VOL. 77 STUDIA POLITOLOGICZNE
DOI: 10.33896/SPolit.2025.77.14

*Michał Szczegielniak**

Wybrane wyzwania związane z bezpieczeństwem e-wyborów

Selected Challenges Related to E-voting Security

Słowa kluczowe: *bezpieczeństwo głosowania elektronicznego, bezpieczeństwo wyborów, dezinformacja, e-demokracja, głosowanie przez Internet*

Key words: *electronic voting security, elections security, disinformation, e-democracy, voting over internet*

Abstrakt: *W artykule zaprezentowano wybrane wyzwania związane z wykorzystaniem nowoczesnych technologii w procesie wyborczym. Autor omawia ryzyka związane z głosowaniem przez Internet (i-voting), takie jak ryzyko kradzieży danych czy też braku transparentności. Następnie charakteryzuje zagrożenia wynikające ze stosowania elektronicznych urządzeń do głosowania – np. podatności na ataki hakerskie czy też brak możliwości kontroli liczenia głosów. Dodatkowo w tekście poruszono zagrożenia wynikające z dezinformacji.*

Abstract: *The article analyzes threats related to the use of modern technologies in elections. The author discusses threats to internet voting (i-voting), such as data theft and lack of transparency. He also addresses challenges with electronic voting such as the possibility of hacking machines and the lack of public oversight. Additionally, the article underscores the danger of disinformation.*

* ORCID ID: https://orcid.org/0000-0003-2001-8622; dr, Wydział Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. E-mail: m.szczegielniak@uw.edu.pl.

Wprowadzenie

Rewolucja informacyjna sprawiła, że nowe technologie przeniknęły do wielu sfer życia społecznego, wpływając także na procesy polityczne i relacje między instytucjami państwa a obywatelami. Maria Marczewska-Rytko uważa, że „wykorzystanie Internetu jest postrzegane jako sposób dostosowania demokracji do potrzeb współczesnych państw, wzmocnienia społeczeństwa demokratycznego zagrożonego wszechwładzą menedżerów oraz przeciwstawienia się reżimom autorytarnym"[1]. Z kolei Dorota Grodzka zaznacza, że „początkowo koncentrowano się na dostarczaniu informacji za pomocą Internetu"[2], następnie zaczęto wykorzystywać systemy teleinformatyczne do konsultacji i sondaży, by w końcu użyć ich do zwiększenia partycypacji obywatelskiej np. dzięki wprowadzeniu elektronicznych inicjatyw ustawodawczych[3]. Prognozuje się, że znaczenie Internetu w procesach politycznych będzie wzrastać, w miarę jak kolejne pokolenia, które dorastały w erze powszechnego dostępu do sieci, będą uzyskiwać prawa wyborcze[4].

Pod pojęciem elektronicznej demokracji rozumie się zwykle wykorzystywanie technologii informacyjno-komunikacyjnych do wspierania procesów demokratycznych, w szczególności podejmowania decyzji[5]. Martin Hagen uznaje za e-demokrację „każdy demokratyczny system polityczny, w którym używa się komputerów i sieci komputerowych do realizacji podstawowych funkcji procesu demokratycznego takich, jak informowanie i komunikacja, artykulacja i agregacja interesów oraz proces decyzyjny (zarówno w sensie dyskusji, jak i w głosowaniu)"[6]. Sebastian Berg i Jeanette Hofmann wyróżnili dwa wymiary e-demokracji. W pierwszym, analitycznym, bada się wpływ technologii cyfrowych na poziom zaangażowania politycznego oraz sposób rządzenia. W drugim, normatywnym, e-demokracja postrzegana jest jako otwarta i zmienna forma organizacji politycznej *in statu nascendi*[7].

---

1 M. Marczewska-Rytko, *Idea demokracji bezpośredniej od okresu antycznego do czasów Internetu i globalizacji*, [w:] M. Marczewska-Rytko, A. K. Piasecki, *Demokracja bezpośrednia. Wymiar globalny i lokalny*, Lublin 2010, s. 25–26.

2 D. Grodzka, *E-demokracja*, «Infos» 16 lipca 2009, nr 14(61), s. 1.

3 Tamże, s. 2.

4 G. Browning, *Electronic Democracy. Using the internet to Transform American Politics*, Medford–New Jersey 2006, s. 176.

5 A. Macintosh, *Characterizing E-Participation in Policy-Making*, [w:] *Proceedings of the 37th Hawaii International Conference on System Sciences*, Big Island 2004, s. 2.

6 M. Hagen, *A Typology of Electronic Democracy*, http://www.uni-giessen.de/fb03/vinci/labore/netz/hag_en.htm (12.10.2017) cyt. za: M. Musiał-Karg, *E-demokracja, e-partycypacja i e-głosowanie, czyli o tym jak zwiększać zaangażowanie obywateli w dobie Internetu*, [w:] M. Rachwał (red.), *Uwarunkowania i mechanizmy partycypacji politycznej*, Poznań 2017, s. 89.

7 S. Berg, J. Hofmann, *Digital democracy*, «Internet Policy Review» 2021, nr 10(4), s. 2.

Głosowanie elektroniczne (*e-voting*) to jedno z narzędzi e-demokracji[8]. Pojęcie to jest niezwykle szerokie i obejmuje różne elektroniczne metody oddawania, przekazywania i liczenia głosów[9]. Wszystkie systemy elektronicznego głosowania łączy jednak to, że opierają się na zaawansowanej technologii, która jest niezbędna do ich prawidłowego działania[10]. Spośród wielu form e-votingu największą popularnością cieszą się głosowania w systemie zamkniętym za pomocą maszyn elektronicznych umieszczonych w lokalu wyborczym (*computer voting*) oraz głosowania w systemie otwartym za pośrednictwem Internetu i dedykowanego oprogramowania, które pozwala oddawać głosy z dowolnego miejsca na Ziemi (*remote i-voting*)[11].

Tomasz Gajowniczek zauważył, że „pierwsze próby wykorzystania «nowych technologii» w celu aktywizacji społeczeństwa miały miejsce w latach siedemdziesiątych XX wieku w USA. W (…) Columbus w miejscowej telewizji kablowej uruchomiono usługę Qube. Widzowie, za pomocą przycisków w pilocie (…), mogli nie tylko zmieniać kanały, ale także uczestniczyć w głosowaniach na żywo"[12]. Z kolei w Brazylii już w 1996 r. odbyły się wybory wspomagane elektronicznie, w których wykorzystano technologię „bezpośredniego zapisu elektronicznego (DRE) na komputerach, bez potwierdzenia w formie papierowej"[13]. W 2000 r. podczas wyborów odbywających się w Arizonie (USA) obywatele mieli możliwość oddawania głosów za pośrednictwem strony interneto-

[8] R. Krimmer, *E-voting as a New Form of Voting*, [w:] A. Balci, C. Can Actan, O. Dalbay (red.), *Explorations in eGovernment & eGovernance. Volume 2: Selected proceedings of the Second International Conference on eGovernment and eGovernance*, Antalya 2010, s. 148; M. Musiał-Karg, *E-voting (as a form of E-democracy) in the European Countries*, [w:] A. Balci, C. Can Actan, O. Dalbay (red.), *Explorations in eGovernment & eGovernance. Volume 2: Selected proceedings of the Second International Conference on eGovernment and eGovernance*, Antalya 2010, s. 156–157; M. Musiał-Karg, *E-demokracja…*, s. 93–94; N. Lubik-Reczek, I. Kapsa, M. Musiał-Karg, *Elektroniczna partycypacja w Polsce. Deklaracje i opinie Polaków na temat e-administracji i e-głosowania*, Poznań 2020, s. 47.

[9] Ü. Madise, P. Vinkel, E. Maaten, *Internet Voting at the Elections of Local Government Councils on October 2005*. Report, http://www.vvk.ee/public/dok/report2006.pdf (11.11.2024), s. 4; M. Nowina Konopka, *Elektroniczna urna*, https://bip.brpo.gov.pl/pliki/12066058070.pdf (11.11.2024), s. 2.

[10] J. P. Gibson, R. Krimmer, V. Teague, J. Pomares, *A review of E-voting: the past, present and future*, «Annals of Telecommunications» 2016, vol. 71, s. 279.

[11] M. Nowina Konopka, *Elektroniczna…*, s. 2–3; M. Musiał-Karg, *Electronic democracy and its organization – a revolution or a modernization? The example of e-voting*, «Politbook» 2012, nr 2, s. 134–135; N. Lubik-Reczek, I. Kapsa, M. Musiał-Karg, *Elektroniczna…*, s. 47–48.

[12] T. Gajowniczek, *Elektroniczna demokracja – istota pojęcia i problemy definicyjne*, [w:] W. Tomaszewski, D. M. Mościcka, A. Jurkun (red.), *Demokracja a wybory. Współczesne dylematy i wyzwania*, Olsztyn 2015, s. 14.

[13] M. Czajkowski, *E-voting na przykładzie Estonii i Brazylii*, «Studia BAS» 2011, nr 3(27), s. 131.

wej[14]. Współcześnie systemy elektronicznego głosowania są wykorzystywane m.in. w Brazylii[15], Estonii[16], Norwegii[17], Szwajcarii[18] oraz USA[19].

Celem artykułu jest przedstawienie podstawowych zagrożeń związanych z wykorzystaniem nowoczesnych technologii w procesie wyborczym. Hipotezą pracy jest twierdzenie, że ich szerokie zastosowanie uniemożliwia budowę wiarygodnego, spełniającego wysokie standardy bezpieczeństwa systemu wyborczego. Na potrzeby weryfikacji ww. hipotezy sformułowano następujące pytania badawcze:

- Czy elektroniczne systemy głosowania zwiększają bezpieczeństwo i poziom wiarygodność wyborów?
- Jakie ryzyka niesie za sobą wdrażanie elektronicznego głosowania?
- Jak problem dezinformacji wpływa na bezpieczeństwo i uczciwość wyborów?

Artykuł ma charakter teoretyczno-empiryczny. Zostały w nim przedstawione główne wyzwania dotyczące bezpieczeństwa elektronicznych wyborów oraz analiza wybranych przykładów, w których zaufanie do zastosowanych rozwiązań zostało podważone. W pracy wykorzystano podejście systemowe, które pozwala na holistyczne spojrzenie na system wyborczy, uwzględniając jego różne elementy i ich wzajemne zależności. Dzięki temu możliwe jest zidentyfikowanie potencjalnych punktów podatnych na ataki i manipulacje. Przywołane w tekście konkretne przykłady naruszenia bezpieczeństwa pokazują, że opisane zagrożenia są realne i mogą mieć poważne konsekwencje dla demokratycznych procesów wyborczych.

Głosowanie wspomagane elektronicznie

W przypadku głosowania wspomaganego elektronicznie decyzje wyborców trafiają do odpowiednich urządzeń, które rejestrują oddane głosy. Następ-

[14] K. Duda, *E-voting jako forma demokracji bezpośredniej. Dotychczasowe doświadczenia i konsekwencje*, «Refleksje», jesień–zima 2011, nr 4, s. 163.

[15] Por. M. Czajkowski, *E-voting*…

[16] Por. M. Musiał-Karg, *Internetowe głosowanie w Estonii na przykładzie wyborów w latach 2005–2009*, «Przegląd Politologiczny» 2011, nr 3.

[17] Por. F. Zagórski, *Głosowanie przez Internet w Norwegii i Estonii*, «Czas Informacji» 2010, nr 2(3).

[18] Por. I. Wróbel, *Szwajcarskie doświadczenia w głosowaniu przez Internet na przykładzie kantonu Zurych – wnioski dla Polski*, «E-Biuletyn Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej» 2008, nr 3.

[19] Por. M. Musiał-Karg, *Analiza doświadczeń związanych z wykorzystaniem głosowania internetowego (i-voting) w wybranych państwach*, «Zeszyty Prawnicze Biura Analiz Sejmowych» 2018, nr 1(57), s. 60–61.

nie zapisują je na nośnikach pamięci, które członkowie komisji wyborczych wprowadzają do centralnego systemu, bądź od razu przesyłają informacje o oddanych głosach do centralnego rejestru. Najpopularniejsze rozwiązania opierają się na systemach optycznego skanowania (*Optical Mark Recognition systems*, OMR), „które rozpoznają głosy oddane przez wyborców na specjalnych kartach do głosowania (dostosowanych do odczytu przez skanery)"[20] i urządzeniach umożliwiających bezpośrednie oddanie głosu na wybranego kandydata (*Direct recording electronic voting machines*, DRE) bez możliwości lub z możliwością uzyskania potwierdzenia jego oddania[21].

W 2006 r. grupa specjalistów od cyberbezpieczeństwa uzyskała dostęp do jednej z najpopularniejszych maszyn do głosowania – AccuVote-TS, za pośrednictwem której głosowało 10% uprawnionych obywateli USA (głównie mieszkańców stanów Georgia i Maryland). Wyniki analizy sprzętu i oprogramowania oferowanego przez spółkę Diebold Election Systems, pokazały, że:

- Złośliwe oprogramowanie może kraść głosy na maszynie do głosowania, pozostając praktycznie niewykrywalne, nawet przy dokładnej analizie zapisów;
- Każdy, kto ma fizyczny dostęp do maszyny do głosowania czy karty pamięci, może zainstalować złośliwe oprogramowanie w ciągu minuty, co jest możliwe ze względu na brak nadzoru nad maszynami;
- Maszyny AccuVote-TS są podatne na wirusy, które mogą automatycznie i niewidocznie rozprzestrzeniać się między urządzeniami i instalować złośliwe oprogramowanie[22].

Wydawać by się mogło, że przedmiotowe wyniki będą stanowiły asumpt do podjęcia działań mających na celu zwiększenia poziomu bezpieczeństwa maszyn wykorzystywanych w głosowaniu. Kroki podjęte przez ich producenta okazały się jednak niewystarczające. W 2018 r. podczas imprezy „Hursti Hack" pokazano, że w systemie do głosowania Diebold wciąż istnieje wiele poważnych luk bezpieczeństwa, natomiast w 2024 r. Hari Hursti bez większych problemów zhakował maszynę do głosowania wykorzystywaną w USA podczas trwającego na żywo podcastu[23]. Świadczy to o tym, że producenci tego rodzaju urządzeń nie przywiązują należytej wagi do zapewnienia odpowiedniego poziomu bezpieczeństwa swoich produktów.

---

20 M. Musiał-Karg, *Analiza doświadczeń*…, s. 48; *Introducing Electronic Voting: Essential Considerations, International Institute for Democracy and Electoral Assistance (International IDEA)*, Policy Paper, December 2011, s. 10–11.

21 Tamże.

22 A. J. Feldman, J. A. Halderman, E. W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, 13 września 2006, http://citp.princeton.edu/pub/ts06full.pdf (31.03.2011), s. 2.

23 PBD Podcast, *"Never Trust, Always Verify" – Harri Hursti Hacks a Voting Machine LIVE on PBD Podcast!*, https://www.youtube.com/watch?v=FTtZgN9oYVQ (25.09.2024).

Należy również postawić pytanie, czy możliwe jest, aby maszyna służąca do liczenia głosów podała błędny wynik? Taka sytuacja zdarzyła się na Florydzie podczas wyborów prezydenckich w 2000 r. Działaczka partii demokratycznej Deborah Tannenbaum obserwując wyniki zamieszczane online zauważyła, że liczba głosów oddanych na Ala Gora zmniejszyła się o nagle 16 000[24]. Wkrótce okazało się, że w okręgu 216. mieszczącym się w hrabstwie Volusia zagłosowało 412 osób, ale George Bush otrzymał tam 2813 głosów, natomiast wynik Ala Gore'a był ujemny i wynosił minus 16 022 głosy. Po krótkim śledztwie stwierdzono, że cała sytuacja była skutkiem błędu karty pamięci[25]. Omawiany przykład pokazuje, że w przypadku braku tradycyjnych kart do głosowanie trudno jest mówić o jakiejkolwiek społecznej kontroli wyników wyborów. W sytuacji, gdy głosy są oddawane na maszynie wyposażonej w ekran dotykowy (DRE) proces ich zliczania nie jest transparentny. Możliwości weryfikacji poprawności zliczania głosów dodatkowo ogranicza producent ze względu na tajemnice przedsiębiorstwa. To właśnie brak możliwości zapewnienia odpowiedniej transparentności procesu wyborczego stał się powodem, dla którego władze Republiki Federalnej Niemiec na początku 2024 r. zakazały używania elektronicznych maszyn do głosowania[26].

Kolejnym zagrożeniem związanym z e-głosowaniem jest ograniczenie możliwości udziału w nim części wyborców, co może wpłynąć na rezultat wyborów i podważyć fundamenty demokratycznego państwa. Można tego dokonać atakując elektroniczne bazy (spisy) wyborców. W przypadku dokonania drobnych zmian w adresach lub numerach identyfikacyjnych (np. PESEL) mogłoby się zdarzyć, że okazywane w lokalach wyborczych dokumenty tożsamości nie byłyby zgodne z danymi znajdującymi się w bazie. Możliwa jest również awaria systemu, która uniemożliwiłaby przeprowadzenie elektronicznego głosowania. Taka sytuacja miała miejsce w 2016 r. w Durnham, kiedy na skutek błędów systemu weryfikacja osób uprawnionych do głosowania stała się niemożliwa. Sytuacja ta wymusiła powrót do tradycyjnej metody głosowania[27]. Chociaż śledztwo władz federalnych nie wykazało, by przyczyną problemów był atak

---

[24] D. Milbank, *Tragicomedy of Errors Fuels Volusia Recount*, https://www.washingtonpost.com/archive/politics/2000/11/12/tragicomedy-of-errors-fuels-volusia-recount/5a74f0e0-565b-4980-8ed6-8bed5ff6b19f (29.09.2024).

[25] P. Meyer, *Glitch led to 'Bush wins' call*, http://www.unc.edu/~pmeyer/usat29nov2000.html (13.03.2013).

[26] D. Levi, *Finnish hacker Harri Hursti hacks U.S. voting machine on live podcast*, https://techstartups.com/2024/09/25/finnish-hacker-harri-hursti-hacks-u-s-voting-machine-on-live-podcast (25.09.2024).

[27] A. de Vouge, D. Sayers, T. LoBiance, *N.C. Board of Elections extends voting in Durham County*, https://edition.cnn.com/2016/11/08/politics/north-carolina-durham-county-glitch (8.11.2016).

hakerski[28], to sytuacja ta pokazała podatność na zagrożenia kolejnego elementu elektronicznego systemu wyborczego.

Głosowanie za pośrednictwem Internetu

Na potrzeby niniejszego artykułu, za Magdaleną Musiał-Karg przyjęto, że „systemy głosowania internetowego polegają na tym, że oddane głosy przekazywane są za pośrednictwem Internetu do centralnego serwera zliczającego głosy. Głosy można oddawać zarówno z komputerów publicznych (maszyn do głosowania), tzw. kiosków wyborczych, jak i z dowolnego komputera z dostępem do Internetu"[29].

Maciej Broniarz i Tomasz Zieliński podkreślają, że „klasyczne wybory [w Polsce – przyp. M. Sz.] to ponad 31 tysięcy obwodów wyborczych. Tak duże rozproszenie sprawia, że trudno zakłócić je w dużej skali. Inaczej mogłoby być podczas wyborów przez Internet. Sabotaż infrastruktury serwerowej wymaga znalezienia tylko jednego słabego punktu – a gdy go nie będzie, pozostaje klasyczny DDOS (atak polegający na zalaniu serwerów taką liczbą żądań, której nie będą w stanie obsłużyć)"[30].

Innym ryzykiem przy głosowaniu przez Internet mogą być ataki phishingowe, w których przestępca podszywa się pod inną osobę lub instytucję w celu zdobycia danych autoryzacyjnych wyborcy lub zainstalowania złośliwego oprogramowania, które pozwoli owe dane pozyskać. Tym sposobem niczego nieświadomy wyborca przekazałby dane umożliwiające oddanie za niego głosu osobie trzeciej. Zespół badawczy FortiGuard Labs wykrył, że w związku z wyborami odbywającymi się w USA w 2024 r. powstało ponad tysiąc nowych domen internetowych zawierających fałszywe informacje, wśród nich m.in. strona imitująca witrynę ActBlue wykorzystywaną do zbierania funduszy na cele polityczne[31]. Dodatkowo zauważono, że pojawiły się

[28] M. Boughton, *Feds: Hacking didn't cause 2016 election problems in Durham*, https://ncnewsline.com/briefs/feds-hacking-didnt-cause-2016-election-problems-in-durham/ (31.12.2019).

[29] M. Musiał-Karg, *Głosowanie przez Internet. Skąd czerpać wzorce i jak wprowadzać innowacje wyborcze?*, Forum Idei Fundacji Batorego, https://www.batory.org.pl/publikacja/glosowanie-przez-internet-skad-czerpac-wzorce-i-jak-wprowadzac-innowacje-wyborcze (10.06.2024); N. Lubik-Reczek, I. Kapsa, M. Musiał-Karg, *Elektroniczna*…, s. 47.

[30] M. Broniarz, T. Zieliński, *Głosowanie internetowe. Dlaczego nie teraz?*, Forum Idei Fundacji Batorego, https://www.batory.org.pl/publikacja/glosowanie-internetowe-dlaczego-nie-teraz (10.06.2024), s. 2.

[31] FortiGuard Research, *Threat Intelligence Report* (Threat Report – 2024100852272), https://www.fortinet.com/content/dam/fortinet/assets/intelligence-reports/FortiGuard-Labs-2024-US-Election-Security-Report.pdf (8.10.2024).

osoby sprzedające zestawy phishingowe zaprojektowane do podszywania się pod kandydatów na prezydenta USA[32].

Paweł Zając uważa, że zasada tajności głosowania jest marginalizowania podczas *i-votingu* z powodu braku rzeczywistej ochrony tajności wyborów[33]. Dzieje się tak gdyż, instytucja publiczna „weryfikując obywatela oraz nadając mu uprawnienia, gromadzi informacje pozwalające na jego późniejszą identyfikację"[34]. Stanowi to wyzwanie, ale dzięki zastosowaniu technologii blockchain możliwe jest usunięcie tożsamości wyborcy zanim dotrze ona do instytucji wyborczej[35]. Inne rozwiązanie zastosowano w Estonii, gdzie system automatycznie szyfruje głos wyborcy, umieszczając go w wirtualnej „wewnętrznej kopercie". Następnie, wyborca potwierdza swój głos, używając podpisu elektronicznego lub kodu PIN2, co tworzy z kolei „zewnętrzną kopertę" zawierającą jego dane osobowe. Wszystkie głosy, zabezpieczone podwójnym systemem kopert cyfrowych, są przesyłane do centralnego systemu. Tam przechodzą weryfikację, której celem jest wykrycie i wyeliminowanie ewentualnych wielokrotnych głosowań. Przed rozpoczęciem liczenia głosów, system usuwa „zewnętrzne koperty", a zaszyfrowane głosy, pozbawione już informacji o głosujących, trafiają do wirtualnej urny wyborczej, gdzie oczekują na zliczenie[36].

Pozostają problemy aktualne dla każdej formy głosowania na odległość tj. możliwość przekazania danych koniecznych do oddania głosu osobie trzeciej bądź głosowanie pod czyimś nadzorem (np. członka rodziny forsującego wybór „właściwej" partii). Podejmowane są jednak próby mające minimalizować możliwość wystąpienia takich sytuacji – przykładowo „system estoński zabezpiecza przed sprzedażą głosów i wymuszeniami poprzez możliwość

---

32 Tamże.

33 P. Zając, *Tajność głosowania a i-voting. Wątpliwości prawne związane z głosowaniem przez internet*, «Cybersecurity and Law» 2019, nr 2, s. 25–37.

34 M. Sobota, *Wybrane aspekty głosowania elektronicznego*, «Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie» 2016, z. 96, s. 419.

35 Por. J. Walewski, *Blockchain a wybory: czy nowa technologia może wzmocnić demokrację i zmienić to, jak głosujemy?*, https://bitcoin.pl/blockchain-wybory (12.10.2023); R. Taş, Ö. Ö. Tanrıöver, *A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting*, «Symmetry» 2020, vol. 12(8); F. S. Hardwick, A. Gioulis, R. N. Akram, K. Markantonakis, *E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy*, [w:] *IEEE 2018 International Congress on Cybermatics. 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology*, Halifax 30 lipca–3 sierpnia 2018.

36 O. Kuban, *Od tradycyjnego głosowania do e-votingu. Analiza doświadczeń Republiki Estońskie*, «Refleksje» 2010, nr 22, s. 20–22; I. Dyś-Branicka, *E-voting jako alternatywna procedura głosowania na przykładzie Estonii – szanse i zagrożenia*, Wrocław 2016, s. 263.

odwołania głosu złożonego elektronicznie"[37]. Ponadto, zgodnie z estońską ordynacją wyborczą „oddawać można kilka głosów, z tym, że ważnym jest zawsze ostatni. Oddanie głosu w sposób tradycyjny unieważniało ten oddany przez Internet"[38].

Konieczne jest również zabezpieczenie infrastruktury i systemu przed nieautoryzowanym dostępem. W przypadku dostania się do niego osoby niepowołanej, istniałoby ryzyko dla integralności danych, polegające na zmianie wyników uzyskanych przez kandydatów lub zaszyfrowania dostępnych danych (atak typu *ransomware*). Kluczowe znaczenie ma tutaj zapewnienie odpowiedniego bezpieczeństwa systemów wykorzystywanych przez komisje wyborcze, bowiem nawet wtedy kiedy wybory odbywają się w formie tradycyjnej, to wyniki głosownia z poszczególnych komisji lub obwodów przekazywane są zwykle droga elektroniczną. W październiku 2014 r., dzień przed ogłoszeniem wyników wyborów prezydenckich na Ukrainie, grupa hakerów nazywająca siebie CyberBerkut zinfiltrowała centralne systemy komputerowe ukraińskiej komisji wyborczej. Gdyby złośliwe oprogramowanie, które zainstalowali, nie zostało odkryte i usunięte, wyświetliłoby fałszywe wyniki wskazujące, że przywódca ultraprawicowego Sektora Prawicy, Dmytro Jarosz, zdobył 37% głosów, zamiast 1%, który otrzymał[39].

Dezinformacja jako zagrożenie dla procesu wyborczego

Kampanie wyborcze w coraz większym stopniu toczą się w przestrzeni wirtualnej. Internet oferuje możliwość skutecznego dotarcia do potencjalnych wyborców oraz pozwala znaleźć wiele informacji o osobach kandydujących. Zdaniem Krzysztofa Dudy, wdrożenie rozwiązań z zakresu elektronicznego głosowania „może spowodować również większe skupienie się na kampanii w Internecie"[40]. Sieć stała się jednak nie tylko miejscem pozyskiwania rzetelnych informacji czy też agitacji wyborczej, ale również polem walki informacyjnej. Od początku XX wieku coraz częściej mamy do czynienie z dezinformacją polegającą na systematycznym i profesjonalnym wykorzystaniu metod propagandowych w celu szerzenia nieprawdziwych informacji głównie w przestrzeni wirtualnej. Podmioty stosujące tego rodzaju działania chcą wpływać na całe

[37] M. Kutyłowski, *E-voting: głosowanie elektroniczne*, «Infos» 2009, nr 10(57), s. 2 za: K. Duda, *E-voting*…, s. 163.
[38] K. Duda, *E-voting*…, s. 163.
[39] *Ukrainian parliamentary election interference*, https://cyberlaw.ccdcoe.org/wiki/Ukrainian_parliamentary_election_interference_(2014) (1.10.2024).
[40] K. Duda, *E-voting*…, s. 166.

populacje wierząc, że „za pomocą odpowiednio dobranego przekazu dezinformacyjnego da się: skłócić państwa; sprawić, że ludzie zerwą relacje z najbliższymi albo znienawidzą się wzajemnie; przekonać innych, by podjęli złe dla swego zdrowia i życia decyzje; wywołać zamieszki; doprowadzić do destabilizacji politycznej w dowolnym kraju; zburzyć zaufanie społeczne do instytucji publicznych, do nauki"[41]. W przypadku wyborów mają one wpłynąć na potencjalnych głosujących zachęcając ich do wsparcia określonego kandydata, bądź zniechęcając do wzięcia udziału w wyborach.

Dezinformatorzy pozostają zazwyczaj anonimowi. Krzysztof Żarna uważa, że są to zwykle członkowie „grup (organizacji, instytucji, agencji, jednostek wojskowych), które prowadzą działania zarówno w sferze wpływu, jak i szeroko rozumianej dezinformacji"[42]. Świadczy to o tym, że takie działania są realizowane w profesjonalny sposób w celu osiągnięcia wyznaczonych celów, a nie są efektem żartów czy też niefrasobliwości użytkowników Internetu.

Hillary Clinton wspominając przegraną kampanię wyborczą podkreśla, że „Rosjanie generowali propagandę (…) na przykład za pośrednictwem stron z fałszywymi wiadomościami oraz internetowych trolli, którzy publikowali napastliwe wpisy na Facebooku i Twitterze. (…) Badacze z Uniwersytetu Południowej Kalifornii odkryli, że niemal 20% wszystkich wpisów na Twitterze o treści politycznej wysłanych między 16 września a 21 października 2016 r. zostało wygenerowanych przez boty. Wiele z nich prawdopodobnie wyszło spod ręki Rosjan"[43]. Jednym z przykładów potwierdzających skuteczność tego rodzaju działań jest tzw. „Pizzagate". Na skutek prowadzonej dezinformacji i fałszywej interpretacji wykradzionych wiadomości mailowych Johna Podesty powstała teoria spiskowa, zgodnie z którą politycy Partii Demokratycznej zamieszani byli w handel dziećmi, który miał odbywać się w Comet Ping Pong Pizza w Waszyngtonie. Do lokalu wtargnął nawet uzbrojony mężczyzna, który z powodu bierności służb chciał sam zbadać sprawę i zakończyć trwający proceder[44]. Przykład ten pokazuje, że dzięki zastosowaniu technik manipulacji i socjotechniki fałszywe informacje, niepoparte wiarygodnymi dowodami, mogą w erze mediów społecznościowych wpłynąć na sposób postrzegania rzeczywistości przez ich odbiorców.

---

41 A. Mierzyńska, *Efekt niszczący: jak dezinformacja wpływa na nasze życie*, Warszawa 2022, s. 5.

42 K. Żarna, *Wybrane przykłady dezinformacji podczas kampanii wyborczej do Rady Narodowej Republiki Słowackiej w 2023 roku*, «Politeja» 2024, nr 1(88/2), s. 158.

43 H. R. Clinton, *Co się stało*, Katowice 2018, s. 396–398.

44 A. Robb, *Pizzagate: Anatomy of a Fake News Scandal*, https://www.rollingstone.com/feature/anatomy-of-a-fake-news-scandal-125877/ (16.11.2017).

Działania dezinformacyjne miały również miejsce podczas wyborów, które odbyły się na Słowacji w 2023 r. Fałszywe sondaże rzekomo opublikowane w zagranicznych mediach, spoty wyborcze wygenerowane z pomocą sztucznej inteligencji i wykorzystujące głosy znanych słowackich polityków czy też fałszywe materiały video wykorzystujące wizerunki politycznych przeciwników (tzw. deepfake'i) były przekazywane za pośrednictwem mediów społecznościowych oraz komunikatorów internetowych[45]. Trudno określić, w jakim stopniu wpłynęły one na końcowy wynik wyborów[46]. O ich skuteczności może jednak świadczyć fakt, że są one kontynuowane na coraz szerszą skalę.

Wnioski

Obowiązujące procedury wyborcze powinny być stale ulepszane i dostosowywane do potrzeb społeczeństwa. Zgodnie z rekomendacjami Organizacji Bezpieczeństwa i Współpracy w Europie system głosowania elektronicznego powinien zapewniać: tajność głosowania, integralność wyników, równość głosu, powszechność głosowania, przejrzystość, rozliczalność, prawo do skutecznego środka odwoławczego, ochronę prywatności i danych osobowych, a także gwarantować właściwy poziom społecznego zaufania do niego[47]. Jednakże, Peter G. Neumann dostrzega w tym pewien paradoks, bowiem z jednej strony dąży się do zachowania wymogu tajności głosowania, ale z drugiej konieczne jest dokładne monitorowanie całego procesu, aby był on jak najbardziej jawny i transparentny[48]. Osiągnięcie obu wymogów jednocześnie jest niemożliwe bez stosowania skomplikowanych mechanizmów, które z kolei mogą wprowadzać nowe potencjalne podatności na ataki[49]. Ponadto „każda technika pozwalająca na identyfikację i uwierzytelnienie wyborcy w przypadku zakwestionowania wyników wyborów niewątpliwie prowadziłaby do nasilenia sporów i dalszego ograniczenia prywatności wyborców"[50]. Warto podkreślić, że samo ryzyko zakwestionowania prawidłowości wyborów może prowadzić do podważenia prawa suwerena do samostanowienia oraz wywołać chaos w państwie, gdyby zwolennicy przegranego kandydata nie uznali wyniku wyborów.

45 K. Żarna, *Wybrane*…, s. 161–165.
46 Tamże, s. 166.
47 Handbook for the Observation of Information and Communication Technologies (ICT) in Elections (OSCE/ODIHR), https://www.osce.org/files/f/documents/c/9/558318_0.pdf, (11.11.2024), s. 23–28.
48 P. G. Neumann, *Security Criteria for Electronic voting*, [w:] *Proceedings of the 16th National Computer Security Conference*, Baltimore 1993, s. 481.
49 Tamże.
50 Tamże.

Głosowanie za pośrednictwem Internetu opiera się na wzajemnym zaufaniu. Obywatele muszą mieć przekonanie, że organy państwa zadbały o to, aby cały proces był nie tylko uczciwy i możliwie jak najbardziej transparentny, ale przede wszystkim bezpieczny. Z kolei przedstawiciele państwa muszą wierzyć, że obywatele nie będą dopuszczali się manipulacji i nadużyć podczas procesu wyborczego. Zasadniczym problemem w przypadku *i-votingu* jest ograniczenie kontroli społecznej rezultatu głosowania. Informacja o zwycięzcy jest przekazywana przez system elektroniczny, tymczasem najlepszym sposobem sprawdzenia wyników wyborów wciąż pozostaje weryfikacja wypełnionych kart do głosowania. Jeśli nie ma papierowego śladu, to w przypadku wątpliwości traci się możliwość skutecznego audytu procesu liczenia głosów.

Z kolei w przypadku głosowań wspomaganych elektronicznie należy pamiętać, że wykorzystywane w nich urządzenia to komputery, które podobnie jak wszystkie inne urządzenia elektroniczne mogą zostać zhakowane. Zdaniem niektórych autorów, systemy do głosowania elektronicznego stworzone przez podmioty prywatne cechują się licznymi lukami w zabezpieczeniach[51]. Dlatego wydaje się, że najlepszym sposobem na zwiększenie poziomu zaufania do wyborów jest zastosowanie rozwiązań typu *open source*. Publiczne udostępnienie kodów źródłowych sprawi, że wykorzystywane rozwiązania zostaną poddane ogromnej liczbie testów, co pozwoli wykryć istniejące podatności i wnikliwie zweryfikować bezpieczeństwo całego systemu.

W przypadku zwalczania dezinformacji konieczna jest współpraca organów państwa z platformami internetowymi w celu szybkiego oznaczania i usuwania nieprawdziwych treści. Ponadto należałoby się zastanowić nad zasadnością ciszy wyborczej. Zwalczanie nieprawdziwych informacji opublikowanych podczas jej trwania jest utrudnione a politycy będący ich ofiarą mają ograniczone prawo do obrony. Ponadto bardzo łatwo można ominąć istniejące restrykcje, gdyż „w Internecie na polskojęzycznych stronach www ulokowanych na zagranicznych serwerach może być prowadzona agitacja wyborcza, a na zagranicznych portalach informacyjnych mogą być podawane wyniki sondaży wyborczych"[52].

Zapewnienie bezpiecznego, transparentnego, uczciwego oraz wiarygodnego procesu wyborczego w erze nowych technologii jest kluczowym wyzwaniem stojącym przez organami władzy publicznej. Elektroniczne systemy głosowania niosą ze sobą zarówno szanse, jak i zagrożenia dla bezpieczeństwa i wiarygodności wyborów. Kluczowe znaczenie ma odpowiednie zaprojektowanie i zabezpieczenie tych systemów, a także zapewnienie wyborcom

51 Tamże.

52 M. Musiał-Karg, *Cisza wyborcza w dobie Internetu*, «Przegląd Sejmowy» 2013, nr 3(116), s. 32.

poczucia bezpieczeństwa i zaufania do nowego rozwiązania. Należy przy tym pamiętać, że podważenie bezpieczeństwa procesu wyborczego może mieć daleko idące skutki. Dlatego możliwość elektronicznego głosowania powinna zostać umożliwiona obywatelom jedynie w przypadku, kiedy państwo jest w stanie zapewnić odpowiednie standardy bezpieczeństwa całego procesu oddawania głosów, a suweren będzie przekonany, że wynik wyborów będzie wiarygodny i rzetelny.

Bibliografia

Berg S., Hofmann J., *Digital democracy*, «Internet Policy Review» 2021, nr 10(4).

Boughton N., *Feds: Hacking didn't cause 2016 election problems in Durham*, https://ncnewsline.com/briefs/feds-hacking-didnt-cause-2016-election-problems-in-durham (31.12.2019).

Broniarz M., Zieliński T., *Głosowanie internetowe. Dlaczego nie teraz?*, Forum Idei Fundacji Batorego, https://www.batory.org.pl/publikacja/glosowanie-internetowe-dlaczego-nie-teraz (10.06.2024).

Browning G., *Electronic Democracy. Using the internet to Transform American Politics*, Medford–New Jersey 2006.

Clinton H. R., *Co się stało*, Katowice 2018.

Czajkowski M., *E-voting na przykładzie Estonii i Brazylii*, «Studia BAS» 2011, nr 3(27).

de Vouge A., Sayers D., LoBiance T., *N.C. Board of Elections extends voting in Durham County*, https://edition.cnn.com/2016/11/08/politics/north-carolina-durham-county-glitch (8.11.2016).

Duda K., *E-voting jako forma demokracji bezpośredniej. Dotychczasowe doświadczenia i konsekwencje*, «Refleksje» 2011, nr 4.

Dyś-Branicka I., *E-voting jako alternatywna procedura głosowania na przykładzie Estonii – szanse i zagrożenia*, Wrocław 2016.

Feldman A. J., Halderman J. A., Felten E. W., *Security Analysis of the Diebold AccuVote-TS Voting Machine*, 13 września 2006, http://citp.princeton.edu/pub/ts06full.pdf (31.03.2011).

Gajowniczek T., *Elektroniczna demokracja – istota pojęcia i problemy definicyjne*, [w:] W. Tomaszewski, D. M. Mościcka, A. Jurkun (red.), *Demokracja a wybory. Współczesne dylematy i wyzwania*, Olsztyn 2015.

Gibson J. P., Krimmer R., Teague V., Pomares J., *A review of E-voting: the past, present and future*, «Annals of Telecommunications» 2016, vol. 71.

Grodzka D., *E-demokracja*, «Infos» 16 lipca 2009, nr 14(61).

Hardwick F. S., Gioulis A., Akram R. N., Markantonakis K., *E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy*, [w:] *IEEE 2018 International Congress on Cybermatics. 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology*, Halifax 30 lipca–3 sierpnia 2018.

Krimmer R., *E-voting as a New Form of Voting*, [w:] A. Balci, C. Can Actan, O. Dalbay (red.), *Explorations in eGovernment & eGovernance. Volume 2: Selected proceedings of the Second International Conference on eGovernment and eGovernance*, Antalya 2010.

Kuban O., *Od tradycyjnego głosowania do e-votingu. Analiza doświadczeń Republiki Estońskie*, «Refleksje» 2010, nr 22.

Kutyłowski M., *E-voting: głosowanie elektroniczne*, «Infos» 2009, nr 10(57).
Levi D., *Finnish hacker Harri Hursti hacks U.S. voting machine on live podcast*, https://tech-startups.com/2024/09/25/finnish-hacker-harri-hursti-hacks-u-s-voting-machine-on-live-podcast (25.09.2024).
Lubik-Reczek N., Kapsa I., Musiał-Karg M., *Elektroniczna partycypacja w Polsce. Deklaracje i opinie Polaków na temat e-administracji i e-głosowania*, Poznań 2020.
Macintosh A., *Characterizing E-Participation in Policy-Making*, [w:] *Proceedings of the 37th Hawaii International Conference on System Sciences*, Big Island 2004.
Madise U., Vinkel P., Maaten R., *Internet Voting at the Elections of Local Government Councils on October 2005. Report*, http://www.vvk.ee/public/dok/report2006.pdf (11.11.2024).
Marczewska-Rytko M., *Idea demokracji bezpośredniej od okresu antycznego do czasów Internetu i globalizacji*, [w:] M. Marczewska-Rytko, A. K. Piasecki, *Demokracja bezpośrednia. Wymiar globalny i lokalny*, Lublin 2010.
Meyer P., *Glitch led to 'Bush wins' call*, http://www.unc.edu/~pmeyer/usat29nov2000.html (13.03.2013).
Mierzyńska A., *Efekt niszczący: jak dezinformacja wpływa na nasze życie*, Warszawa 2022.
Milbank D., *Tragicomedy of Errors Fuels Volusia Recount*, https://www.washingtonpost.com/archive/politics/2000/11/12/tragicomedy-of-errors-fuels-volusia-recount/5a74f0e0-565b-4980-8ed6-8bed5ff6b19f/ (29.09.2024).
Musiał-Karg M., *Analiza doświadczeń związanych z wykorzystaniem głosowania internetowego (i-voting) w wybranych państwach*, «Zeszyty Prawnicze Biura Analiz Sejmowych» 2018, nr 1(57).
Musiał-Karg M., *Cisza wyborcza w dobie Internetu*, «Przegląd Sejmowy» 2013, nr 3(116).
Musiał-Karg M., *E-demokracja, e-partycypacja i e-głosowanie, czyli o tym jak zwiększać zaangażowanie obywateli w dobie Internetu*, [w:] M. Rachwał (red.), *Uwarunkowania i mechanizmy partycypacji politycznej*, Poznań 2017.
Musiał-Karg M., *E-voting (as a form of E-democracy) in the European Countries*, [w:] A. Balci, C. Can Actan, O. Dalbay (red.), *Explorations in eGovernment & eGovernance. Volume 2: Selected proceedings of the Second International Conference on eGovernment and eGovernance*, Antalya 2010.
Musiał-Karg M., *Electronic democracy and its organization – a revolution or a modernization? The example of e-voting*, «Politbook» 2012, nr 2.
Musiał-Karg M., *Głosowanie przez Internet. Skąd czerpać wzorce i jak wprowadzać innowacje wyborcze?*, Forum Idei Fundacji Batorego, https://www.batory.org.pl/publikacja/glosowanie-przez-internet-skad-czerpac-wzorce-i-jak-wprowadzac-innowacje-wyborcze, (10.06.2024).
Musiał-Karg M., *Internetowe głosowanie w Estonii na przykładzie wyborów w latach 2005–2009*, «Przegląd Politologiczny» 2011, nr 3.
Neumann P. G., *Security Criteria for Electronic voting*, [w:] *Proceedings of the 16th National Computer Security Conference*, Baltimore 1993.
Nowina Konopka M., *Elektroniczna urna*, https://bip.brpo.gov.pl/pliki/12066058070.pdf (11.11.2024).
Robb A., *Pizzagate: Anatomy of a Fake News Scandal*, https://www.rollingstone.com/feature/anatomy-of-a-fake-news-scandal-125877 (16.11.2017).
Sobota M., *Wybrane aspekty głosowania elektronicznego*, «Zeszyty Naukowe Politechniki Śląskiej. Organizacja i zarządzanie» 2016, z. 96.
Taş R., Tanrıöver Ö. Ö., *A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting*, «Symmetry» 2020, vol. 12(8).

Walewski J., *Blockchain a wybory: czy nowa technologia może wzmocnić demokrację i zmienić to, jak głosujemy?*, https://bitcoin.pl/blockchain-wybory (12.10.2023).
Wróbel I., *Szwajcarskie doświadczenia w głosowaniu przez Internet na przykładzie kantonu Zurych – wnioski dla Polski*, «E-Biuletyn Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej» 2008, nr 3.
Zagórski F., *Głosowanie przez Internet w Norwegii i Estonii*, «Czas Informacji» 2010, nr 2(3).
Zając P., *Tajność głosowania a i-voting. Wątpliwości prawne związane z głosowaniem przez internet*, «Cybersecurity and Law» 2019, nr 2.
Żarna K., *Wybrane przykłady dezinformacji podczas kampanii wyborczej do Rady Narodowej Republiki Słowackiej w 2023 roku*, «Politeja» 2024, nr 1(88/2).