl.

się na potencjalnych zagrożeniach – cyberprzestępczości – oraz w szczególności na wyzwaniach w zapewnieniu cyberbezpieczeństwa. Rozwój szeroko rozumianej partycypacji w dobie technologicznych przemian mimowolnie przekształca strukturę sektorów ludzkiej działalności w polityce, gospodarce, infrastrukturze i w wielu innych sektorach. W tym artykule, oprócz możliwości związanych z elektronicznymi narzędziami służącymi do zrzeszania obywatelskiego, poruszone są także kwestie destrukcyjnie wpływające na jednostki i masy funkcjonujące w sieci, nakreślone zostały perspektywy na radzenie sobie z przeszkodami stojącymi przed sektorami publicznymi oraz możliwości, jakimi te sektory obecnie dysponują, do ochrony przed atakami cybernetycznymi. Na razie społeczeństwo i całe państwo nie są gotowe na tak szybkie przemiany technologiczne w dziedzinie partycypacji obywatelskiej – wynika to z braku odpowiednich narzędzi, zapewniających bezpieczne z niej korzystanie. Należy zwrócić uwagę na działania podjęte przez państwa i ich sektory publiczne oraz ocenić, czy obecnie są one wystarczające do wprowadzenia demokracji internetowej.

2. Mechanizmy e-partycypacji, crowdsourcing i jej narzędzia uczestnictwa – znaczenie w życiu społecznym

Współcześnie e-partycypacja umożliwia poszerzenie i pogłębienie uczestnictwa w życiu społecznym, co przyczynia się do większego zaangażowania w działalność społeczną obywateli. Przy pomocy technologii informacyjno-komunikacyjnych obywatele mogą szybko i łatwo nawiązywać ze sobą kontakty oraz swobodniej kontaktować się z urzędnikami czy innymi przedstawicielami władzy. W przeciwieństwie do tradycyjnych metod partycypacyjnych nowoczesne technologie sprzyjają dotarciu do grupy odbiorców w krótkim czasie i w zrozumiałym sposób, w bardziej przystępnej formie. Tym samym e-partycypacja jawi się jako odpowiedź na współczesne potrzeby społeczeństw demokratycznych oraz narzędzie kształtowania polityki przez obywateli. Wśród najważniejszych mechanizmów e-partycypacji należy wymienić: głosowanie elektroniczne (e-wybory) i e-referendum, petycje internetowe, elektroniczne konsultacje oraz crowdsourcing. Ich szczególna rola objawia się w tym, że wspierają bardziej aktywne i świadome uczestnictwo obywateli w życiu publicznym, co jest kluczowe dla zdrowego funkcjonowania demokracji.

E-wybory w *Europeane Participation Report* z listopada 2009 r. zdefiniowane zostały jako wybory polityczne lub referenda, w których środki elektroniczne wykorzystywane są na jednym lub kilku etapach. Najbardziej powszechne jest oddawanie głosu z wykorzystaniem mechanizmu e-głosowania. Elektroniczne głosowanie pozwala przyspieszyć procedury, skrócić czas całego procesu i zredukować koszty związane z organizacją tradycyjnego głosowania. Ponadto zdalna forma zapewnia wygodę obywatelom, w szczególności osobom ze szczególnymi potrzebami: pozwala głosować z dowolnego

miejsca i w dowolnym czasie (ograniczonym jedynie do czasu przeznaczonego na głosowanie, np. dwa tygodnie). Wspomniane czynniki mogą zwiększyć frekwencję wyborczą oraz zaangażowanie obywateli. Jednak trzeba mieć świadomość wad tego rozwiązania, np. przepaści cyfrowej między danymi grupami w społeczeństwie. W wielu krajach skorzystano już z rozwiązania e-głosowania, a inne państwa przygotowują się do jego wdrożenia. Aby uporządkować tę tematykę, przedstawimy trzy sposoby wykorzystywania nowych technologii podczas głosowania internetowego.

Pierwszy z nich polega na zbieraniu i przedstawieniu wyników głosowania przeprowadzonych tradycyjną metodą, przy których systemy komputerowe pełnią rolę pomocniczą, np. wspomagają przekazywanie wyników z komisji do centrali krajowej. Drugi sposób obejmuje elektroniczne wspomaganie głosowania przez maszyny zwane głosomatami. Są to specjalne maszyny służące do przyjmowania i zliczania głosów. Ostatnim sposobem wykorzystywania nowych technologii jest głosowanie przez Internet. W tym przypadku głosy są oddawane zdalnie, z dowolnego miejsca, bez konieczności udania się do lokalu wyborczego. Przyjmowaniem i zliczaniem głosów zajmuje się centralny komputerowy system wyborczy².

Głosowanie internetowe jest obecnie przedmiotem dyskursu naukowego, a nie rzeczywistą praktyką wprowadzaną do systemu wyborczego państw. E-głosowanie w wyborach powszechnych budzi liczne kontrowersje dotyczące wymagań konstytucyjnych; duże wątpliwości wzbudza bezpieczeństwo tych wyborów, zabezpieczenie ich może być bowiem bardzo trudne do zrealizowania.

Kolejnym mechanizmem e-partycypacji są petycje internetowe. Polegają one na elektronicznym skierowaniu zbiorowego pisma lub protestu do władz. Osoby podpisujące się pod daną petycją umieszczają w Internecie swoje nazwiska i adresy zamieszkania. E-petycje są potencjalnie przydatną formą uczestnictwa społeczeństwa w życiu politycznym – pozwalają na szybkie zebranie podpisów, liczne dyskusje na portalach internetowych, integrację społeczną oraz rozwój społeczeństwa obywatelskiego³.

Ostatnim zagadnieniem są e-konsultacje, czyli sposób wyrażania, integrowania i gromadzenia opinii obywateli. Istnieją dwie formy konsultacji: badania opinii publicznej oraz dyskusje polityczne przeprowadzane drogą elektroniczną⁴. E-konsultacje umożliwiają obywatelom wywieranie bezpośredniego i pośredniego wpływu na proces podejmowania decyzji. Dla polityków ten mechanizm może być przydatny choćby w celu przetestowania programu politycznego. E-konsultacje mają duże szanse na powszechne stosowanie w przyszłości. Organizowanie forów politycznych pozwoli obywatelom

2 R. Balicki, *E-voting przyszłość demokracji?*, „CBKE e-BIULETYN” 2007, nr 3.

3 I. Harechko, *Basic Mechanisms of E-participation of Citizens in Policy-Making*, „Toruńskie Studia Międzynarodowe” 2011, nr 1 (4), s. 2.

4 Przykładem zastosowania e-konsultacji jest fińska strona <https://www.otakantaa.fi>, na której obywatele tego kraju mogą uczestniczyć w chatkach.

wyrażać swoje zdanie na temat różnych wniosków i zgłaszać projekty, a urzędnikom – zapoznać się z tymi opiniami⁵.

Wraz z rozwojem nowych technologii i mediów społecznościowych pojawiło się pojęcie crowdsourcingu. Jest to cyfrowy model wykorzystania inteligencji internautów w celu rozwiązania danego problemu lub pozyskania informacji poprzez oddelegowanie danych zadań do tłumu przez organizatora. Choć ta idea powstała stosunkowo niedawno i uważana jest za przyszłość biznesu i partycypacji obywatelskiej, to jej początki sięgają czasów wojen napoleońskich⁶. Obecnie z crowdsourcingiem obywatele mogą się zetknąć przy głosowaniach na projekty realizowane z budżetu obywatelskiego. Takie rozwiązania są bardzo rozsądne, ponieważ to obywatele najlepiej wiedzą, z jakimi problemami mają do czynienia na co dzień, które aspekty życia w okolicy są najbardziej zaniedbane i co należy zmienić lub naprawić⁷.

3. Przystępność i konflikty w kontekście tworzenia się cyberspołeczności

Jesteśmy świadkami tworzenia się nowej społeczności, a nawet nieświadomie stanowimy jej część. Na skutek przemian technologicznych, industrializacji i rozwoju państw powstaje cyberspołeczność, z nową kulturą i zasadami. Globalne społeczeństwo charakteryzuje się łatwym i powszechnym dostępem do informacji⁸.

Wyrok NSA z dnia 30 października 2002 r. traktuje informacje jako wszelkie informacje wytwarzane przez różnego rodzaju podmioty publiczne lub gospodarujące publicznym mieniem, niezależnie od tego, przez kogo zostały one stworzone. Obszerny zakres działalności podmiotów publicznych ma znaczący wpływ na równie duże ich występowanie. Powszechność informacji oznacza, że wykorzystywane są one do bardziej przystępnej formy komunikacji, a co za tym idzie, tworzenia się społeczności posiadającej własną specyfikę i rządzącej się swoimi zasadami. Zasady te oraz przepływ informacji wymagają pewnego unormowania w celu umożliwienia prawidłowego funkcjonowania cyberspołeczności, co z pewnością jest utrudnione przez brak własnego terytorium czy innego miejsca, któremu można przypisać sferę jej działań⁹.

Aktywność państwa coraz bardziej uzależniona jest od możliwości technologicznych, którymi dysponuje. Możliwości informacyjne i komunikacyjne

5 I. Harechko, *Basic Mechanisms...*

6 S. Barczak, *Crowdsourcing. Co to znaczy? Przykłady w Polsce i za granicą*, <https://interviewme.pl/blog/crowdsourcing> (4.09.2024).

7 E. Stokłuska, *E-partycypacja – o co właściwie chodzi i jak to może wyglądać*, <https://publicystyka.ngo.pl/e-partycypacja-o-co-wlasciwie-chodzi-i-jak-to-moze-wygladac> (4.09.2024).

8 *Cyberbezpieczeństwo wyzwaniem XXI wieku*, red. T. Dębowski, Łódź–Wrocław 2018, s. 33.

9 *Ibidem*, s. 31.

stały się podstawą prawidłowego, a nawet podstawowego funkcjonowania obywateli. Cyberprzestrzeń determinuje funkcjonowanie państwa, dlatego też utworzono nowe pojęcie: cyberdemokracji – a ta powstała na skutek wykorzystywania technologii, funkcjonowania jednostki w społeczeństwie oraz działań administracji publicznej. Cyberdemokracja stanowi szansę na wzmocnienie roli jednostki w życiu społecznym, ale stawia także przed obywatelami konkretne wyzwania. Wraz z powstaniem globalnej sieci pojawiły się konkretne zachowania, w tym również anomalie¹⁰, co może być istotnym problemem dla partycypacji i życia całej społeczności¹¹.

Cyberprzestrzeń funkcjonuje w każdej sferze życia społecznego, a koszty ekonomiczne związane z cyberprzestępczością obejmują równie szeroki zakres, a więc straty finansowe związane z kradzieżą danych, koszty naprawy systemów informatycznych oraz straty reputacyjne dla firm i instytucji. Jednym ze szczególnie niebezpiecznych trendów mogących znacząco zagrażać przedsiębiorcom i instytucjom publicznym jest wzrost złożoności i innowacyjności ataków cybernetycznych. Przykładem jest rozwój ransomware'u¹². Jest to złośliwe oprogramowanie szyfrujące dane zapisane na komputerze, blokujące dostęp do niego. Robak Petya to typ ransomware'u, za pomocą którego w 2017 r. przeprowadzono atak na infrastrukturę IT wielu przedsiębiorców głównie na Ukrainie, jednak inne kraje również zostały nim dotknięte, w tym Polska¹³. Ofiarami były firmy, instytucje rządowe, banki, linie lotnicze i media. Petya atakował sektory rozruchowe dysków twardych, co sprawiło, że system operacyjny nie mógł się uruchomić. Celem było wymuszenie¹⁴. Wniosek, jaki nasuwa się po tym incydencie, jest jeden: należy wzmocnić systemy bezpieczeństwa cybernetycznego na szczeblu globalnym oraz tworzyć kopie zapasowe danych, by w przypadku ataku – nawet jeśli utracimy oryginalne dane – pozostały kopie. Innym przestępstwem jest phishing, w którym chodzi o wyłudzenie danych poufnych. Przestępcy wysyłają w tym celu maile lub SMS-y oraz prowadzą fałszywe strony internetowe. W tej formie manipulacji wykorzystywana jest właściwa tylko ludziom emocjonalność; nie da się wyrzucić presji na maszynach i systemach, nie da się wzbudzić w nich ciekawości czy zaproponować im nagrody, by skłonić je do niepożądanych działań. Phishing polega na rozesłaniu maili, często zawierających dokument, który po otwarciu może spowodować przejęcie lub uszkodzenie systemu urządzenia. Często przybiera to formę SMS-ów, maili, wiadomości w mediach społecznościowych

10 B. Hołtys, *Bezpieczeństwo – ogólne problemy badawcze*, Warszawa 2014, s. 300.

11 Mafia PL, *E-MAFIA | Jak działają w Polsce grupy cyberprzestępcze*, <https://www.youtube.com/watch?v=SMu7EPmK9F4&list=LL&index=93> (1.10.2022).

12 M. Nosowski, *Prawne aspekty cyberbezpieczeństwa. Praktyczne wskazówki dla przedsiębiorców*, Warszawa 2019, s. 97.

13 K. Majdan, *Hakerzy wywołali chaos na Ukrainie. Jak doszło do ataku ransomware?*, <https://businessinsider.com.pl/technologie/nowe-technologie/notpetya-atak-zlosliwym-oprogramowaniem-na-ukraine/s7bnll2> (28.06.2017).

14 M. Nosowski, *Prawne aspekty...*, s. 98.

czy spear phishingu, czyli spersonalizowanego, bardziej osobistego charakteru. Walka z tego typu atakami jest bardzo utrudniona w dużej mierze ze względu na jej transgraniczność. Tego typu wyłudzenia często dokonywane są spoza granic naszego kraju, najczęściej ze Wschodu, Afryki i Azji¹⁵.

W związku z chęcią usprawnienia komunikacji i ułatwienia czynności formalnych, rejestracyjnych i procesowych działania administracji publicznej zmierzają do załatwiania spraw obywatelskich online. Z pewnością wiele celów z tym związanych zostaje uzyskanych, a e-partycypacja społeczna i obywatelska jest bardzo pożądaną formą funkcjonowania we wspólnocie publicznej¹⁶. Trzeba sobie jednak zdawać sprawę z tego, że wspomniane niebezpieczne trendy mogą nieść negatywne skutki dla udziału obywateli w życiu społecznym, politycznym i publicznym.

W pierwszej kolejności aktywności takie jak phishing mogą powodować utratę zaufania do platform online, w tym portali rządowych, mediów społecznościowych czy stron internetowych organizacji społecznych, w szczególności gdy dochodzi do podszywania się pod takie instytucje. W związku z utratą zaufania obywatele mogą nie chcieć udostępniać swoich danych lub uczestniczyć w dyskusjach online, w obawie przed oszustwem. Tracąc kontrolę nad swoimi danymi, mogą rezygnować z rejestracji online na platformach e-partycypacji. Ponadto, jeśli atak zostanie pozytywnie przeprowadzony, utrata danych osobowych i wrażliwych uniemożliwia korzystanie z konkretnych platform, co skutecznie blokuje szansę na udział w wielu procedurach politycznych czy administracyjnych, np. głosowaniu czy załatwianiu spraw urzędowych przez Internet¹⁷.

Podane przez nas przykłady dotyczą obywateli mniej lub bardziej bezpośrednio. Jednak to, co je łączy, to transgraniczność. Cyberataki nie zawsze, choć bardzo często, są podejmowane z innych miejsc na świecie niż państwo, którego sieć, urządzenie czy oprogramowanie jest celem ataku. Należy zauważyć, że cyberprzestrzeń to nie tylko obywatele, ale także cały system państwowy i rządowy¹⁸. Naturalne jest więc, że skoro państwo samo stwarza warunki obywatelom do partycypacji w sieci, to tak samo stwarza je sobie w celu funkcjonowania na zewnątrz, w przestrzeni międzynarodowej – w ten sposób państwa przenoszą miejsce współpracy i rywalizacji do sieci. Konflikty pojawiają się w zupełnie nowej rzeczywistości, alternatywnej, często równie niebezpiecznej, jak realny świat.

15 Mafia PL, *E-MAFIA | Jak działają...*

16 N. Lubik-Reczek, I. Kapsa, M. Musiał-Karg, *Elektroniczna partycypacja obywatelska w Polsce. Deklaracje i opinie Polaków na temat e-administracji i e-głosowania*, Poznań 2020, s. 10.

17 M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, s. 216.

18 T. Terlikowski, *Bezpieczeństwo cyberprzestrzeni wyzwaniem naszych czasów. System cyberbezpieczeństwa w Polsce (w świetle obowiązującego prawa)*, „Zeszyty Naukowe SGSP” 2019, nr 3, s. 84.

Cyberwojna, pomimo że nie jest działaniem wojennym powszechnie kojarzającym się z fizycznymi, militarnymi ruchami wojsk, z pewnością jest już stałym elementem w pierwszej fazie konfliktu oraz w jego trakcie. Internet stanowi główne źródło wywiadowcze, co pozwala na szybsze podejmowanie decyzji odnośnie do taktyk i strategii walki¹⁹. Aktualny wyścig zbrojny może przypominać wojnę informacyjną, w której w kluczowej fazie zbrojeń odchodzi się od tradycyjnego ulepszania i powiększania wyposażenia militarnego. Ważniejsze okazują się teraz dane, które można wykorzystać w nowej technologii dla przeprowadzenia ataków cybernetycznych. W kontekście współzycia społecznego i partycypacji dla obywateli ważna jest każda faza konfliktu²⁰. Cyberwojna ułatwia bowiem szerzenie dezinformacji, wpływanie na morale i manipulację ludnością. Niejednokrotnie to nastawienie obywateli do wojny wpływa na jej wynik. W erze cyfrowej kształtowanie postrzegania konfliktu przez obywateli, jest o wiele łatwiejsze niż 100 lat temu²¹.

W raporcie pt. *Botnets, Cybercrime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress* określono cyberwojnę jako „Bezprawny atak na komputery, sieci oraz informacje w nich zawarte, ukierunkowane na zastraszenie, lub zmuszenie rządu oraz społeczeństwa w celu osiągnięcia korzyści politycznych oraz społecznych”²². Za przykład mogą posłużyć ataki na Estonię (2007) i Gruzję (2008), gdzie podjęte działania prowadziły do destabilizacji rządu podczas konfliktów. Stuxnet (2010) sabotował irańskie instalacje nuklearne, a NotPetya (2017) uderzył w Ukrainę, paraliżując globalną infrastrukturę. W 2016 r. za pomocą cyberataków ingerowano w wybory prezydenckie w USA, podważając tym samym zaufanie do procesu demokratycznego.

Cyberdemokracja, tak znacząca w e-partycypacji, ma to do siebie, że jej celem jest umożliwienie obywatelom podejmowania swoich obywatelskich obowiązków i inicjatyw za pośrednictwem sieci. Jednak cyberdemokracja może stanowić jeden z głównych celów ataku, ponieważ wpływ na nią może prowadzić do nieodpowiedniego funkcjonowania państwa, tym bardziej, że zniszczenie demokratycznego funkcjonowania państwa jest możliwe na wiele sposobów, np. poprzez szerzenie dezinformacji, uniemożliwienie obywatelom wzięcia udziału w głosowaniu czy fałszowanie poprzez sieć wyników wyborów²³.

Przytaczając poszczególne przykłady, można zauważyć, że Internet jest dla cywilizacji ogromną szansą, ale jak każda wielka zmiana szybki rozwój

19 *Cyberbezpieczeństwo wyzwaniem...*, s. 40.

20 Narodowy Instytut Cyberbezpieczeństwa, *Cyberwojna – 15 minut z cyberbezpieczeństwem*, <https://www.youtube.com/watch?v=PhNK7wmmqLM&list=LL&index=92&t=752s> (15.11.2022).

21 *Ibidem*.

22 C. Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Updated January 29, 2008.

23 P. Jankowski, *Cyberterroryzm jako współczesne zagrożenie dla administracji publicznej*, „Młody Jurysta” 2018, nr 4, s. 15.

cyberświata i sztucznej inteligencji niesie ze sobą wiele nowych zagrożeń, które należy regularnie badać i na których nadejście należy być przygotowanym. Przestępstwa i ataki w cyberprzestrzeni świadczą o możliwości korzystania w sposób negatywny z sieci i bezpośredniego wpływania i narażania społeczeństwa na niebezpieczeństwo ze strony grup hakerów, a także samych państw. Sytuacja ta wymaga znalezienia sposobu skutecznego chronienia się i środków prawnych, które należy wdrożyć²⁴, aby przeciwdziałać tym i wielu innym problemom związanym z cyberbezpieczeństwem²⁵.

4. Odpowiedź na zagrożenia – cyberbezpieczeństwo

Sektor publiczny powinien być gwarantem bezpieczeństwa przepływu informacji i wprowadzania niezbędnych mechanizmów zapewniających prawidłowe funkcjonowanie i przepływ danych w cyberprzestrzeni. Jest on odpowiedzialny za świadczenie wielu kluczowych usług publicznych, takich jak opieka zdrowotna, edukacja, transport czy administracja. W skład sektora publicznego wchodzi przede wszystkim podmioty zobowiązane, które wymienia ustawa, podkreślając tym samym ich znaczenie dla prawidłowego współżycia społeczeństwa obywatelskiego. Są to wszystkie podmioty, od których na podstawie ustawy o krajowym systemie cyberbezpieczeństwa wymaga się przestrzegania określonych przepisów z niej wynikających. Są to m.in. samorządy terytorialne, jednostki budżetowe, związki metropolitarne, uczelnie, NFZ²⁶. Można więc zauważyć, że te podmioty niejednokrotnie bezpośrednio przenikają do życia obywateli i stanowią jego integralną część. Bezpieczeństwo usług sektora publicznego jest istotne dla stabilności społecznej i gospodarczej, dlatego to on ma duże znaczenie w zapewnieniu bezpieczeństwa przepływu informacji. Od administracji rządowej i samorządowej wymaga się, by były w pełni bezpieczne i odpowiednio przygotowane na zagrożenia opisane wcześniej, dlatego też często samo działanie sektora publicznego (choć jest jednym z kluczowych działaczy w tym zakresie) nie wystarcza i potrzeba zaangażowania sektora prywatnego, społeczeństwa obywatelskiego i międzynarodowej współpracy w celu skutecznego zwalczania zagrożeń cybernetycznych. Należy przyjrzeć się i zrozumieć, jak ma przebiegać ta współpraca, gdyż dopiero wtedy możliwe będzie zapewnienie integralności tych sektorów w obszarach bezpieczeństwa sieciowego²⁷.

Aby zapewnić poufność danych przetwarzanych w systemach informatycznych, należy podjąć wiele niezbędnych czynności, w tym: określić organizacyjne i techniczne wymogi bezpieczeństwa przetwarzania, nadać

24 *Cyberbezpieczeństwo wyzwaniem...*, s. 43.

25 B. Hołtyś, *Bezpieczeństwo...*, s. 280.

26 M. Nosowski, *Prawne aspekty...*, s. 49.

27 *Ibidem*, s. 9.

określony stopień tajności informacji, zarządzać przetwarzaniem, szkolić kadry, inwestować w struktury systemów informatycznych, przygotowywać dokumentację i tworzyć kopie zapasowe. Te wszystkie czynności wchodziły w skład polityki bezpieczeństwa informacji (PBI)²⁸. Polityka bezpieczeństwa informacji to zestaw zasad, procedur, wytycznych i praktyk, które mają na celu zapewnienie ochrony informacji, danych i zasobów informacyjnych w organizacji. Chroni ona systemy informatyczne przed atakami cybernetycznymi, zapewnia integralność, poufność i dostępność danych. Polityka ta określa również procedury zapobiegania incyidentom oraz reakcji na nie w razie potrzeby²⁹.

Pojęcie incydentów występuje także w ustawie o krajowym systemie cyberbezpieczeństwa³⁰. Pojawienie się incydentu warunkuje konieczność podjęcia określonych zachowań ze strony danych podmiotów. Znajomość i odróżnienie od siebie konkretnych rodzajów podmiotów jest konieczne dla prawidłowego rozpoznania, jakie czynności należy wykonać. Wyżej wymieniona ustawa określa pięć rodzajów incydentów:

- a) incydent – sytuacja, która wywołuje lub może wywołać negatywny skutek; samo jej wystąpienie nie warunkuje podjęcia określonych działań;
- b) zdarzenie krytyczne – zdarzenie, które ma istotny wpływ na bezpieczeństwo cybernetyczne i obejmuje incydenty, które mają duży wpływ na działanie krytycznych usług i systemów, czyli ataki na systemy kontroli przemysłowej, prawa i wolności obywatelskie, infrastrukturę energetyczną czy systemy łączności;
- c) incydent poważny – powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej; operatorzy usług kluczowych są odpowiedzialni za działalność społeczną i gospodarczą w znaczeniu kluczowym dla utrzymania ich krytycznego funkcjonowania; są to np. przedsiębiorstwa energetyczne, podmioty prowadzące działalność transportową czy ochrony zdrowia;
- d) incydent istotny – incydent, który ma istotny wpływ na świadczenie usługi cyfrowej, np. spowodował utratę zdolności do prawidłowego przetwarzania danych bądź ich poufności;
- e) incydent w podmiocie publicznym – działanie negatywnie wpływające na realizowanie zadań publicznych³¹.

Znajomość rodzaju incydentu służy do rozpoznawania zagrożenia, z jakim mamy do czynienia, jednak aby do niego nie dopuścić, musimy ustalić stopień ryzyka, czyli rozeznaczyć, jaka jest szansa na jego wystąpienie. Zrozumienie

28 A. Rogacka, *Ochrona informacji w jednostkach samorządu terytorialnego poprzez stosowanie polityki bezpieczeństwa informacji*, w: *Bezpieczeństwo informacji w administracji publicznej*, D. Fleszer (red.), Sosnowiec 2017, s. 101.

29 *Ibidem*, s. 99.

30 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018, poz. 1560.

31 M. Nosowski, *Prawne aspekty ...*, s. 34.

i zarządzanie ryzykiem w cyberbezpieczeństwie jest kluczowe dla zapewnienia skutecznej ochrony przed incydentami oraz minimalizacji skutków tych incydentów w przypadku ich wystąpienia³². Ustawa nie określa dokładnie, w jaki sposób ma się dokonać jego ocena, podmioty wdrażające zabezpieczenia mają zatem pewną dowolność w tej sferze³³.

Rozporządzenie o ochronie danych osobowych (RODO) w art. 32 („Bezpieczeństwo przetwarzania”) nakłada minimalne wymagania, jakie muszą zostać uwzględnione w procesie oceny ryzyka. Są to m.in. „stan wiedzy technicznej i koszty ich wdrożenia, a także charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych”³⁴. Administrator musi też pamiętać o zasadzie rozliczalności, a więc musi wykazać, że zostały wdrożone środki zgodne z przepisami RODO. Wraz z rozwojem nowych technologii zmieniają się również trendy wśród cyberprzestępstw i innych zagrożeń, dlatego ważne jest regularne analizowanie i uaktualnianie strategii odpowiednich dla nowych wyzwań.

Dla oceny dobrze jest uwzględnić kluczowe elementy, które warto brać pod uwagę. Są to np.

- a) analiza i identyfikacja zagrożeń,
- b) ocena potencjalnych skutków, jakie mogą nieść te zagrożenia,
- c) identyfikacja aktywów informacyjnych i infrastruktury IT,
- d) uwzględnienie formy i rodzaju działalności podmiotu, przetwarzającego dane i informacje,
- e) procesy transferowania danych,
- f) ustalenie akceptowalnego poziomu ryzyka³⁵.

Jeśli pomimo zaopatrzenia przedsiębiorstw i innych podmiotów wykorzystujących systemy IT w środki służące zwiększeniu cyberbezpieczeństwa zagrożenie nadal występuje i może naruszać prawa i wolności obywateli, zaleca się, by w takich sytuacjach skorzystać z konsultacji z organem nadzorczym.

Warto w tym miejscu wspomnieć o dwóch zasadach mogących zwiększyć bezpieczeństwo osób korzystających z metod e-partycypacji w życiu obywatelskim. Są nimi *privacy by default* oraz *privacy by design*. Pierwsza zakłada ochronę prywatności jako domyślne ustawienie każdego programu (systemu), a zmiana takiego ustawienia powinna następować jedynie na wyraźne żądanie użytkownika programu. Przewiduje możliwe najszerzą, domyślną ochronę prywatności użytkowników danego systemu dla osiągnięcia każdego konkretnego celu przetwarzania. Z kolei *privacy by design* to zasada wbudowanej ochrony prywatności w każdy projekt zakładający przetwarzanie

32 *Ibidem*, s. 52.

33 *Ibidem*.

34 Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (RODO).

35 M. Nosowski, *Prawne aspekty...*, s. 62.

danych osobowych, tak aby od początku jego istnienia ochrona prywatności stanowiła jego część składową³⁶.

Zabezpieczenie danych zgodnie z RODO wymaga zastosowania odpowiednich środków technicznych i organizacyjnych, takich jak:

- a) szyfrowanie danych dla zapewnienia ich poufności, integralności i pouczalności podczas przesyłania i przechowywania,
- b) pseudonimizacja w celu minimalizacji ryzyka identyfikacji,
- c) monitorowanie systemów informatycznych w celu wykrywania nieprawidłowości,
- d) ustalenie procedur reagowania na incydenty,
- e) tworzenie kopii zapasowych i sprawozdań,
- f) zarządzanie w postaci sprawowania kontroli dostępu oraz monitorowania aktywności³⁷.

Wyżej przytoczone przykłady stanowią jedynie wycinek tego, w jaki sposób podmioty działające w cyberprzestrzeni powinny gwarantować bezpieczeństwo użytkowników. Sektor publiczny jest tym, który wprowadza pewne mechanizmy w celu ułatwiania procesów życia społecznego, jednak samodzielnie nie jest on zdolny do zagwarantowania pełnej nienaruszalności informacji. Można zminimalizować, lecz nie wykluczyć, zagrożenia związane z nowymi technologiami. Warto także zwrócić uwagę na działania służące uświadamianiu społeczeństwa i współpracy międzynarodowej.

Osoby korzystające z Internetu w jakimś wymiarze są narażone na socjotechniki stosowane przez hakerów. Najpopularniejszą z nich jest już wspomniany wyżej phishing, prosty do zrealizowania i dlatego tak powszechny. Warto organizować szkolenia mające na celu uświadamianie obywateli o istnieniu zagrożeń i możliwościach zabezpieczenia się przed nimi, a także zaopatrzyć się w antywirusy i na bieżąco aktualizować systemy operacyjne i przeglądarki³⁸.

Istnieje także ustawa o Krajowych Ramach Interoperacyjności, które mają na celu zapewnienie odpowiedniej współpracy między jednostkami publicznymi a obywatelami³⁹. Ustawa zawiera informacje przytoczone przez nas już wcześniej, w tym dotyczące zarządzania ryzykiem i rozpoznawania incydentów. Wskazuje także na konieczność prowadzenia systemu zarządzania bezpieczeństwem informacji. Warto, aby działania władz skupiały się na rozpowszechnianiu informacji i wiedzy na temat stosowania ustawy w codziennym życiu, nie tylko w przedsiębiorstwach i jednostkach samorządowych.

36 *Na czym polegają zasady privacy by default i privacy by design?*, <https://odo24.pl/wiedza/abc-rodod/odpowiedz-na-pytanie.na-czym-polegaja-zasady-privacy-by-default-i-privacy-by-design> (1.09.2024).

37 M. Nosowski, *Prawne aspekty...*, s. 69.

38 Narodowy Instytut Cyberbezpieczeństwa, *Cyberwojna...*

39 Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2012, poz. 526.

To, co zwykła jednostka może samodzielnie wdrożyć w ramach cyberbezpieczeństwa, to uwierzytelnianie. Jest to proces polegający na weryfikacji danej osoby poprzez przekazanie jej konkretnych uprawnień. Uwierzytelnianie zapewnia poufność, rozliczalność, dostępność oraz niezaprzeczalność co do uzyskania dostępu, np. do urządzenia lub oprogramowania, dzięki czemu niepowołana do tego osoba tego dostępu nie uzyska. Posłużyć do tego mogą hasła, tokeny, a także indywidualne cechy fizyczne, takie jak np. linie papilarne czy rysy twarzy. Wskazane, by wymienione wyżej metody były stosowane jednocześnie, co zapewni zwiększenie poziomu zabezpieczeń⁴⁰.

Dla zapewnienia należytego bezpieczeństwa, państwa często nie mogą być zdane same na siebie. Współpraca międzynarodowa odgrywa bardzo ważną rolę w zakresie bezpieczeństwa cybernetycznego. Chęć wzmocnienia wzajemnych działań zmierzających do pomocy stała się szczególnie ważna w okresie pandemii, kiedy życie przeniosło się w dużej mierze do świata wirtualnego. Wtedy podjęto wiele decyzji zmierzających do wzmocnienia współpracy bilateralnej z zagranicznymi partnerami⁴¹.

Państwa mogą korzystać m.in. z umów dwu- lub wielostronnych, szkoleń czy wspólnych projektów badawczych. Przykładem współpracy dwustronnej jest podpisanie przez Dyrektora Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC) z Łotwą oraz Estonią porozumienia w zakresie współpracy zespołów reagowania na incydenty bezpieczeństwa komputerowego. W 2021 r. NCBC prowadziło ze Stanami Zjednoczonymi bliską współpracę, która m.in. polegała na braniu udziału w ćwiczeniach, spotkaniach ekspertów i rozmowach o tematyce cyberbezpieczeństwa.

Polska również ma swój udział w ćwiczeniach zwiększających kompetencje w tej tematyce. Jednym z ćwiczeń jest Cyber Flag – symulowane są sytuacje związane z atakami i obroną w cyberprzestrzeni. Zadaniem zespołów biorących w nim udział jest atakowanie lub obrona przed atakiem zespołu przeciwnika. Dla Polski ważna jest również współpraca podejmowana w ramach sojuszu północnoatlantyckiego, np. zorganizowano takie ćwiczenia, jak Cyber Coalition 2021, Crossed Swords 2021 i Coalition Warrior Interoperability Exercise⁴².

Komputer może być narzędziem pracy, ale użyty w niewłaściwym celu może powodować poważne szkody, dlatego ważne jest, aby w dobie cyfryzacji i wdrażania możliwości obywatelskiej partycypacji w Internecie osoby z niej korzystające były w pełni bezpieczne. Zabezpieczenia, rozpoznawanie incydentów i odpowiednie zarządzanie ryzykiem powinny być wpisane w główne zadania podmiotów sektora publicznego. Państwo jest odpowiedzialne za bezpieczeństwo jednostki, dlatego polityka informacyjna stanowi ważny element ochrony. Należy dbać o udostępnianie nowych wiadomości na temat zagrożeń

40 M. Nosowski, *Prawne aspekty...*, s. 90.

41 Wojsko Polskie, *Współpraca międzynarodowa*, <https://www.wojsko-polskie.pl/woc/wspolpraca-miendzynarodowa/> (10.07.2024).

42 *Ibidem*.

cybernetycznych i tego, jak się przed nimi chronić. Współpraca międzynarodowa w ostatnich latach działa w obszarze bezpiecznej sieci, lecz nadal brakuje norm i sankcji stanowczo regulujących reakcje na ataki przestępców działających w sieci. Ważne jest jednak, aby nowe technologie nie zagrażały korzystającemu z nich społeczeństwu obywatelskiemu, ale stanowiły pomoc w codziennym życiu i ciągle rozwijającej się partycypacji⁴³.

Niektóre mechanizmy e-partycypacji są z powodzeniem wykorzystywane już teraz. Przykładem są projekty finansowane z budżetu obywatelskiego w formie crowdsourcingu. W dużej mierze e-partycypacja jest postrzegana jako możliwość, która nadal się rozwija i może się wiązać ze znacznymi korzyściami dla rządu i obywateli. Warto jednak zaznaczyć, że wraz z jej rozwojem postęp dotyka także nowych technologii, które dzięki ulepszaniu mogą narażać obywateli na utratę prywatności i nagły wyciek danych. Dlatego tak istotne jest utrzymanie kontroli rządu nad zmianami zachodzącymi poprzez ciągły postęp technologiczny i wdrożenie środków pomocniczych i ochronnych wraz z nowymi platformami e-partycypacyjnym.

5. Wnioski

Technologia stała się nieodzownym elementem życia społecznego, a wraz z jej rozwojem wzrosła liczba postulatów dotyczących jej zastosowania w procesach demokratycznych, takich jak wybory. Niemniej jednak hipoteza postawiona w niniejszym artykule, mówiąca o tym, że społeczeństwo i państwo nie są gotowe na tak szybkie przemiany technologiczne w obszarze e-partycypacji ze względu na brak odpowiednich narzędzi zapewniających bezpieczeństwo, znajduje potwierdzenie w analizie obecnych uwarunkowań.

Chociaż niektóre państwa podejmują próby wdrażania mechanizmów e-partycypacji na szczeblu lokalnym, ich doświadczenia są niejednoznaczne. Wprowadzenie demokracji internetowej budzi istotne obawy dotyczące możliwości zachowania demokratyczności procesów wyborczych, które stanowią fundament współczesnego państwa prawa. Szczególnie istotnym problemem pozostaje brak pełnej skuteczności narzędzi zabezpieczających przed cyberatakami, jak phishing czy ransomware, a także zaawansowane ataki, jak te przeprowadzone przy użyciu Petyi w 2017 r.

Chociaż państwa podejmują liczne działania w celu ochrony swoich systemów informacyjnych, takich jak czynności związane z wykrywaniem incydentu i odpowiednie jego sklasyfikowanie, zarządzanie ryzykiem, wprowadzanie procesów transferowania danych, ustalanie akceptowalnego poziomu ryzyka, a także implementacja aktów prawnych nakładających wymogi odpowiedniego ograniczania i radzenia sobie z nowymi trendami wśród przestępstw hakerskich, to współczesne cyberzagrożenia często przerastają

43 K. Liderman, *Bezpieczeństwo informacyjne – nowe wyzwania*, Warszawa 2017, s. 10.

ich możliwości. Przykłady ataków na instytucje publiczne oraz dane rządowe pokazują, że mimo rozwijającej się współpracy międzynarodowej i zaawansowanych mechanizmów obronnych w pełni skuteczna ochrona procesów wyborczych w świecie cyfrowym jest nadal nieosiągalna.

Obecny stan technologii oraz cyberprzestępczości, w szczególności wzrost ataków hakerskich, sugeruje, że przeniesienie kluczowych procesów demokratycznych do świata cyfrowego mogłoby nieść ze sobą więcej strat niż korzyści. Chociaż sektor publiczny wdraża działania mające na celu ograniczenie cyberzagrożeń, to niepełna ochrona przed atakami oraz złożoność cyberprzestrzeni wskazują na brak gotowości państw do pełnej integracji e-partycypacji w procesach demokratycznych.

Bibliografia

- Balicki R., *E-voting przyszłość demokracji?*, „CBKE e-BIULETYN” 2007, nr 3.
- Barczak S., *Crowdsourcing. Co to znaczy? Przykłady w Polsce i za granicą*, <https://interviewme.pl/blog/crowdsourcing> (4.09.2024).
- Cieślak J., *E-voting. Możliwości zastosowania głosowania elektronicznego w Polsce*, Biblioteka Cyfrowa, <https://www.bibliotekacyfrowa.pl/Content/34346/PDF/E-voting.pdf> (4.09.2024).
- Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y*, gov.pl, Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y> (13.08.2024).
- Górka M., *Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa*, w: *Cyberbezpieczeństwo wyzwaniem XXI wieku*, T. Dębowski (red.), Łódź–Wrocław 2018.
- Harechko I., *Basic Mechanisms of E-participation of Citizens in Policy-Making*, „Toruńskie Studia Międzynarodowe” 2011, nr 1 (4).
- Holtys B., *Bezpieczeństwo – ogólne problemy badawcze*, Warszawa 2014.
- Jankowski P., *Cyberterrorizm jako współczesne zagrożenie dla administracji publicznej*, „Młody Jurysta” 2018, nr 4.
- Kozłowski A., *Petya/NotPetya – analiza tajemniczego malware’u który zaatakował Ukrainę*, SCS 2017, <https://cyberdefence24.pl/petyanotpetya-analiza-tajemniczego-malwareu-ktory-zaatakowal-ukraine-scs-2017> (4.09.2024).
- Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015.
- Liderman K., *Bezpieczeństwo informacyjne – nowe wyzwania*, Warszawa 2017.
- Lubik-Reczek N., Kapsa I., Musiał-Karg M., *Elektroniczna partycypacja obywatelska w Polsce. Deklaracje i opinie Polaków na temat e-administracji i e-głosowania*, Poznań 2020.
- Mafia PL, *E-MAFIA | Jak działają w Polsce grupy cyberprzestępcze*, <https://www.youtube.com/watch?v=SMu7EPmK9F4&list=LL&index=93> (20.10.2024).
- Majdan K., *Hakerzy wywołali chaos na Ukrainie. Jak doszło do ataku ransomware’?*, <https://businessinsider.com.pl/technologie/nowe-technologie/notpetya-atak-zlosliwym-oprogramowaniem-na-ukraine/s7bnll2> (2.09.2024).

- Na czym polegają zasady *privacy by default* i *privacy by design*?, <https://odo24.pl/wiedza/abc-rodo/odpowiedz-na-pytanie.na-czym-polegaja-zasady-privacy-by-default-i-privacy-by-design> (1.09.2024).
- Narodowy Instytut Cyberbezpieczeństwa, *Cyberwojna – 15 minut z cyberbezpieczeństwem*, <https://www.youtube.com/watch?v=PhNK7wmmqlM&list=LL&index=92&t=752s> (4.09.2024).
- Nosowski M., *Prawne aspekty cyberbezpieczeństwa. Praktyczne wskazówki dla przedsiębiorców*, Warszawa 2019.
- Rogacka A., *Ochrona informacji w jednostkach samorządu terytorialnego poprzez stosowanie polityki bezpieczeństwa informacji*, w: *Bezpieczeństwo informacji w administracji publicznej*, D. Fleszer (red.), Sosnowiec 2017.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2012, poz. 526.
- Stokłuska E., *E-partycypacja – o co właściwie chodzi i jak to może wyglądać*, <https://publicystyka.ngo.pl/e-partycypacja-o-co-wlasciwie-chodzi-i-jak-to-moze-wygladac> (4.09.2024).
- Terlikowski T., *Bezpieczeństwo cyberprzestrzeni wyzwaniem naszych czasów. System cyberbezpieczeństwa w Polsce (w świetle obowiązującego prawa)*, „Zeszyty Naukowe SGSP” 2019, nr 3.
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018, poz. 1560.
- Wilson C., *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Updated January 29, 2008.
- Wojsko Polskie, *Współpraca międzynarodowa*, <https://www.wojsko-polskie.pl/woc/wspolpraca-miendzynarodowa/> (11.05.2024).

Cyberbezpieczeństwo w perspektywie rozwoju e-partycypacji i w obliczu zagrożeń ery cyfrowej

Streszczenie

Era cyfrowa niesie ze sobą dynamiczny rozwój technologii informatycznych, które zaczęły opanowywać każdą gałąź naszego życia, zmieniając sposób, w jaki społeczeństwo komunikuje się i uczestniczy w życiu społecznym. Wymusiła zmiany w administracji publicznej i dostosowała ją do potrzeb obywateli. Elektroniczna partycypacja stanowi przedmiot zainteresowania badaczy, organizacji międzynarodowych oraz instytucji władzy państwowej i lokalnej. Rozwój różnorodnych form e-partycypacji otwiera przed nami wiele możliwości, jednak stawia również liczne wyzwania. W analizie zawartej w niniejszym artykule skupiamy się na identyfikacji kluczowych zagrożeń, takich jak dezinformacja, cyberprzemoc czy zagrożenia związane z ochroną prywatności. Przenikanie się życia w Internecie i w świecie realnym jest przyczyną coraz większych przemian gospodarczych, społecznych i kulturowych, w szczególności dotyczących ochrony danych osobowych, integralności systemów informatycznych oraz przeciwdziałania atakom cybernetycznym.

Rozwój nowych technologii prowadzi do automatyzowania procesów administracyjnych w społeczeństwie. Wraz z rozwojem pojawiają się nowe potrzeby w zakresie komunikacji i funkcjonowania społeczeństwa w procesach obywatelskich. Pomimo widocznych zalet tego zjawiska powstaje także niebezpieczeństwo w postaci cyberprzestępstw tym samym rozwój nowych technologii wymaga udzielenia odpowiedzi na pytania związane z faktycznym stopniem ochrony, a także z gotowością na pełne wdrożenie informatycznych rozwiązań w zakresie partycypacji obywatelskiej w erze cyfrowej. Poprzez analizę tych aspektów chcemy dostarczyć kompleksowego spojrzenia na świat e-partycypacji, zwracając uwagę na trudności i na potencjalne korzyści, jakie niesie ze sobą ta nowa forma interakcji społecznej. Warto się zastanowić, czy wprowadzone do tej pory systemy działań są wystarczająco optymalne dla zapewnienia bezpieczeństwa i swobodnego wykorzystywania możliwości technologicznych w życiu obywatelskim, jakie mechanizmy regulacyjne oraz społeczne powinny być wprowadzone, aby maksymalnie wykorzystać potencjał e-partycypacji przy jednoczesnym minimalizowaniu jej negatywnych skutków.

Słowa kluczowe: e-partycypacja, cyberbezpieczeństwo, społeczność obywatelska, era cyfrowa, nowe technologie

Cybersecurity in the Context of E-Participation Development and the Threats of the Digital Era

Abstract

The modern digital era has brought about the dynamic development of information technologies that have begun to permeate every aspect of our lives, transforming the way society communicates and engages in public life. This shift has necessitated changes in public administration, requiring adaptation to meet the evolving needs of citizens. Electronic participation has become a subject of growing interest among researchers, international organizations, and state and local government institutions. The development of various forms of e-participation offers many opportunities but also presents significant challenges. This analysis focuses on identifying key threats such as disinformation, cyberbullying, and privacy protection issues. The intersection of online life with the real world is driving substantial economic, social, and cultural transformations, particularly in the areas of personal data protection, IT system integrity, and the prevention of cyberattacks. The advancement of new technologies is accelerating the automation of administrative processes within society. At the same time, new communication needs and expectations surrounding civic engagement are emerging. Despite the clear advantages of this phenomenon, the growing risk of cybercrime raises concerns and necessitates an examination of the actual level of protection and preparedness for the full implementation of IT solutions in civic participation. By analyzing these issues, the article aims to provide a comprehensive overview of the world of e-participation, highlighting both the difficulties and the potential benefits of this evolving form of social interaction. It is worth considering whether the systems implemented thus far are sufficiently optimized to ensure security and allow for the free use of technological tools in civic life, as well as what regulatory and social mechanisms should be introduced to maximize the potential of e-participation while minimizing its negative consequences.

Keywords: e-participation, cybersecurity, civic community, digital era, new technologies