VOL. 20 | STUDIA POLITOLOGICZNE

Daniel Mider

Głosowanie przez Internet a demokracja

Słowa kluczowe:
socjologia Internetu, elektroniczna demokracja, wybory przez Internet, elektroniczne głosowanie, głosowanie przez Internet

Wstęp

Głosowanie uznawane jest za istotę systemu demokratycznego, jego fundamentalną zasadę, warunek konieczny i wystarczający wielu znaczących definicji w teorii demokracji. Gwarantuje ono obywatelom możliwość sprawowania władzy poprzez przedstawicieli wybranych z zachowaniem określonych procedur[1]. Takie stanowisko odnajdujemy w rozważaniach uznanych badaczy demokracji; szczególnie wyraziste ujęcie występuje w koncepcji demokracji proceduralnej Josepha A. Schumpetera, który uważał, że aktywność obywateli w demokracji powinna ograniczać się wyłącznie do aktu wyborów[2]. Za podstawową regułę demokracji wybory uznają również Robert A. Dahl[3], Philippe C. Schmitter i Terry L. Karl[4],

---

1 A. Ranney, W. Kendall, *Basic Principles for a Model of Democracy*, [w:] Ch.F. Cnudde, D.E. Neubauer (ed.), *Empirical Democratic Theory*, Chicago 1969, s. 45–51.

2 J.A. Schumpeter, *Kapitalizm, socjalizm, demokracja*, Warszawa 1995, s. 368. Podobne stanowisko odnajdujemy u pierwszych badaczy demokracji: André Siegfrieda (A. Siegfried, *Tableau politique de la France de l'ouest sous la troisième République*, Paryż 1913 (reedycja 1980), Herberta Tingstena (H. Tingsten, *Political Behavior: Studies in Election Statistics*, Londyn 1937) oraz Harolda Gosnella (H. Gosnell, *Why Europe Votes*, Chicago 1930).

3 R.A. Dahl, *Demokracja i jej krytycy*, Warszawa 1995.

4 P.C. Schmitter, T.L. Karl, *What Democracy is … and is not*, „Journal of Democracy" 1991, nr 2 (3), s. 75–88.

a także Samuel P. Huntington[5], Francis Fukuyama[6] i Seymour M. Lipset[7]. Instytucja wyborów ma podstawowe znaczenie dla legitymizacji systemu politycznego i elit, jest ponadto silnie zinstytucjonalizowana – co przejawia się między innymi uregulowaniem jej w ustawie zasadniczej oraz aktach prawa międzynarodowego.

W niniejszym artykule podjęto próbę oceny wpływu głosowania z użyciem Internetu na demokrację przedstawicielską. Wybory w demokracjach mają charakter powtarzalny, regularny, wymagają cyklicznego wysiłku aparatu administracyjnego, elit politycznych i wyborców, wiążą się ponadto ze znacznymi kosztami, stąd wynikają stałe poszukiwania nowych rozwiązań, które czyniłyby je tańszymi i bardziej efektywnymi. Szczególną rolę w procesie usprawniania mechanizmu wyborów w demokracjach odgrywają nowe technologie, ich pojawienie się nieodmiennie budzi nadzieje na wyeliminowanie defektów demokracji przedstawicielskiej. Pierwsze próby ułatwienia procesu głosowania za pomocą środków technicznych szły w parze z rozwojem demokracji i upowszechnianiem praw wyborczych. W pierwszej połowie XIX wieku w Wielkiej Brytanii Czartyści zaproponowali wdrożenie mechanicznego urządzenia do głosowania wynalezionego przez Benjamina Jolly[8], a w 1869 roku w Stanach Zjednoczonych Tomasz A. Edison opatentował pierwszą elektryczną maszynę umożliwiającą oddawanie głosów[9]. Dotychczasowe próby zastosowania rozwiązań technicznych do przeprowadzania wyborów nie przyniosły oczekiwanych efektów – w demokracjach wciąż dominuje tradycyjny sposób głosowania z użyciem papierowych kart i urn wyborczych. Pojawienie się Internetu obudziło szczególnie silne nadzieje – uznano go za wynalazek mający najbardziej doniosłe w historii demokracji znaczenie nie tylko dla modernizacji technik wyborczych, lecz również umożliwiający naprawę wadliwie działających niektórych instytucji i procedur tego systemu. Postulat wyborów przy użyciu tego medium podejmowany jest

---

5 S.P. Huntington, *Trzecia fala demokratyzacji*, Warszawa 1995, s. 16, 17.

6 F. Fukuyama, *Koniec historii*, Poznań 1996, s. 77.

7 S.M. Lipset, *Some Social Requisites of Democracy: Economic Development and Political Legitimacy,* [w:] Ch.F. Cnudde, D.E. Neubauer (ed.), *Empirical Democratic…,* s. 152–153.

8 D.W. Jones, *Early Requirements for Mechanical Voting Systems, First International Workshop on Requirements Engineering for E-voting Systems*, http://www.cs.uiowa.edu/~jones/voting/ReVote09history.pdf, 31.08.2009.

9 T.A. Edison, *Patent number 90646. Electric Vote-Recorder*, http://www.google.com/patents?id=k-REAAAAEBAJ&printsec=abstract&zoom=4#v=onepage&q&f=false, 1.06.1869. Był to pierwszy patent T.A. Edisona; maszyna pozwalała na prosty wybór „tak" lub „nie" przedstawionych opcji i rejestrowała informacje. Wynalazek nie wzbudził jednak zainteresowania waszyngtońskiego kongresmana i popadł w zapomnienie.

przez liczne grona naukowców, publicystów i decydentów politycznych. Pomysły modernizacji sposobu oddawania głosów uzasadniane są koniecznością odchodzenia od tradycyjnej papierowej technologii narażonej na ryzyko nadużyć i nieprawidłowości (*vide*: Stany Zjednoczone i Włochy) oraz wymagającej dużych nakładów finansowych; wśród wymienianych argumentów pojawia się także nadzieja na rewitalizację sfery publicznej, zwiększenie frekwencji wyborczej, a nawet na istotne głębokie przemiany w funkcjonowaniu systemu demokratycznego[10].

Głosowanie przez Internet (*remote Internet voting, remote I-voting*) jest jednym z typów głosowania elektronicznego i stanowi jego najbardziej zaawansowaną pod względem technologicznym formę. Pojęcie *głosowanie elektroniczne* (*electronic voting, e-voting*) jest najszersze i oznacza oddawanie głosu za pomocą mediów takich jak: elektroniczna maszyna do głosowania w postaci komputera lub terminalu (zwanego elektronicznym głosomatem, elektronicznym automatem do głosowania), telewizja kablowa, komputer osobisty stacjonarny lub mobilny, palmtop lub telefon komórkowy. Dane o głosowaniu gromadzone przez te urządzenia mogą być przesyłane za pomocą sieci Internet, sieci komputerowej innej niż Internet, sieci telefonii komórkowej, sieci telewizji kablowej lub przenoszone fizycznie. W literaturze przedmiotu najczęściej wyróżnia się rodzaje elektronicznego głosowania ze względu na miejsce oddania głosu. Najprostszym, najbezpieczniejszym, wymagającym najmniej nakładów i jednocześnie najbardziej rozpowszechnionym sposobem elektronicznego głosowania jest oddawanie głosu w lokalu wyborczym właściwym dla miejsca zamieszkania głosującego (nazywanym w anglojęzycznej literaturze *poll site* lub *precinct voting*). Proces ten jest nadzorowany przez komisję wyborczą, odbywa się za pomocą komputera lub terminalu. Jeśli głosowanie takie prowadzone jest z wykorzystaniem Internetu jako środka przesyłania wyników, wówczas w literaturze anglojęzycznej używa się nazwy *Internet voting at the polling place* (IV@PP). Nieco bardziej zaawansowaną technicznie formą głosowania elektronicznego jest umożliwienie wyborcom oddawania głosu nie tylko we właściwej dla nich komisji wyborczej, lecz w dowolnym lokalu wyborczym, a więc na terenie danego okręgu wyborczego lub nawet kraju (w zależności od typu wyborów). Tak jak w powyższym przypadku, nad prawidłowością procesu głosowania czuwają członkowie komisji. Tego typu głosowanie określane jest w zachodnioeuropejskiej literaturze przedmiotu mianem

[10] P. Gomułkiewicz, *Wirtualne wybory,* http://pigom.wroclaw.pl/teksty/wirtualne-wybory.html.

regional poll site lub *national poll site*. Najbardziej zaawansowane informatycznie i najtrudniejsze do wdrożenia jest głosowanie elektroniczne na odległość (nazywane *remote electronic voting* i czasem skrótowo, lecz błędnie *remote voting*). Obejmuje ono dwa typy rozwiązań technicznych. Pierwsze z nich to głosowanie z dedykowanych komputerów lub terminali rozmieszczonych w miejscach publicznych (na przykład w centrach handlowych, urzędach, domach kultury i innych ogólnodostępnych lokalizacjach). Nosi ono nazwę głosowania z komputerów/terminali publicznych (*kiosk voting*). W tym przypadku instytucja komisji wyborczych jest zbędna, a głosy wyborców przesyłane są bezpośrednio do centralnego serwera. Drugim typem głosowania na odległość jest możliwość oddania głosu z dowolnego miejsca – na przykład z domu lub z pracy, co może odbywać się za pomocą rozmaitych mediów: komputera stacjonarnego lub mobilnego, palmtopa, telefonu komórkowego lub telewizji kablowej. Sporadycznie do przekazania głosu wyborcy używany jest telefaks[11]. Jeśli głosowanie na odległość odbywa się z wykorzystaniem sieci Internet jako kanału przekazu między wyborcą a centralnym serwerem zbierającym głosy, wówczas nazywa się je głosowaniem przez Internet (głosowaniem *online*). W stosunku do tego typu głosowania używane są w literaturze anglojęzycznej określenia takie jak *remote Internet voting* (RIV), *online electronic/Internet voting*[12]. Należy zwrócić uwagę, że część autorów stosuje

[11] Użycie tego medium przekazu narusza zasadę tajności głosowania i dlatego jest ono wykorzystywane w nielicznych, szczególnych wypadkach, na przykład w wyborach w Stanach Zjednoczonych w głosowaniu wojskowego personelu pozostającego poza granicami kraju w dniu wyborów. R.M. Alvarez, T.E. Hall, *Point, Click & Vote. The Future of Internet Voting*, Waszyngton 2004, s. 28.

[12] Przedstawiona typologia technicznych sposobów głosowania została opracowana na podstawie następujących źródeł: *A Report on the Feasibility of Internet Voting,* California Internet Voting Task Force, http://www.sos.ca.gov/elections/ivote/final_report.pdf, 01.2000, s. 14; K. Coleman, *Internet Voting*, http://www.infousa.ru/information/rs20639.pdf, 31.01.2003, strony nienumerowane; R.K. Gibson, *Internet Voting and the European Parliament Elections. Problems and Prospects*, [w:] A.H. Trechsel, F. Mendez (ed.), *The European Union and E-voting. Addressing in the European Parliament's Internet Voting Challenge*, Londyn, Nowy Jork 2005, s. 31; A. Kiayias, M. Korman, D. Walluck, *An Internet Voting System Supporting User Privacy,* http://www.acsac.org/2006/papers/130.pdf, 2006, strony nienumerowane; T. Mägi, *Practical Security Analysis of E-voting Systems*, niepublikowana praca magisterska, Tallin University of Technology, Tallin 2007, s. 12; M. Nowina-Konopka, *Elektroniczna urna*, http://www.rpo.gov.pl/pliki/12066058070.pdf, s. 2–3; A.M. Oostveen, P. Besselaar van den, *Internet Voting Technologies and Civic Participation: the Users' Perspective,* „The Public" 2004, nr 1, s. 61, 63–64; R.L. Rivest *Electronic Voting,* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.28.5723&rep=rep1&type=pdf, 2000.

w odniesieniu do wyborów przez Internet na odległość błędne nazewnictwo, używając takich określeń jak głosowanie elektroniczne lub głosowanie elektroniczne na odległość[13]. W Tabeli 1 przedstawiono typologię technicznych sposobów głosowania porządkującą używane w literaturze przedmiotu pojęcia.

Tabela 1. Typologia technicznych sposobów oddawania głosów

<table>
<tr><td></td><td colspan="3">Zakres kontroli nad głosowaniem</td></tr>
<tr><td></td><td>Głosowanie kontrolowane bezpośrednio przez czynnik ludzki (komisję wyborczą)</td><td colspan="2">Głosowanie niekontrolowane bezpośrednio przez czynnik ludzki (komisję wyborczą)</td></tr>
<tr><td rowspan="2">Głosowanie tradycyjne</td><td rowspan="2">Głosowanie w lokalu wyborczym za pomocą tradycyjnego papierowego głosu wypełnianego ręcznie lub za pomocą mechanicznej maszyny do głosowania na przykład z użyciem kart perforowanych lub wydruku</td><td colspan="2">Głosowanie za pośrednictwem poczty tradycyjnej</td></tr>
<tr><td colspan="2">Głosowanie przez pełnomocnika</td></tr>
<tr><td rowspan="3">Głosowanie elektroniczne</td><td>Głosowanie elektroniczne z przypisaniem głosującego do określonego lokalu wyborczego (z użyciem urządzeń połączonych lub niepołączonych z siecią)</td><td rowspan="2">Głosowanie elektroniczne na odległość</td><td>Głosowanie z komputerów/ terminali publicznych</td></tr>
<tr><td>Głosowanie elektroniczne w dowolnym lokalu wyborczym (z użyciem urządzeń połączonych lub niepołączonych z siecią)</td><td>Głosowanie z dowolnego miejsca (za pomocą komputera podłączonego do Internetu (I-voting), podłączonego do sieci innej niż Internet, telefonu komórkowego, telewizji kablowej, telefaksu)</td></tr>
</table>

Źródło: zmodyfikowana i uzupełniona tabela, [za:] M. Abraham, U. Gatterbauer i in., *Remote Electronic Voting. Example Austria: General Set-Up and Political and Legal Dimensions*, http://staatswissenschaft.univie.ac.at/fileadmin/user_upload/inst_staat swissenschaften/Frisch/21063courseWebsite/remotevoting–gatterbauer–etal.pdf, 2008, s. 5.

[13] A.M. Oostveen, P. Besselaar van den, *Internet Voting…*, s. 61.

Głosowanie przez Internet może odbywać się za pomocą strony internetowej, specjalnie instalowanego programu służącego do głosowania lub z użyciem dedykowanego systemu operacyjnego instalowanego na komputerze głosującego na czas oddawania głosu. Oprogramowanie to służy do złożenia głosu oraz zaszyfrowania go. Głosy wyborców magazynowane są na centralnym serwerze, a następnie obliczane i sprawdzane. Ponadto konieczne jest oprogramowanie i infrastruktura, łączące program i maszynę używaną przez wyborcę z programami znajdującymi się na serwerze, przesyłające zaszyfrowany głos wyborcy. W głosowaniu na odległość przez Internet wyróżnia się dwie zasadnicze fazy oddawania głosu. Pierwsza z nich to rejestracja głosującego, w efekcie której wyborca otrzymuje informacje umożliwiające jego zidentyfikowanie i wzięcie udziału w głosowaniu. Druga faza, właściwa, rozpoczyna się potwierdzeniem tożsamości wyborcy, sprawdzeniem czy oddawał już głos, wskazaniem preferowanego kandydata a następnie zapisaniem dokonanego przez głosującego wyboru[14].

Próby wdrażania głosowania przez Internet na odległość

W latach 1996–2007 przeprowadzono 104 próby wyborów elektronicznych w czternastu, głównie zachodnioeuropejskich, krajach[15]. Elektroniczne głosowanie w lokalach wyborczych usiłowały z mniejszymi lub większymi sukcesami wdrażać między innymi Belgia[16], Brazylia[17], Fili-

[14] T. Mägi, *Practical Security Analysis…*, s. 16–17.

[15] M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy wyborcze. Raport*, http://www.e-glosowanie.org/images/pdf/raport_e-voting.pdf, 2008, s. 64.

[16] Elektroniczne wybory były wdrażane w Belgii od początku lat dziewięćdziesiątych. W wyborach do Parlamentu Europejskiego skorzystała z możliwości oddania głosu z użyciem komputera w lokalu wyborczym niemal połowa głosujących (44 proc.). W grudniu 2006 roku rząd belgijski powołał badaczy z siedmiu krajowych uniwersytetów do badań nad elektronicznym głosowaniem. Zakres badań stanowiły analizy organizacyjne prawne, socjologiczne i politologiczne. Szczególny nacisk położono na zapewnienie powszechności wyborów osobom niepełnosprawnym. Belgijski system głosowania przewiduje możliwość oddania głosu tylko w komisji wyborczej, nie głosuje się na odległość. Cyt. za: M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy…*, s. 14; Hasło: *Electronic voting in Belgium*, „Encyklopedia Wikipedia", http://en.wikipedia.org/wiki/Electronic_voting_in_Belgium.

[17] Eksperymenty z e-głosowaniem Brazylia rozpoczęła w drugiej połowie lat dziewięćdziesiątych, by w 2000 roku stać się jedynym krajem Ameryki Południowej, w którym wybory przeprowadzane są w pełni elektroniczne. Cyt. za: *E-Voting. Countries with e-voting projects*, ACE The Electoral Knowledge Network, http://aceproject.org/ace-en/focus/e-voting/countries, 2010.

piny[18], Holandia[19], Indie[20], Irlandia[21], Niemcy[22] i Włochy[23]. Natomiast próby z internetowym głosowaniem przeprowadziły: Australia, Estonia, Finlandia, Francja, Holandia, Japonia, Kanada, Niemcy, Stany Zjednoczone, Szwajcaria, Szwecja oraz Wielka Brytania. Prace nad wdrożeniem głosowania w Internecie kontynuują Estonia, Holandia, Szwajcaria, Australia, Francja, Japonia, Szwecja, Wielka Brytania, Kanada i Finlandia. Wdrażanie głosowania z użyciem Internetu zarzucono natomiast na skutek poniesionych porażek w Stanach Zjednoczonych oraz Niemczech.

Niewątpliwym liderem w zakresie głosowania przez Internet jest Estonia[24]. Pomysł wyborów elektronicznych pojawił się w Estonii w 2001 roku, kiedy do władzy doszły siły zorientowane na wdrażanie nowych technologii[25]. W 2002 roku wpłynął do estońskiego parlamentu projekt ustawy umożliwiający przeprowadzenie wyborów elektronicznych na szczeblu

---

[18] Kraj ten poniósł szereg porażek we wdrażaniu elektronicznego głosowania od 2010 roku. Problemy dotyczyły przede wszystkim zawodnego sprzętu. P. Cahill, E. Baculinao, *Filipinos go to the (computerized) polls*, http://worldblog.msnbc.msn.com/_news/2010/05/07/4376624-filipinos-go-to-the-computerized-polls, 7.05.2010.

[19] W Holandii na skutek licznych kontrowersji wynikłych z udowodnienia możliwości naruszenia tajności głosowania oraz fałszowania głosów w maszynach do głosowania NEDAP w 2007 roku minister spraw wewnętrznych Anna T.B. Bijleveld-Schouten zapowiedziała zaniechanie głosowania elektronicznego i powrót do głosowania na kartach papierowych, jednocześnie przyznała, że Holandia nie jest gotowa również do głosowania za pośrednictwem Internetu. J. Libbenga, *Dutch pull the plug on e-voting*, „The Register", http://www.theregister.co.uk/2007/10/01/dutch_pull_plug_on_evoting/, 1.10.2007.

[20] Indie wdrażają konsekwentnie elektroniczne głosowanie już od 1982 roku, kiedy przeprowadzono eksperymentalne wybory w stanie Kerala. Elektroniczne głosowanie działa obecnie na ogromną skalę, żadne państwo na świecie nie może się z nim równać. Cyt. za: *E-Voting*… .

[21] Irlandczycy ostatecznie zrezygnowali z elektronicznego głosowania w 2009 roku po poniesieniu ogromnych kosztów wdrażania systemu. Cyt. za: *Electronic voting system to be scrapped*, „RTÉ News", http://www.rte.ie/news/2009/0423/evoting.html, 23.04.2010.

[22] Niemcy zaprzestały prac nad elektronicznym głosowaniem po orzeczeniu Trybunału Konstytucyjnego, że ich wdrożenie wymagałoby zmiany niemieckiej konstytucji. Saper, *Niemiecki Trybunał Konstytucyjny uznał wybory elektroniczne za niezgodne z konstytucją*, Internet Society Poland, http://www.isoc.org.pl/200903/evotingniemcy, 03.03.2009.

[23] Pierwsze udane eksperymenty z e-głosowaniem w lokalach wyborczych przeprowadzili Włosi w 2006 roku. *Hasło: Electronic voting examples*, „Encyklopedia Wikipedia", http://en.wikipedia.org/wiki/Electronic_voting_examples#cite_note-29.

[24] D. Springer, *E-voting, czyli wybory przez Internet*, http://www.egospodarka.pl/11274,E-voting-czyli-wybory-przez-Internet,1,20,2.html, 2005, strony nienumerowane; D. Pszczółkowska, *Cała E-stonia w sieci*, „Gazeta Wyborcza", 13.01.2004.

[25] *Electronic Voting by Country: Indian Voting Machines, Electronic Voting in Canada, Electronic Voting in Estonia, Electronic Voting in Belgium*, Memphis 2010, s. 11.

samorządowym[26]. Po udanym i sprawnie przeprowadzonym teście nowej technologii – internetowych wyborach króla puszczy, w których można było wybierać pomiędzy niedźwiedziem, jeleniem i łosiem Estończycy – jako pierwsi na świecie – głosowali przez Internet w wyborach samorządowych, a także wybierali parlament[27]. W wyborach samorządowych w 2005 roku oddano 496 336 głosów, z czego 9 317 za pośrednictwem Internetu, co stanowiło 1,85 proc. wszystkich głosów[28], nie stwierdzono wówczas żadnych prób ataku na system[29]. Od 26 do 28 lutego 2007 roku obywatele Estonii mogli głosować z użyciem Internetu w wyborach parlamentarnych. Co trzydziesty z nich (3,4 proc., 30 275 osób) skorzystał z tej możliwości wyrażenia swojej woli. Znacznie wyższą frekwencję odnotowano w wyborach samorządowych w 2009 roku; przez Internet głosowało 104 415 wyborców, czyli 9,5 proc. uprawnionych do głosowania[30]; badacze skarżyli się na zbyt małą popularność tego typu głosowania w społeczeństwie[31]. Estoński system wyborczy nosi nazwę EstEVS. Podstawą identyfikacji wyborców jest dowód osobisty wyposażony w kartę chipową. Dowód umożliwia również składanie podpisów elektronicznych[32]. Posiadanie takiej karty jest obecnie w Estonii obowiązkowe; do marca 2007 roku zostało wydanych 1,08 miliona kart (populacja kraju liczy 1,34 miliona). Głosowanie na odległość przez Internet jest dostępne na cztery do sześciu dni przez dniem głosowania. Wyborca może oddać głos w tym czasie dowolną liczbę razy, każdy kolejny wybór znosi poprzedni; może także głosować tradycyjnie – wówczas anulowany zostaje zapis głosowania elektronicznego, nie jest jednak możliwa zmiana lub anulowanie swojego elektronicznego głosu w dniu wyborów[33]. Głos wyborcy jest szyfrowany za pomocą protokołu SSL (*Secure Sockets Layer*)[34]. W estońskich głosowaniach stosowany jest system podwójnej

---

[26] J. Zieliński, *W Estonii wybory przez Internet*, „Winter. Wiadomości Internetowe", http://www.winter.pl/internet/w1020.html, 8.01.2001.

[27] *Electronic Voting by Country*…, s. 11; K. Zuchowicz, *Urna w wersji online*, „Rzeczpospolita", 3.03.2007.

[28] *Electronic Voting by Country*…, s. 12.

[29] T. Mägi, *Practical Security Analysis*…, s. 15.

[30] *Electronic Voting by Country*…, s. 12.

[31] R. Balicki, *E-voting – przyszłość demokracji*, „CBKE e-Biuletyn", http://cbke.prawo.uni.wroc.pl/files/ebiuletyn/E-voting.pdf, 24.09.2007, s. 5.

[32] M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 54–55.

[33] *Electronic Voting by Country*…, s. 12; M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 57; T. Mägi, *Practical Security Analysis*…, s. 20.

[34] Jest to protokół kryptograficzny opracowany przez firmę Netscape służący do bezpiecznej transmisji danych w Internecie, używany na przykład przez zwykłych, indywidual-

koperty gwarantujący tajność głosu. Głos oddany przez wyborcę jest zaszyfrowywany przez aplikację służącą do głosowania (analogią jest umieszczenie listu w nieprzejrzystej kopercie). Następnie, do takiej zaszyfrowanej informacji dołączany jest kod identyfikujący osobę oddającą głos (tak, jakby pierwsza koperta została umieszczona w drugiej z danymi nadawcy). Taka informacja przesyłana jest do centralnego systemu. Obydwie informacje są rozdzielane – dane identyfikujące głosującego służą do odpowiedniego oznaczenia w bazie danych tak, aby głosujący nie mógł głosować ponownie, natomiast jego głos jest liczony. Ponowne połączenie danych nie jest możliwe. Warto dodać, że w sytuacji ataku na infrastrukturę informatyczną Komisja Wyborcza może przerwać głosowanie przez Internet, a także ma prawo do anulowania wyników, ponadto serwer, na którym przechowywane są głosy jest fizycznie odseparowany od sieci publicznej[35].

W Australii wdrożono internetowe wybory na niewielką skalę w 2007 roku, umożliwiając głosowanie członkom australijskich sił zbrojnych oraz personelowi cywilnemu przebywającemu na misjach w Afganistanie, Iraku, Timorze Wschodnim oraz na Wyspach Salomona. Zarejestrowało się 2 012 osób, a 1 511 oddało swoje głosy. Oddane w ten sposób głosy zostały przesłane do Australii, tam wydrukowane i doliczone do ogólnej ich puli[36].

Finlandia rozpoczęła wdrażanie wyborów internetowych na odległość od szczebla samorządowego. Odbyły się one w październiku 2008 roku w trzech jednostkach samorządowych – Karkkila, Kauniainen i Vihti. Oddano 12 234 głosy przez Internet. Ponad połowa biorących udział w głosowaniu (58,06 proc.) skorzystała z możliwości oddania głosu przez Internet. Wybory nie zakończyły się sukcesem, przeprowadzono je ponownie w wymienionych jednostkach ze względu na problemy informatyczne, ponieważ połączenia niektórych wyborców zostały przerwane[37].

---

nych użytkowników w operacjach bankowych online lub podczas wykonywania zakupów w sklepach internetowych. T. Mägi, *Practical Security Analysis…*, s. 29.

35 Tamże, s. 20. Dane pomiędzy serwerem, na który przesyłane są głosy, a serwerem na którym są przechowywane przenoszone są za pomocą fizycznych nośników danych. Patrz także: M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy…*, s. 54–55.

36 Szerzej na ten temat: *Report into Remote Electronic Voting at the 2007 Federal Election for Overseas Australian Defence Force Personnel*, Australian Electoral Commission, http://www.aec.gov.au/pdf/voting/evoting_reports/adf/adf_trial_report.pdf, 18.04.2010, s. 1–125.

37 *Electronic voting experiment in a positive feedback – about 200 votes, however, was interrupted by mistake*, Oikeusministeriö Justitieministeriet, http://www.om.fi/Etusivu/Ajankohtaista/Uutiset/1224166604122, 28.10.2008.

Głosowanie przez Internet we Francji wdrożono w 2003 roku podczas wyborów do Zgromadzenia Narodowego. Możliwość oddania głosu za pośrednictwem Internetu mieli obywatele francuscy przebywający za granicą[38]. Ponad połowa uprawnionych i zarejestrowanych w Stanach Zjednoczonych skorzystała z tej możliwości[39]. We Francji internetowe głosowanie prowadzono także na poziomie lokalnym w ramach ogólnoeuropejskiego projektu CyberVote[40]. CyberVote to projekt Komisji Europejskiej mający na celu przetestowanie efektywności i możliwości użycia w głosowaniu stacjonarnych i mobilnych połączeń przez Internet[41]. System CyberVote wdrażany przez Komisję Europejską od 2000 roku pozwalał na wybory przez przeglądarkę internetową, także z użyciem telefonów i handheldów. Pilotażowe próby prowadzono w Niemczech i Szwecji[42]. W 2004 roku Parlament Europejski podjął decyzję o rozwijaniu elektronicznego głosowania, jednakże została ona zmieniona i skoncentrowano się na głosowaniu korespondencyjnym. Ta decyzja spowodowana została rekomendacjami amerykańskich ekspertów od zabezpieczeń, którzy spowodowali również zamknięcie w Stanach Zjednoczonych systemu o nazwie *Secure Electronic Registration and Voting Experiment* (SERVE)[43]. We Francji CyberVote zorganizował 11 grudnia 2002 roku w mieście Issy-les-Moulineaux wybory do rady dystryktu. W rok później przeprowadzono wiążące wybory z użyciem Internetu w kilku innych francuskich dystryktach[44]. W wyborach 7 czerwca 2009 roku system ten objął rezydentów w Afryce i Ameryce. Około 6 000 (9 proc. głosujących) francuskich obywateli pozostających za granicą oddało swoje głosy za pośrednictwem Internetu[45].

W Holandii pierwszą próbę głosowania internetowego podjęto podczas wyborów do Parlamentu Europejskiego w 2004 roku. Powstał wówczas system wyborczy KOA – *Kiezen op Afstand* co znaczy System Wyborczy na Odległość autorstwa firmy LogicaCMG działający za pośrednictwem

[38] Zgodnie z Artykułem 24 Konstytucji V Republiki Francuskiej z 4 października 1958 roku Francuzi zamieszkali poza Francją są reprezentowani w Senacie.

[39] *Recommendation. What is the Future of Electronic Voting in France?*, http://www.foruminternet.org/telechargement/documents/reco-evote-en-20030926.pdf, 26.09.2003, s. 1–42.

[40] L. Acharya, *Internet Voting*, http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/PRB-e/PRB0306-e.pdf, 1.07.2007, s. 4.

[41] R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 143.

[42] R.K. Gibson, *Internet Voting*…, s. 31.

[43] T. Mägi, *Practical Security Analysis*…, s. 15.

[44] L. Acharya, *Internet*…, s. 4.

[45] *New French experience of e-voting*, Citizens 2.0, http://www.edemocracy-forum.com/2009/07/frencevoting2009.html, 10.07.2009.

Internetu. W wyborach do Parlamentu Europejskiego udostępniono ten system wyborcom aktualnie przebywającym poza krajem (ich liczbę oszacowano na kilkanaście tysięcy). Wybory prowadzone w systemie KOA składają się z dwóch faz: fazy rejestracji i fazy głosowania. W pierwszej fazie wyborca wybiera dla siebie kod PIN (*Personal Identity Number* – Osobisty Numer Identyfikacyjny) i rejestruje się w systemie. Następnie otrzymuje informacje o możliwości wyboru (kandydatów, partii) oraz informacje autoryzacyjne i kod identyfikacyjny. W fazie głosowania wyborca używa kodu PIN oraz kodu otrzymanej uprzednio karty wyborczej, a kandydata wybiera poprzez wpisanie odpowiedniego kodu przypisanego danemu kandydatowi; na koniec potwierdza swój wybór i otrzymuje kod transakcji (sesji), który pozwala mu na zweryfikowanie, czy jego głos został właściwie policzony. Komunikacja przeprowadzana jest za pomocą systemu SSL, uznawanego za bezpieczny. Z zarejestrowanych 16 000 holenderskich emigrantów z systemu internetowego (lub równolegle oferowanej możliwości głosowania przez telefon) skorzystało 5 351 osób. W lipcu 2004 roku kod źródłowy KOA został opublikowany i stał się pierwszym systemem *Open Source*[46].

Japońskie doświadczenia z użyciem Internetu w głosowaniu rozpoczęły się w drugiej połowie lat dziewięćdziesiątych. W 1996 roku w mieście Fujisawa w prefekturze Kanagawa wdrożono pierwsze forum konsultacyjne umożliwiające dialog z władzami (*denshi shimin kaigishitsu – e-citizens' council room*). W trzy lata później przeprowadzono pilotażowy projekt głosowania *online* w Kawaguchi, który objął 360 000 obywateli w 78 obwodach wyborczych[47]. Z kolei w 2001 roku oferowano możliwość głosowania przez Internet w wyborach gubernatora Hiroszimy[48]. Rok później miasto Niimi w prefekturze Okayama przeprowadziło głosowanie *online* w wyborach burmistrza i członków rady miasta[49].

Eksperyment z internetowym głosowaniem przeprowadziła kanadyjska Nowa Partia Demokratyczna (*New Democratic Party*), która skorzystała w tym zakresie z usług firmy election.com, aby w styczniu 2003 roku wybrać swojego lidera. Członkowie partii mogli głosować listownie, przez Internet lub osobiście. Internetowy kanał głosowania padł ofiarą ataku typu odmowy dostępu usługi i w związku z tym eksperyment uznano

[46] M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy…*, s. 79–80; D. Springer, *E-voting…*, strony nienumerowane.

[47] Y. Takao, *Democratic Renewal by 'Digital' Local Government in Japan*, „Pacific Affairs" 2004, nr 77 (2), s. 253.

[48] R.K. Gibson, *Internet Voting…*, s. 33.

[49] Y. Takao, *Democratic Renewal…*, s. 253.

za nieudany[50]. W Nowej Szkocji, w wyborach samorządowych wyborcom również udostępniono możliwość oddawania głosu przez Internet. Otrzymywali oni numer PIN w liście, który mogli odebrać wyłącznie osobiście. W systemie byli identyfikowani za pomocą tego numeru oraz daty urodzenia. Na uwagę zasługuje przyjazny klimat prawny tworzony przez kanadyjskich legislatorów[51].

W Szwajcarii w styczniu 2003 roku odbyło się pierwsze głosowanie w wyborach samorządowych z wykorzystaniem Internetu w kantonie Genewa, a następnie w Zurychu[52]. Pilotaż zakończył się sukcesem, odbył się bez incydentów. Miał on charakter wiążący, 323 osoby zagłosowały przez Internet[53]. Szwajcarzy wynajęli też grupę hakerów „białych kapeluszy"[54], którzy w okresie trzech tygodni próbowali bezskutecznie złamać system (wyborcom udostępniony był przez dwa dni)[55]. W rok później ponownie przeprowadzono wybory w kantonie Genewa. Karty do głosowania wyposażone w chip zostały wysłane wyborcom na kilka tygodni przed rozpoczęciem wyborów. Zawierały one kod zwany kluczem prywatnym wygenerowanym i potwierdzonym przez Infrastrukturę Klucza Publicznego. Karty przeznaczone były wyłącznie do wykorzystania w tym jednym głosowaniu. Obywatele dokonywali wyboru i potwierdzali go kluczem prywatnym oraz wprowadzeniem danych osobowych – daty i miejsca urodzenia. Informacja udzielona przez głosującego była szyfrowana i przesyłana na serwer, zastosowano – podobnie jak w Estonii – system podwójnej koperty[56].

Również Szwecja w ramach projektu CyberVote przeprowadziła próbne wybory w dniach 27–31 stycznia 2003 w dzielnicy Sztokholmu Kista. Był to eksperyment mający na celu sprawdzenie możliwości

---

50 L. Acharya, *Internet*…, s. 4–5.

51 *Electronic Voting by Country*…, s. 6, 8.

52 D. Springer, *E-voting*…, strony nienumerowane; J. Gerlach, U. Gasser, *Three Case Studies from Switzerland: E-Voting*, Internet and Democracy Case Study Series, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Gerlach-Gasser_SwissCases_Evoting.pdf, 1.03.2009, s. 1–17; R. Balicki, *E-voting*…, s. 5.

53 R.M. Alvarez, T.E. Hall, Point, *Click & Vote*…, s. 145.

54 „Białe kapelusze" zwani także „białymi rycerzami" lub sneakers to specjaliści od zabezpieczeń Internetu, sieci i systemów operacyjnych, których działalność skupiona jest na wyszukiwaniu luk w systemach w celu wskazania ich nieświadomym zagrożeń użytkownikom, instytucjom, by mogli podjąć działania naprawcze i ustrzec się przez niebezpieczeństwem. Więcej na ten temat: *What is a White Hat?*, „Secpoint", http://www.secpoint.com/What-is-a-White-Hat.html.

55 R.M. Alvarez, T.E. Hall, Point, *Click & Vote*…, s. 145.

56 T. Mägi, *Practical Security Analysis*…, s. 13–14.

zaimplementowania demokracji deliberatywnej i podejmowania decyzji w populacjach specyficznych – głosować mogli wyłącznie obywatele powyżej 55 roku życia, wielu z nich było imigrantami nieznającymi języka szwedzkiego[57].

W Wielkiej Brytanii przeprowadzono serię prób głosowania elektronicznego w wyborach lokalnych w 2002 i 2003 roku[58]. W maju 2003 roku przeprowadzono aż 59 prób e-głosowania w wyborach lokalnych; siedemnaście z nich był to *I-voting*[59]. W dniach 26 kwietnia–2 maja 2002 roku w ramach wyborów samorządowych w pięciu obwodach wyborczych dwóch w Liverpoolu i trzech w Sheffield eksperymentalnie umożliwiono głosowanie drogą elektroniczną: poprzez Internet, SMS oraz z wykorzystaniem kiosków informacyjnych (infomatów) i kart mikroprocesorowych, służących do identyfikacji wyborców. Był to pierwszy tego rodzaju eksperyment na świecie. Głosowano także w sposób tradycyjny na kartach wyborczych składanych w lokalach wyborczych lub przesyłanych pocztą. Jednakże głosy tradycyjne liczone były elektronicznie, za pomocą specjalnych kodów[60]. Łącznie z możliwości głosowania elektronicznego skorzystało prawie 5000 osób. Popularność głosowania drogą elektroniczną i jego sposób były bardzo zróżnicowane. W okręgu Manor w Sheffield, gdzie udział głosujących był najmniejszy i wyniósł jedynie 17 proc., przeszło połowę głosów elektronicznych oddano za pomocą wiadomości SMS. Z kolei w okręgu Everton w Liverpoolu największą popularnością cieszył się telefoniczny, interaktywny system odpowiedzi głosowych (*Interactive Voice Response,* IVR), za pomocą którego oddano 48 proc. wszystkich głosów elektronicznych. Wyniki wyborów (z głosami elektronicznymi włącznie) były prawnie wiążące. Eksperyment został przygotowany przez British Telecom oraz firmę election.com[61]. Na uwagę zasługują także działania środowiska akademickiego – zespół z De Montford University podjął interdyscyplinarne studia na temat internetowego głosowania,

---

57 L. Acharya, *Internet*…, s. 4; R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 144; *CyberVote: The Trials*, http://www.eucybervote.org/trials.html, 9.02.2006, strony nienumerowane.

58 R.K. Gibson, *Internet Voting*…, s. 32; D. Springer, *E-voting*…, strony nienumerowane; T. Mägi, *Practical Security Analysis*…, s. 15; Z. Zwierzchowski, *Alternatywa dla kartki i urny*, „Rzeczpospolita" 6.08.2001.

59 P. Norris, *E-Voting as the Magic Ballot for European Parliamentary Elections? Evaluating E-voting in the Light of Experiments in UK Local Elections*…, s. 73.

60 B. Czerniejewski, *UK online*, „PC Kurier" 2002, nr 13, http://www.egov.pl/index.php?option=content&task=view&id=71&Itemid=62.

61 Tamże; Z. Zwierzchowski, *Alternatywa*…, strony nienumerowane.

obejmując zakresem analiz przede wszystkim kwestie społeczne (w oparciu o badania ilościowe) oraz problemy techniczne[62].

Pierwsze wybory, podczas których korzystano z głosowania przez Internet, odbyły się w Stanach Zjednoczonych. Partia Republikańska w 2000 roku na Alasce wdrożyła system internetowego głosowania umożliwiający dokonanie wyboru kandydatów w prawyborach. Ten sposób wyboru kandydata nie spotkał się jednak z szerokim odzewem elektoratu – spośród 3500 osób, którym umożliwiono oddanie głosu za pośrednictwem Internetu, zagłosowało w ten sposób zaledwie 35 osób, a więc mniej niż jeden procent uprawnionych[63]. Kolejny eksperyment przeprowadzono w stanie Arizona w marcu 2000 roku[64]. Ponad 800 000 wyborców stanu umożliwiono wybór kandydata z Partii Demokratycznej za pośrednictwem strony internetowej[65]. Wybory te nie miały charakteru wiążącego[66], ponadto odbyły się za późno, gdy w szesnastu stanach wybory kandydatów już zakończono. W wyborach tych można było oddawać głosy nie tylko przez Internet, ale też poprzez komputery umieszczone w miejscach publicznych[67]. Każdy spośród 843 323 zarejestrowanych wyborców otrzymał numer PIN w tradycyjnym liście. Numer ten służył nie tylko potwierdzeniu tożsamości głosującego, ale połączony był z bazą wyborców, co miało zapobiegać powtórnemu oddaniu głosu[68]. Głosujący przez Internet ściągał i uruchamiał na swoim komputerze kontrolkę ActiveX, stanowiącą aplikację wyborczą osadzoną na stronie internetowej[69]. Z listy kandydatów wskazywał preferowanego, a następnie proszony był o potwierdzenie swojego wyboru[70]. Po oddaniu głosu nie można było głosować w lokalu wyborczym. Możliwość głosowania była dostępna zarówno przed, jak i w trakcie wyborów; można było głosować nawet na 30 dni przed wyborami[71]. Spośród wszystkich biorących udział w prawyborach, 41,6 proc. oddało swój głos przez Internet, 37,7 proc. za

---

62 R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 145.

63 R.K. Gibson, *Internet Voting*…, s. 31.

64 R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 124. Więcej na temat tego eksperymentu: A. Elberse, M.L. Halle, W.H. Dutton, *Guiding Voters through the Net: the Democracy Network in a California Primary Election*, [w:] K.L. Hacker, J. Dijk van (ed.), *Digital Democracy*, Londyn, Thousand Oaks, New Delhi 2000, s. 130–148.

65 Z. Zwierzchowski, *Alternatywa*…, strony nienumerowane.

66 R.K. Gibson, *Internet Voting*…, s. 31.

67 K. Coleman, *Internet Voting*…, strony nienumerowane.

68 R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 128.

69 M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 56.

70 R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 128.

71 T. Mägi, *Practical Security Analysis*…, s. 29.

pomocą tradycyjnej poczty, 4,8 proc. skorzystało z komputerów w miejscu publicznych, a 16,4 proc. pozostało przy tradycyjnym, papierowym głosie. Największe problemy wyborcom korzystającym z Internetu sprawił sposób użycia certyfikatu (34 proc. zgłoszeń na infolinii dotyczyło tego problemu), trudności w dostępie do strony internetowej, na której odbywało się głosowanie (25 proc.) oraz sposób instalacji przeglądarki internetowej Netscape (24 proc.)[72]. W tym samym roku w wyborach powszechnych uruchomiono projekt *Voting Over Internet* (VOI) w czterech stanach: Floryda, Karolina Południowa, Teksas i Utah, jednak wyniki były niezadowalające – liczba oddanych głosów wyniosła zaledwie 84. Projekt ten został zawieszony w tym samym roku ze względu na defekty techniczne wykazane w raporcie bezpieczeństwa opublikowanym przez Davida Jeffersona, Aviela D. Rubina, Barbarę Simons, Davida Wagnera[73]. Amerykańskie systemy głosowania zostały określone jako podatne na ataki, niezdolne do zapewnienia tajności głosów i poprawności wyników wyborów[74]. Od stycznia 2004 roku próbowano wdrażać system SERVE. Projekt ten skierowany był do personelu wojskowego pozostającego poza granicami Stanów Zjednoczonych. Grupa docelowa stanowiła sześć milionów wyborców. Projekt został przerwany ze względów bezpieczeństwa, ogłoszony raport w tej sprawie przedstawiał system jako niezdolny do działania[75]. System SERVE przekazywał głosy za pomocą protokołu SSL, jednak były one magazynowane na serwerze podłączonym do sieci publicznej[76]. Ostatecznie zaprzestano udostępniania personelowi militarnemu tego sposobu głosowania[77].

W Niemczech prowadzono równolegle prace nad głosowaniem elektronicznym w lokalach wyborczych i w Internecie od 2003 roku[78]. Pierwszy eksperyment z internetowym głosowaniem przeprowadzono w dniach od 13 do 15 stycznia 2003 roku na uniwersytecie w Bremie podczas

---

72 R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 129, 141.

73 M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 70–71; D. Jefferson, A.D. Rubin, B. Simons, D. Wagner, *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*, http://www.servesecurityreport.org/paper.pdf, 21.01.2004, s. 1–34.

74 D. Jefferson, A.D. Rubin, B. Simons, D. Wagner, *A Security Analysis*…, s. 1–34; T. Mägi, *Practical Security Analysis*…, s. 14.

75 T. Mägi, *Practical Security Analysis*…, s. 9.

76 Tamże, s. 29; D. Springer, *E-voting*…, strony nienumerowane.

77 R. Maze, *No Internet voting for military this year*, „Navy Times", http://www.navytimes.com/news/2008/04/military_absenteeballot_voting_041508w/, 16.04.2008.

78 Z. Zwierzchowski, *Alternatywa*…, strony nienumerowane.

wyborów uniwersyteckich[79]. Minister Spraw Wewnętrznych Otto Schily zapowiadał pierwsze próby zastosowania Internetu w procesie głosowania w wyborach lokalnych w 2006 roku oraz wdrożenie ich na szeroką skalę w wyborach parlamentarnych w 2010 roku[80]. Z prac nad elektronicznymi systemami głosowania zrezygnowano po orzeczeniu Niemieckiego Trybunału Konstytucyjnego wydanym 3 marca 2009 roku stwierdzającym niezgodność takiego sposobu wyrażania woli wyborców z konstytucją[81].

W Polsce jak dotąd nie zastosowano w wyborach lokalnych lub powszechnych głosowania przez Internet na odległość, aczkolwiek jest ono przedmiotem dyskusji publicystów, naukowców i decydentów. Na uwagę zasługują projekty zmian w prawie wyborczym oraz korzystny grunt prawny dla rozwoju elektronicznego głosowania. Podkreśla się, że z punktu widzenia Konstytucji nie ma przeszkód dla wprowadzenia elektronicznego głosowania, w tym głosowania przez Internet, a zatem konieczne prace legislacyjne dotyczyłyby ustaw zwykłych[82]. Pomysły modyfikacji polskiego prawa wyborczego w kontekście wyborów przez Internet pojawiły się po raz pierwszy w 2003 roku przed wyborami do Parlamentu Europejskiego VI kadencji[83]. Rzecznik Praw Obywatelskich V kadencji Janusz B. Kochanowski apelował o wprowadzenie przepisów umożliwiających osobom niepełnosprawnym głosowanie w wyborach między innymi za pośrednictwem Internetu[84]. Podkreśla się, że nieuregulowany stan prawny związany z systemem podpisu elektronicznego nie byłby przeszkodą dla wdrożenia głosowania za pomocą Internetu. Planuje się obecnie modyfikacje istniejących ordynacji wyborczych dla umożliwienia internetowej rejestracji wyborców poprzez umożliwienie im składania pocztą elektroniczną wniosków o dopisanie do spisu wyborców poza miejscem zamieszkania oraz wniosków o wydanie zaświadczenia, że wyborca jest uprawniony do głosowania[85]. Na życzliwą uwagę zasługuje inicjatywa studencka Polska Młodych proponująca wprowadzenie

---

79 L. Acharya, *Internet*…, s. 4; R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 144; Z. Zwierzchowski, *Alternatywa*…, strony nienumerowane.

80 R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 144–145; R.K. Gibson, *Internet Voting*…, s. 32.

81 M. Chmielewski, *Wybory elektroniczne dla Niemców niezgodne z konstytucją*, „Chip Online", http://www.chip.pl/news/wydarzenia/prawo-i-polityka/2009/03/wybory-elektroniczne-dla-niemcow-niezgodne-z-konstytucja, 4.03.2009.

82 A. Stankiewicz, *E-wybory, czyli głosowanie przez Internet*, „Rzeczpospolita" 28.10.2005.

83 Tenże, *Urny szeroko otwarte*, „Rzeczpospolita" 3.01.2003.

84 DF, *Internet zamiast urny*, „Rzeczpospolita" 6.01.2007.

85 K. Manys, *Jak przyciągnąć ponad połowę Polaków do urn*, „Rzeczpospolita" 21.03.2008.

głosowania przez Internet i prowadząca akcję zbierania podpisów pod takim wnioskiem[86]. Organizacja ta dzięki Stypendium Lesława Pagi opracowała i zaprezentowała przy udziale polskiego eksperta w tej dziedzinie – Mirosława Kutyłowskiego w czerwcu 2009 roku prototyp systemu umożliwiający bezpieczne głosowanie przez Internet[87]. Przeprowadzono również próby usprawnienia procesu głosowania za pomocą Internetu. Lokalna próba wdrożenia internetowych konsultacji odbyła się w Warszawie w latach 2000 i 2002. Pierwsza z nich poddana została ostrej krytyce ze względu na to, że nie zabezpieczono się przed wielokrotnym przesyłaniem treści z tego samego adresu. Po zakończonych konsultacjach skonstatowano, że trzy czwarte głosów sprzeciwu pochodzi z jednego komputera. Ponadto zarejestrowano nadaktywność gminy Białołęka. W lutym 2002 roku umożliwiono internautom komentowanie projektu ustroju miasta stołecznego Warszawy. Blisko pół tysiąca propozycji zmian w projekcie (448 zgłoszeń, to jest 84,5 proc. wszystkich przesłanych) zostało skierowanych do Ratusza za pomocą Internetu[88]. Trwają ponadto w Polsce prace nad wdrożeniem elektronicznego głosowania w lokalach wyborczych. Dotychczas mają one charakter próbny, nie stosowano ich na większą skalę. Podczas wyborów w 2005 roku w dwóch lokalach wyborczych w Warszawie oraz Sopocie, w których oddawali swe głosy Lech Kaczyński i Donald Tusk zaprezentowano z inicjatywy Polskiej Grupy Badawczej komputery wyborcze iPOS firm Wincor Nixdorf oraz Suport[89]. Z kolei Urząd Miasta Częstochowy poddał pod głosowanie elektroniczne wyłączenie z ruchu kołowego jednej z głównych ulic miasta. Inny polski eksperyment dotyczący wdrażania systemów głosowania elektronicznego miał miejsce w Głuchołazach w dniach 24–25 maja 2003 roku. W trakcie odbywającego się tam prareferendum europejskiego w jednym z obwodów umożliwiono wyborcom głosowanie za pomocą głosomatów, wyposażonych w ekrany dotykowe. Skorzystało z nich aż 80 proc. wyborców (w czterech lokalach wyborczych, w których pilotaż się odbywał)[90]. Warto również wspomnieć o inicjatywie usprawniania procesu wyborów w postaci systemu *Platforma Wyborcza* zaprojektowanego i wdrożonego przez firmę Pixel Technology (we współpracy z firmami Mikrobit i eo

86 DF, *Internet*… .

87 *E-głosowanie*, http://www.e-glosowanie.org/.

88 M. Nowina-Konopka, *Rola Internetu w rozwoju demokracji w Polsce*, Kraków–Nowy Sącz 2008, s. 239.

89 A. Maciejewski, *Warszawa i Sopot głosowały elektronicznie*, http://www.computerworld.pl/news/84427.html, 24.10.2005.

90 M. Nowina-Konopka, *Elektroniczna*…, s. 13, 15.

networks, które zapewniały wizualizację wyborów do Sejmu i Senatu w 2007 roku oraz w wyborach samorządowych w 2006 roku) na zlecenie Krajowego Biura Wyborczego. System ten zastosowano w wyborach do Parlamentu Europejskiego w 2004 i 2009 roku, w wyborach do Sejmu i Senatu w 2005 i 2007 roku, w wyborach na urząd Prezydenta w 2005 i w 2010 roku oraz w wyborach samorządowych w 2002 i 2006 roku. Jego funkcje obejmują: przygotowanie i przeprowadzenia zadań umożliwiających sprawne i poprawne ustalenie wyników głosowania, wyników wyborów i referendów; wykonywanie ustawowo określonych zadań dotyczących nadzoru nad organami niższego szczebla; sprawowanie nadzoru nad przestrzeganiem prawa wyborczego oraz sprawowanie nadzoru nad prowadzeniem rejestru wyborców. Oprogramowanie to działa w ponad 20 000 lokalizacji i jest dostosowane do obsługi wyborów wszystkich rodzajów. System ten zapewnia obsługę organów wyborczych w zakresie rejestracji, przetwarzania i udostępniania danych, zawiera między innymi bazę geografii wyborczej, bazy podmiotów uczestniczących w wyborach, w tym rejestry wyborców oraz wyniki poszczególnych wyborów[91]. W wyborach samorządowych w 2002 roku system ten zawiódł w zakresie zliczania głosów; przedstawiciele firmy zrezygnowali z części wynagrodzenia[92].

Porównanie zaawansowania technologicznego demokracji w różnych krajach dokonywane jest na podstawie indeksu partycypacji opracowanego przez Organizację Narodów Zjednoczonych. Może on przyjmować wartości od zera do jedności, gdzie 0 oznacza najniższą wartość, a 1 najwyższą. Indeks ten ocenia jakość oraz użyteczność informacji i usług dostarczanych przez rząd danego kraju w celu zaangażowania obywateli w politykę. Ocenie podlegają następujące trzy wymiary: a/ dostarczanie obywatelom przez Internet informacji dotyczących polityki, a koniecznych do samodzielnego podejmowania przez nich decyzji (*e-information*), b/ rozwijanie internetowych konsultacji (*e-consultation*), c/ popieranie rozwoju systemu internetowego służącego do podejmowania decyzji politycznych przez obywateli w tym różnych form głosowania elektronicznego (*e-decision*)[93]. Wartość indeksu e-partycypacji wzrosła w ciągu ostatniego pięciolecia (2005–2010). W 2005 roku średnia dla 192 krajów świata wynosiła 0,152, a w 2010 wyniosła już 0,190. Polska na tle innych krajów świata lokuje się na 52 miejscu pomiędzy Białorusią i Kenią. Polska w 2010 roku osiągnęła

[91] Opis systemu można znaleźć na stronie domowej Pixel Technology: http://www.pixel.com.pl/strony/index.php/aktualnosci.html.

[92] R. Balicki, *E-voting*…, s. 3.

[93] *United Nations e-Government Knowledge Base*, http://www2.unpan.org/egovkb/egovernment_overview/eparticipation.htm.

indeks e-partycypacji w wysokości 0,242. W 2005 roku indeks ten był wyższy i wynosił 0,349, lokując Polskę na 29 miejscu wśród krajów świata. W Europie pierwsze trzy miejsca należą do Hiszpanii, Wielkiej Brytanii oraz Estonii z indeksami odpowiednio: 0,827, 0,771 i 0,659. Spośród 43 badanych państw europejskich Polska znalazła się na 25 miejscu[94].

Możliwości rozwoju głosowania przez Internet

W literaturze przedmiotu spotkać można zarówno pozytywne, jak też negatywne oceny głosowania za pośrednictwem Internetu[95]. W zasadzie brak jest pogłębionej, szerokiej i systematycznej analizy skutków politycznych, społecznych i ekonomicznych wdrożenia takich rozwiązań.

Zwiększenie frekwencji wyborczej stanowi główny, najczęściej przytaczany argument zwolenników głosowania przez Internet[96]. Fakt obniżania się frekwencji wyborczej w stabilnych demokracjach jest przedmiotem sporów uczonych. Część badaczy (powołujących się wyłącznie na statystyki frekwencji wyborczej) sugeruje, że mamy do czynienia z kryzysem demokracji, inni natomiast argumentują, że – mimo spadku udziału w głosowaniach – wzrasta natężenie innych, pozawyborczych form partycypacji politycznej, a społeczeństwo niezmiennie pozostaje aktywne politycznie[97]. Badacze zgadzają się jednak na ogół co do tego, że uczestnictwo wyborcze stanowi kluczowy element legitymizacji władzy w demokracjach i jego brak lub niskie natężenie mogą w efekcie doprowadzić do poważnych problemów politycznych i społecznych[98]. Parlament Europejski postrzega elektroniczne głosowanie jako jeden ze sposobów likwidacji lub zmniejszenia zjawiska deficytu demokracji w politycznych strukturach europejskich[99].

---

94 Opracowanie własne na podstawie baz danych: *United Nations e-Government…* .

95 Szerzej na ten temat: D.A. Henningfeld (ed.), *Should the United States Move to Electronic Voting?*, Detroit 2008.

96 J. Corrales, *Lessons from Latin America*, [w:] L.D. Simon, J. Corrales, D.R. Wolfensberger (ed.), *Democracy and the Internet. Allies or Adversaries?*, Waszyngton 2002, s. 34.

97 Omówienie przeciwstawnych stanowisk można znaleźć między innymi w: R.G. Niemi, H.F. Weisberg, *Why Is Voter Turnout Low (and Why Is It Declining)?,* [w:] R.G. Niemi, H.F. Weisberg (ed.), *Controversies in Voting Behavior*, Waszyngton 2001, s. 30–31.

98 Patrz na przykład: P. Norris, *Democratic Phoenix: Reinventing Political Activism*, Cambridge 2002, s. 5 oraz G.B. Powell, Contemporary Democracies: Participation, Stability, and Violence, Cambridge 1982, s. 206.

99 F. Mendez, A.H. Trechsel, *The European Union and E-voting: Upgrading Euro-elections*, [w:] A.H. Trechsel, F. Mendez (ed.), *The European Union and E-voting…*, s. 6. Pojęcie deficytu demokracji zostało po raz pierwszy sformułowane w 1979 roku przez Davida Marquanda w: D. Marquand, *Parliament for Europe*, Londyn 1979.

Dostrzegane są szanse na zwiększenie zaangażowania w proces wyborczy takich grup społecznych jak młodzież, niepełnosprawni, przewlekle chorzy i pozostający w domach z innych powodów, przebywający poza granicami kraju i inni niemogący lub niechcący uczestniczyć w głosowaniu. Wejście w wiek wyborczy kategorii wiekowej (obecnie w wieku 18–25 lat) nazywanej Cyfrową Generacją (*Digital Generation*), której istotnym elementem socjalizacji w ramach nauki, zabawy i pracy były komputery osobiste oraz Internet budzi szczególne nadzieje badaczy na zwiększenie frekwencji wyborczej[100]. Paweł Kubicki wskazuje, że możliwość zwiększenia frekwencji ludzi młodych należy rozpatrywać w kontekście szeregu zmian socjodemograficznych jakie zaszły w ostatnich latach w Polsce, a w ostatnich dziesięcioleciach w demokracjach zachodnioeuropejskich. Uważa on, że przyczyną niezadowalającego poziomu uczestnictwa w wyborach młodzieży jest jej hipermobilność w zglobalizowanych społeczeństwach – migracje wewnętrzne i zewnętrzne. Istotną podgrupą, do której winna być adresowana możliwość głosowania z użyciem Internetu są studenci; na przykład w Polsce studiuje obecnie około dwóch milionów osób przy czym ponad dwie trzecie z nich poza miejscem zamieszkania. Dojazdy do miejsca zamieszkania są kosztochłonne, czasochłonne i niekiedy niemożliwe, co negatywnie wpływa na frekwencję wyborczą. Kolejna grupa to osoby przyjeżdżające w celach zarobkowych do dużych aglomeracji miejskich – Warszawy, Krakowa, Trójmiasta, Poznania i Wrocławia. Ze względu na zbyt wysokie ceny mieszkań niewielu z nich jest w stanie nabyć własne lokum i uzyskać stały meldunek, który pozwoliłby im głosować w miejscu zamieszkania i pracy. Głosowanie elektroniczne mogłoby przyciągnąć również przebywających czasowo na emigracji zarobkowej (migracja wahadłowa). Lokale wyborcze w ambasadach i konsulatach często są nieosiągalne dla pracujących na prowincji[101]. Takie głosowanie zwiększyłoby też frekwencję personelu zagranicznego oraz podróżujących w interesach, a także przebywających na wakacjach[102]. Wskazuje się również na niepełnosprawnych, przewlekle chorych, w podeszłym wieku i innych pozostających w domach jako beneficjentów internetowego głosowania. Powszechność i równość głosowania w przypadku tych

[100] Patrz na przykład: K. Montgomery, B. Gottlieb-Robles, G.O. Larson, *Youth as E-Citizens: Engaging the Digital Generation*, Center for Social Media, http://dspace.wrlc.org/bitstream/1961/4649/1/youthreport.pdf, 03.2004; A.M. Oostveen, P. Besselaar van den, *Internet Voting*…, s. 62.

[101] P. Kubicki, *Skutki społeczne wprowadzenia e-głosowania w Polsce*, http://www.e-glosowanie.org/images/pdf/analiza_socjologiczna.pdf, strony nienumerowane.

[102] A.M. Oostveen, P. Besselaar van den, *Internet Voting*…, s. 64.

kategorii osób jest we współczesnych demokracjach silnie naruszona[103]. Ułatwienie im głosowania za pośrednictwem Internetu jest istotną szansą na przełamanie barier uczestnictwa w życiu publicznym[104]. Głosowanie internetowe mogłoby przyciągnąć także kategorię niegłosujących (*non-voters*), którzy nie uczestniczą w wyborach z powodu braku wygody w głosowaniu, na przykład konieczności dojazdu do lokalu wyborczego[105]. Hipotezę o prawdopodobnym wzroście frekwencji wyborczej wymienionych grup opiera się na ogół na twierdzeniu, że oczekują one przede wszystkim zwiększenia wygody i dostępności głosowania i jest to jedyna bariera braku ich uczestnictwa[106]. Przypuszczenie to potwierdzają nieliczne badania jakościowe[107]. Eksperymenty z internetowym głosowaniem wydają się także potwierdzać te domniemania, choć niejednoznacznie. Na przykład zaobserwowano istotny wzrost frekwencji wyborczej podczas Arizona Democratic Primary w 2000 roku, lecz było to nie tylko konsekwencją wyłącznie internetowych wyborów; zmienił się elektorat (doszły nowe roczniki), a ponadto Partia Demokratyczna zwiększyła też swoją aktywność i zmieniła wzorce prowadzenia kampanii wyborczej[108]. W Szwajcarii, gdzie wyborcy od kilku lat mogą przesłać swój głos listem poleconym lub przez Internet, frekwencja wzrosła o blisko 20 procent[109]. Wyniki wyborów eksperymentalnych w Wielkiej Brytanii w 2003 roku pokazują, że w okręgach, gdzie umożliwiono głosowanie przez Internet frekwencja wyborcza była wyraźnie niższa niż w okręgach, gdzie takiego rozwiązania nie wprowadzono[110]. W Estonii w 2005 i 2007 roku nie stwierdzono wzrostu frekwencji, była ona porównywalna z poprzednimi wyborami[111]. Warto także podkreślić, że reformy wyborcze we współ-

---

[103] M. Nowina-Konopka, *Elektroniczna…*, s. 4.

[104] P. Gomułkiewicz, *Wirtualne…*; P. Kubicki, *Skutki społeczne…*, strony nienumerowane; A.M. Oostveen, P. Besselaar van den, *Internet Voting…*, s. 64.

[105] Około miliona wyborców amerykańskich nie głosowało (2,8 proc.) ze względu na niedogodności takie jak długie kolejki czy niekorzystne godziny głosowania. Patrz: *A Report on the Feasibility…*, s. 42; A.M. Oostveen, P. Besselaar van den, *Internet Voting…*, s. 64.

[106] R.K. Gibson, *Internet Voting…*, s. 36; A.M. Oostveen, P. Besselaar van den, *Internet Voting…*, s. 70.

[107] L. Acharya, *Internet…*, s. 2.

[108] R.K. Gibson, *Internet Voting…*, s. 36–37.

[109] J. Bielecki, *Boją się wyborców*, „Rzeczpospolita" 26.10.2005.

[110] P. Norris, *E-Voting…*, s. 82.

[111] M. Abraham, U. Gatterbauer i in., *Remote Electronic Voting. Example Austria: General Set-Up and Political and Legal Dimensions*, http://staatswissenschaft.univie.ac.at/fileadmin/user_upload/inst_staatswissenschaften/Frisch/21063courseWebsite/remotevoting-gatterbauer-etal.pdf, 20.01.2009, s. 6.

czesnych demokracjach na ogół nie przynosiły skutków w postaci zwiększenia partycypacji wyborczej, na przykład wprowadzenie głosowania pocztowego czy ułatwienie i uproszczenie procedur rejestracji wyborców pozostały bez znaczącego wpływu[112]. Włączenie wymienionych grup wiązałoby się z realizacją powszechności i równości wyborów stanowiących elementarną zasadę demokracji[113].

Użycie programu komputerowego w procesie wyborczym uniemożliwia pomyłki obywateli podczas głosowania oraz oddanie głosu nieważnego (między innymi pozwala uniknąć zjawiska *over-votingu*, to jest oddania głosu na kandydata spoza listy)[114]. Jak poważna jest utrata głosów z przyczyn proceduralnych, pokazują dane zebrane w raporcie *US Census Bureau*. W wyborach prezydenckich w 2000 roku w Stanach Zjednoczonych zaginęło od czterech do sześciu milionów głosów ze stu milionów oddanych: od półtora do dwóch milionów zginęło ze względu na wadliwy sprzęt do głosowania, półtora do trzech milionów ze względu na defektywne systemy rejestrowania wyborców, jeden milion ze względu na błędy popełnione w komisjach wyborczych. Podkreśla się także istotny efekt edukacyjny tego rodzaju głosowania. Strona internetowa, na której oddaje się głos może zawierać materiały pozwalające wyborcy lepiej zapoznać się z ofertą polityczną, a nawet nawiązać dyskusję z kandydatem, jego zwolennikami i przeciwnikami[115]; tego rodzaju działania uznaje się za potencjalny czynnik silnie wzmacniający demokrację[116].

Zwolennicy wyborów przy użyciu Internetu podkreślają możliwość znacznej redukcji kosztów związanych z obsługą wyborów[117]. Struktura kosztów tradycyjnego głosowania przedstawia się następująco: jedną trzecią pochłaniają wydatki na rejestrację, jedną trzecią operacje biura wyborczego oraz jedną trzecią stanowią koszty obsługi głosowania w lokalach wyborczych. Głosowanie za pośrednictwem Internetu pozwala zmniej-

---

112 A.M. Oostveen, P. Besselaar van den, *Internet Voting*…, s. 65.

113 R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 35.

114 R.K. Gibson, *Internet Voting*…, s. 36–37.

115 *A Report on the Feasibility*…, s. 39; A.M. Oostveen, P. Besselaar van den, *Internet Voting*…, s. 71.

116 N. Frangakis, *Digital Democracy and Threats to Privacy*, http://26konferencja.giodo.gov.pl/data/resources/FrangakisN.pdf, 14–16.09.2004, s. 2; M. Margolis, D. Resnick, *Politics as Usual. The Cyberspace 'Revolution'*, Thousand Oaks, Londyn, New Delhi 2000, s. 212.

117 M. Abraham, U. Gatterbauer i in., *Remote Electronic Voting*…, s. 7; R.K. Gibson, *Internet Voting*…, s. 36; P. Norris, *E-Voting*…, s. 63; A.M. Oostveen, P. Besselaar van den, *Internet Voting*…, s. 61; G. Schryen, *E-Democracy: Internet Voting*, http://www-users.rwth-aachen.de/guido.schryen/publications/Schryen%20-%20E-Democracy%20Internet%20Voting%20-%20IADIS.pdf, 2003, strony nienumerowane.

szyć istotnie (po wcześniejszej inwestycji) koszt pierwszego i drugiego czynnika a wyeliminować trzeci[118]. Kalkulacje nakładów pieniężnych nie są jednak całkowicie jednoznaczne. W Stanach Zjednoczonych koszt jednego głosu oddawanego metodą tradycyjną oszacowano na kwotę od trzech do siedmiu dolarów, natomiast głos oddany elektronicznie to wydatek rzędu dziesięciu centów[119]. Inne kalkulacje wydatków mówią o mniejszej różnicy – koszt głosu oddawanego metodą tradycyjną określa się na dziesięć dolarów amerykańskich, a oddawanego przez Internet – na dwa dolary[120]. Z kolei koszt jednego głosu oddanego przez Internet w Australii w wyborach 2007 roku wyniósł od 521 do 1159 (w zależności od rodzaju kalkulacji kosztów) dolarów australijskich[121]. Z kolei Bohdan Szczęśniak, zastępca kierownika Krajowego Biura Wyborczego, ocenia, że jednorazowy rachunek uruchomienia bezpiecznego internetowego systemu wyborczego wyniósłby w Polsce 25 milionów złotych[122]. Istnieją też możliwości zmniejszenia kosztów wyborów. Wprowadzenie głosowania przez Internet nie wymagałoby kosztownych w skali państwach inwestycji infrastrukturalnych[123], a także stwarza szanse zwiększenia efektywności działania aparatu administracyjnego oraz uproszczenia procedur głosowania[124]. Zmniejsza się również ryzyko potencjalnych nadużyć; problem ten w zasadzie nigdy nie został rozwiązany w wyborach przeprowadzanych tradycyjnie[125].

Bariery rozwoju głosowania przez Internet

Wdrożenie głosowania internetowego jest przez wielu ekspertów uznawane za niemożliwe z przyczyn technicznych[126]. Bariery techniczne wskazuje się jako podstawową przyczynę powolnego wdrażania głosowania za pośrednictwem Internetu. Głosowanie przez Internet nie zapewnia

[118] *A Report on the Feasibility…*, s. 42.
[119] M. Usidus, *Czyj jest e-lektorat*, „Rzeczpospolita" 7.12.2000.
[120] *A Report on the Feasibility…*, s. 42.
[121] *Report into Remote Electronic Voting at the 2007…*, s. 22.
[122] J. Bielecki, *Boją się…* .
[123] R.M. Alvarez, T.E. Hall, *Point, Click & Vote…*, s. 31.
[124] T. Mägi, *Practical Security Analysis…*, s. 13.
[125] D. Springer, *E-voting…*, strony nienumerowane.
[126] Patrz na przykład: *Stanowisko Stowarzyszenia Internet Society Poland w sprawie głosowania elektronicznego w wyborach powszechnych przyjęte przez Zarząd Stowarzyszenia*, Uchwała Zarządu ISOC Polska nr 2/2007, http://www.isoc.org.pl/200701/wybory, 10.01.2007.

wystarczającego bezpieczeństwa przesyłania i magazynowania głosów[127]. Zgodnie z uznanymi międzynarodowymi standardami demokratycznymi głosowanie elektroniczne może być stosowane jedynie wówczas, gdy jest ono bezpieczne i niezawodne, w szczególności musi się odbywać z zachowaniem tajności głosowania[128]. Liczni eksperci są przekonani, że ze względu na techniczną strukturę Internetu jest to obecnie niemożliwe, uznając problem tajności głosowania za podstawową barierę niepozwalającą na wdrożenie wyborów przez Internet[129]; dyskusja na ten temat przyjmuje głównie wymiar techniczny[130]. Tajności głosowania nie zapewnia na przykład infrastruktura wdrożona w Estonii[131], aczkolwiek analitycy podkreślają, że złamanie anonimowości na dużą skalę byłoby w tym systemie nieopłacalne ze względu na koszty. Z kolei amerykański system SERVE umożliwiał złamanie tajności głosowania na dużą skalę[132].

Tajność głosowania jest pojęciem wieloaspektowym – oznacza ona tajność wobec komisji wyborczych, tajność wobec sprzętu używanego przez wyborcę do złożenia głosu oraz tajność wobec osób trzecich, szczególnie tych, którzy mogliby posunąć się do próby kupna głosów lub wymuszenia określonego sposobu głosowania[133]. W kulturze Internetu rozwinęły się zaawansowane sposoby służące do zdobywania informacji o użytkownikach bez ich wiedzy i zgody. Wciąż doskonalone są i powstają nowe, liczne programy określane mianem *spyware*[134] lub programów naru-

---

[127] L. Acharya, *Internet*…, s. 5; Por.: A.D. Rubin, *Brave New Ballot. The Battle to Safeguard Democracy in the Age of Electronic Voting*, Nowy Jork 2006.

[128] *Code of Good Practice in Electoral Matters. Guidelines and Explanatory Report*, European Commission For Democracy Through Law (Venice Commission), Kodeks przyjęty na posiedzeniu Komisji Weneckiej podczas 51. i 52. sesji w Strasburgu, http://www.venice.coe.int/docs/2002/CDL-AD(2002)023rev-e.pdf, 2002, s. 8, *22*.

[129] R.K. Gibson, *Internet Voting*…, s. 38; R. Krimmer, s. Triessnig, M. Volkamer, *The Development of Remote E-Voting around the World: A Review of Roads and Directions*, http://www.e-voting.cc/static/evoting/files/VOTE-ID-2007.pdf, 2007, s. 9; G. Schryen, *E-Democracy: Internet Voting*, http://www-users.rwth-aachen.de/guido.schryen/publications/Schryen%20-%20E-Democracy%20Internet%20Voting%20-%20IADIS.pdf, 02.2003.

[130] D. Chaum, *Secret-Ballot Receipts: True Voter-Verifiable Elections*, „IEEE Security and Privacy", http://www.computer.org/portal/web/csdl/doi/10.1109/MSECP.2004.1264852, 2004, s. 38–47.

[131] *Porównanie procedur wyborczych*, „Computerworld", http://www.computerworld.pl/artykuly/50398/Porownanie.procedur.wyborczych.html, 02.01.2006.

[132] M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 63.

[133] Tamże, s. 5.

[134] Jest to zbitek słów *spy* – szpieg i *software* – oprogramowanie.

szających prywatność (*privacy-invasive software*)[135]. Ich rozpowszechnienie i trudności w opanowaniu doprowadziło do powstania w 2005 roku Anti-Spyware Coalition zrzeszającej kilkadziesiąt podmiotów takich jak na przykład AOL, Dell, Google, HP, McAfee, Microsoft, Panda Software, Sophos, Symantec oraz Yahoo![136], a także przeciwdziałania rządu amerykańskiego przez penalizację działań związanych z wykorzystywaniem tego typu oprogramowania w *Internet Spyware Prevention Act*[137]. Powstały również liczne komercyjne i niekomercyjne narzędzia służące do zwalczania *spyware*'u. Programy typu *spyware* mogą z powodzeniem posłużyć do złamania zasady tajności głosowania. Zwykli użytkownicy Internetu na ogół nie są w stanie uniknąć niebezpieczeństwa zainfekowania swojej maszyny takim programem. Innym przykładem możliwości złamania tajności głosowania jest technika nazywana w literaturze przedmiotu *man in the middle*. Polega ona na podsłuchu i modyfikacji wiadomości przesyłanych między dwiema stronami bez ich wiedzy. Amerykański system SERVE okazał się wyjątkowo wrażliwy na tego rodzaju ataki[138]. Obecnie trwają intensywne prace kryptografów w celu usunięcia problemu zagrożeń tajności głosowania; zaproponowano rozwiązanie techniczne zwane wyborami weryfikowalnymi (E2E, *end-to-end*) zapewniające tajność głosowania, możliwość sprawdzenia przez głosującego, czy jego głos został dodany do puli głosów, czy nie został on zmodyfikowany (a jeśli tak to zapewniona jest możliwość udowodnienia manipulacji). Wadą tego rozwiązania jest wysoki stopień złożoności systemu, mogący przeciętnemu wyborcy sprawić kłopoty ze zrozumieniem jego istoty. Dotychczas opracowano następujące modele wyborów weryfikowalnych: schemat *Threeballot* Ronalda Rivesta, *Punchscan* Davida Chauma w 2005 roku, *Prêt à Voter* Davida Chauma, Petera Ryana i Steve Schneidera w tym samym roku, *Scan Integrity* Davida Chauma i zespołu oraz *Scratch, Click and Vote* polskich autorów Filipa Zagórskiego i M. Kutyłowskiego[139]. Warto również

[135] Dobrym przykładem typowego działania spyware jest Zlob.Trojan, który zapisywał informacje o odwiedzanych przez użytkownika zainfekowanego komputera stronach internetowych oraz zapisywał naciśnięcia klawiszy, a zgromadzone informacje przesyłał do bazy danych znajdującej się na odległym serwerze. Patrz: *New Malware Silently Changes Router Settings*, „PCmag.com Security Watch", http://blogs.pcmag.com/securitywatch/2008/06/new_malware_silently_changes_r.php,11.06.2008.

[136] Anti-Spyware Coalition, http://www.antispywarecoalition.org/about/index.htm.

[137] G. Gross, *US lawmakers introduce I-Spy bill*, „InfoWorld", http://www.infoworld.com/d/security-central/us-lawmakers-introduce-i-spy-bill-040, 16.03.2007.

[138] M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 70–71; D. Jefferson, A.D. Rubin, B. Simons, D. Wagner, *A Security Analysis*…, s. 1–34.

[139] M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 2.

wskazać, że zapewnienie technicznej tajności głosowania utrudnia znacznie zaimplementowanie procedur uniemożliwiających ataki sprzętowe[140].

Istotną barierą rozwoju internetowego głosowania jest niebezpieczeństwo manipulacji wynikami wyborów. Wyobrażenie o możliwości manipulacji rezultatami głosowania daje proste porównanie z bezpieczeństwem w dziedzinie bankowości internetowej. Nadużycia dokonane przez osoby trzecie w bankowości internetowej w Stanach Zjednoczonych dotyczą aż 10 proc. transakcji. Jeśli przeniesiemy skalę tego zjawiska na płaszczyznę głosowania, to taki wynik bezapelacyjnie podważa legitymizację jakichkolwiek wyborów przeprowadzonych z użyciem Internetu[141]. Podkreślić należy, że różnica pomiędzy papierową kartą do głosowania a porcją bitów reprezentujących głos obywatela polega na tym, że ta pierwsza jest trwalsza, przez co możliwość manipulacji jest znacznie ograniczona i wykrywalna[142]. W przypadku wprowadzenia internetowego głosowania pojawiają się dwie grupy osób posiadających dostęp do infrastruktury informatycznej, potencjalnie mogących dokonać manipulacji. Pierwsza z tych grup to informatycy należący do zespołu odpowiedzialnego za stworzenie, wdrożenie i obsługę internetowego systemu wyborczego. Próby manipulacji wynikami głosowania internetowego pojawiały się już w praktyce wyborczej. Najbardziej znanym przypadkiem jest fałszerstwo kodu programu do głosowania z użyciem Internetu dokonane przez amerykańskiego programistę Clintona *Clinta* Curtisa, pracującego dla firmy Yang Enterprises. Programista ten – jak sam stwierdził w wydanym w 2004 roku oświadczeniu – został nakłoniony przez swego pracodawcę do umieszczenia w pisanym programie kodu, który miał w niezauważalny sposób fałszować zebrane wyniki wyborów[143]. Tego typu działa-

---

[140] Tamże, s. 9.

[141] K. Coleman, *Internet Voting…*, strony nienumerowane; G. Monbiot, *Death of the Secret Ballot*, „The Guardian", http://www.monbiot.com/archives/2003/04/29/death-of-the-secret-ballot/, 29.04.2003.

[142] Dobitnie pokazuje to przykład polskich wyborów samorządowych w 2002 roku, kiedy pilotażowy system obsługi wyborów w krytycznym momencie odmówił posłuszeństwa, a pracownicy państwowych komisji obwodowych nie mogli za jego pośrednictwem przekazać danych do Krajowego Biura Wyborczego. Więcej na ten temat: T. Marcinek, *Głosy nie podliczone*, „Computerworld", http://www.computerworld.pl/artykuly/26990.html, 4.11.2002.

[143] K. Zetter, *More Questions for Florida*, „Wired", http://www.wired.com/politics/security/news/2004/12/66002, 13.12.2004. Więcej na temat przypadku Clintona Curtisa: P. Krawczyk, *Wyborcza lekcja prawdy*, http://www.computerworld.pl/artykuly/45498.html, 13.10.2006 oraz *Hasło: Clint Curtis*, „Encyklopedia Wikipedia", http://en.wikipedia.org/wiki/Clint_Curtis.

nia w socjolekcie programistów systemów operacyjnych nazywane są tworzeniem tylnych drzwi (*backdoor*) i polegają na pozostawieniu luki w systemie zabezpieczeń danego programu, z której można skorzystać w dowolnym czasie, na przykład uzyskując prawa administratora systemu. Tylne drzwi często są tworzone jako wygodny sposób testowania programu w trakcie pracy nad nim lub jako sposób wygodnego serwisowania programu, a więc intencjonalnie nie muszą być przygotowaniem do przyszłych nadużyć. Drugą grupą stanowią dowolne osoby spełniające warunek posiadania odpowiedniej wiedzy informatycznej oraz motywacji manipulowania wynikami głosowania, mogące uzyskać dostęp do infrastruktury za pomocą Internetu. Stwarzają one szczególne niebezpieczeństwo, bowiem na obecnym etapie rozwoju Internetu i narzędzi programistycznych włamywanie się do komputerów jest banalnie proste. Świadczyć może o tym choćby fakt, że dokonujących włamań nazywa się *script kiddies*, ze względu na ich dyletantyzm w dziedzinie informatyki oraz posługiwanie się gotowymi narzędziami programistycznymi służącymi do dokonywania włamań, w jakie nadzwyczaj łatwo można zaopatrzyć się w sieci[144]. Zakres manipulacji może obejmować: skasowanie głosów, zamianę głosów już oddanych, dodanie głosów, umożliwienie głosowania wielokrotnego uprawnionym lub nieuprawnionym do głosowania[145]. Wdrażane dotychczas systemy służące do głosowania przy użyciu Internetu zapewniały zróżnicowany poziom bezpieczeństwa. Estońscy analitycy – Ahto Buldas i Triinu Mägii – przeprowadzili opartą na teorii gier analizę opłacalności określonych typów wrogich działań wobec systemów głosowania przez Internet. Okazało się, że w amerykańskim systemie SERVE zmiana głosów na dużą skalę była możliwa i opłacalna (stosunek kosztów i zysków). Odbywała się poprzez uzyskanie kontroli nad serwerem przechowującym głosy. Również możliwe i opłacalne było anulowanie głosów na dużą skalę. Z kolei estoński system EstEVS okazał się odporny zamianę głosów oraz ich anulowanie[146].

W Internecie rozwinęły się liczne sposoby przeprowadzania ataków polegające na spowolnieniu lub uniemożliwieniu działania komputerów.

[144] W celach edukacyjnych, by unaocznić jak łatwo można zdobyć a następnie posłużyć się tego typu oprogramowaniem, zamieszczam odnośnik do programu o nazwie Netbus: http://www.packetstormsecurity.nl/trojans/index5.html. Program ten służy do przejęcia w kontroli nad komputerem innego użytkownika. Powstał on w 1999 roku i wykrywany jest przez wszystkie współczesne programy antywirusowe, nie stanowi więc niebezpieczeństwa.

[145] T. Mägi, *Practical Security Analysis…*, s. 50.

[146] M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy…*, s. 63.

Do tego celu wykorzystuje się technikę określaną mianem odmowy usługi (DoS – *Denial of Service*) lub specjalnie skonstruowane wirusy[147] bądź robaki komputerowe[148]. Atak typu odmowa usługi stwarza szczególne zagrożenie dla funkcjonowania komputerów i sieci komputerowych[149]. W celu jego przeprowadzenia wykorzystuje się nieusuwalną słabość sieci Internet, jaką jest możliwość wysyłania w krótkich odstępach czasu cyklicznych zapytań z jednego komputera do drugiego. Takie zapytania angażują zasoby komputera, który je otrzymuje. Jeśli zapytania pochodzą z wielu komputerów i wysyłane są w jednym czasie, wówczas generowany sztucznie ruch zajmuje zasoby komputera i w efekcie doprowadza do znacznego spowolnienia działania komputera, zawieszania się lub uniemożliwiania innym użytkownikom dostępu do jego zasobów[150]. Sieć komputerów służąca do dokonywania tego typu działań, a uprzednio przejęta w sposób nieuprawniony nazywana jest *botnetem*[151]. Pojedyncze

---

147 Wirus (*virus*) – jest to obcy program, który zawiera określony przez twórcę – najczęściej szkodliwy – algorytm działania. Cechami definicyjnymi wirusa są – przez analogię do wirusa biologicznego – niewielkie rozmiary oraz konieczność znalezienia nosiciela – jego kod *dokleja się* do funkcjonujących w zainfekowanym systemie programów.

148 Robak (*worm*) – jest to obcy program, który – podobnie jak wirus – może zawierać szkodliwy algorytm działania. Robak – w przeciwieństwie do wirusa – nie potrzebuje nosiciela, jest programem samodzielnym, zaś jego zadanie polega na rozprzestrzenianiu się z wykorzystaniem luk w danym systemie bezpieczeństwa, albo naiwności użytkowników.

149 W literaturze przedmiotu przedstawiono liczne klasyfikacje działań typu DoS, jednakże większość z nich odwołuje się do technicznej strony przedsięwzięcia, nie różniąc się zbytnio pod względem tych aspektów, które są interesujące z punktu widzenia niniejszego artykułu. Najdokładniejszą i najbardziej obszerną klasyfikację informatyczną przedstawili: M. Handley, E. Rescorla, *Internet Denial-of-Service Considerations, Request for Comments nr 4732*, http://tools.ietf.org/html/rfc4732, 11.2006. Ze względu na techniczną różnorodność tego typu działań funkcjonuje bardzo wiele pojęć je określających. Przyjęto, że działanie typu *Denial of Service* jest pojęciem najbardziej ogólnym i mieści w sobie wszystkie możliwe sposoby działania polegające na wykorzystaniu mechanizmu odmowy dostępu, w tym najnowsze odmiany, jak rozproszona odmowa usługi DDoS (*Distributed Denial of Service*) oraz rozproszona odbita odmowa usługi DRDoS (*Distributed Reflected Denial of Service*). Często dwa pojęcia – DoS i DDoS – używane są w innym znaczeniu: DoS oznacza działanie bezpośrednio z komputera użytkownika prowadzącego tę formę ataku, zaś DDoS działanie rozproszone (stąd nazwa) z użyciem wielu komputerów, których użytkownik nie jest właścicielem.

150 Atak tego typu jest podtypem ataku typu DoS i nazywany jest rozproszoną odmową usługi (DDoS – *Distributed Denial of Service*). S.M. Specht, R.B. Lee, *Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasure*, http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf, 09.2004, strony nienumerowane.

151 Jest to zbitek angielskich słów *bot* od robot oraz *net* od sieć.

komputery należące do takiej sieci określane są w języku użytkowników sieci *zombie* (żywe trupy). Szacuje się, że liczba komputerów *zombie* wykorzystywana do przeprowadzania ataków tego typu stanowi około 10 proc. wszystkich komputerów w Internecie[152]. Najistotniejszą cechą tego rodzaju działania jest to, że może je z łatwością podjąć pojedynczy użytkownik, skutecznie uniemożliwiając funkcjonowanie nawet największych instytucji. Działania takie skierowane przeciwko instytucjom finansowym lub rządowym mogą spowodować ogromne straty[153]. Prawodawstwa wielu krajów zadecydowały o penalizacji tego typu działań. Na przykład w Polsce przeprowadzenie takiego ataku zagrożone jest karą do pięciu lat pozbawienia wolności[154]. Postuluje się także, aby uregulować to zjawisko przez prawo międzynarodowe[155]. Najbardziej znanym zdarzeniem tego rodzaju jest – przeprowadzony w lutym 2000 roku przez Mike›a Clacka noszącego pseudonim *Mafiaboy* – atak na serwery Yahoo!, Amazon, Dell, E*TRADE, eBay i CNN. Nastoletniemu hakerowi udało się przez kilka dni blokować serwery wymienionych instytucji. Innym znanym przypadkiem jest przejęcie przez Amerykanina Jeansona J. Ancheta kontroli nad pół milionem komputerów, za pomocą których można było dokonywać ataków typu DDoS oraz wysyłać spam[156]. Innym, głośnym przypadkiem podjęcia tego typu ataku przez nieznanych, jak dotąd, sprawców było zaatakowanie w pierwszych tygodniach maja 2007 roku serwerów, na których mieściły się strony internetowe estońskiego prezydenta, premiera, parlamentu oraz innych urzędów państwowych, a także serwerów największego banku Estonii – Hansabank i serwerów kilku gazet codziennych. Działania te zostały najprawdopodobniej podjęte w proteście przeciwko usunięciu Pomnika Wyzwolicieli Tallina z centrum stolicy Estonii. O ich inspirowanie oskarżana jest Federacja

---

[152] M. Furst i in., *Emerging Cyber Threats. Report for 2008 Leading technology experts share thoughts on top emerging Internet threats for 2008*, Georgia Tech Information Security Center, 2.10.2007, s. 3.

[153] Straty spowodowane przez M. Clacka vel *Mafiaboy'a* oceniono podczas procesu na 7,5 miliona dolarów amerykańskich. Patrz: *Prison Urged For Mafiaboy*, „Wired News Report", http://www.wired.com/politics/law/news/2001/06/44673, 20.06.2001.

[154] A. Makosz, *Za blokowanie serwera może grozić 5 lat więzienia*, „Rzeczpospolita" 27.08.2007.

[155] M.P. Pręgowski, *Estonia, cyberwojna, prawda medialna*, http://error300.org/2007/06/estonia-cyberwojna-prawda-medialna.html, 1.06.2006.

[156] Więcej na ten temat: D. Verton, *Pamiętniki hakerów*, Gliwice 2002, s. 67–97 oraz *Prison Urged For Mafiaboy*…, a także: P. Konieczny, *Największy komputerowy porywacz wszechczasów?*, „Dziennik Internautów", http://di.com.pl/archiwum/12631.html, 26.01.2006, patrz także akt oskarżenia J.J. Ancheta: http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf, 02.2005.

Rosyjska, jednak nie przedstawiono na to dowodów[157]. Działania tego typu przeprowadzono także podczas konfliktu w Kosowie w 1999 roku. Podjęli je, sympatyzujący ze stroną serbską, użytkownicy Internetu ze Stanów Zjednoczonych, Chin, Rosji oraz Serbii. Atakowali oni serwery dowództwa wojsk Paktu Północnoatlantyckiego w Brukseli[158]. Podobne działania podejmowano także przeciwko duńskim gazetom, w proteście przeciw opublikowaniu karykatur Mahometa w Jyllands-Posten[159], a także po zamachach z 11 września 2001 roku[160]. Ataki typu DDoS zostały po raz pierwszy wykorzystane przeciwko systemowi głosowania przez Internet w styczniu 2003 roku. Ofiarą padła kanadyjska Nowa Partia Demokratyczna (*New Democratic Party*), która korzystała z usług firmy election.com, aby wybrać swojego lidera[161]. Bezbronny wobec ataków rozproszonej odmowy dostępu okazał się po próbach przeprowadzonych przez ekspertów w dziedzinie zabezpieczeń amerykański system SERVE[162]. Podobny problem ujawnili w holenderskim systemie głosowania KOA pracownicy grupy Security of Systems sformowanej przez Uniwersytet w Nijmegen. W swoim raporcie orzekli o poważnych lukach bezpieczeństwa, podkreślając, że przeprowadzenie ataku typu odmowy usługi było banalnie proste[163]. Ataki mające na celu opóźnienie lub uniemożliwienie działania komputerów i sieci są również przeprowadzane z użyciem wirusów lub robaków. Działanie takich programów mogłoby również polegać na zajęciu przestrzeni przez zaszyfrowanie informacji na danym komputerze[164]. Programy takie może z powodzeniem wykorzystać nawet średniozaawan-

---

[157] *Estonia leczy rany po swojej pierwszej cyberwojnie*, „Gazeta Wyborcza", 06.2007, za: „New York Times News Service", http://swiat.polskaprasa.pl/pp65694.html, oraz B. Vamosi, *Cyberattack in Estonia – what it really means*, „ZDNet News", http://news.zdnet.com/2100-1009_22-6187133.html, 05.2007.

[158] D. Verton, *Pamiętniki*…, s. 71.

[159] P. Gorzkowicz, *Islamscy hackerzy atakują duńskie serwery*, „Hacking.pl", http://hacking.pl/pl/news-5742-Islamscy_hackerzy_atakuja_dunskie_serwery.html, 02.2006.

[160] K.R. Campbell, *Cyber Protests – The Threat to Information Assurance*, „Ianewsletter", http://iac.dtic.mil/iatac/download/Vol4_No4.pdf, 2001/2002, s. 8–9. Zaatakowano m.in. arabskie strony jak: http://www.taleban.com/, http://www.talibanonline.com/.

[161] L. Acharya, *Internet*…, s. 4–5.

[162] D. Jefferson, A.D. Rubin, B. Simons, D. Wagner, *A Security Analysis*…, s. 1–34.

[163] M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 81.

[164] Pierwszym, zastosowanym na masową skalę w celach przestępczego szantażu był wirus o nazwie: Virus.Win32.Gpcode.ai, którego działanie polegało na zaszyfrowaniu zaatakowanego dysku twardego. Za przywrócenie status quo przestępcy żądali od zaatakowanej instytucji okupu.

sowany użytkownik Internetu[165]. Jednym z najbardziej wstrząsających przykładów zagrożeń, jakie stwarza wykorzystanie złośliwego oprogramowania wobec instytucji posiadających dobrze zabezpieczone sieci komputerowe jest robak komputerowy Stuxnet odkryty w czerwcu 2010 roku przez białoruskich ekspertów od zabezpieczeń sieci z firmy VirusBlokAda. Infekuje on informatyczne infrastruktury przemysłowe kontrolujące przebieg procesów technologicznych. Wykonuje dwie czynności: zbiera informacje o zaatakowanym systemie oraz przeprogramowuje go w sposób niezauważalny dla administratorów. Rozprzestrzenia się także za pomocą fizycznych nośników danych (na przykład pendrive›ów), aby móc zainfekować komputery fizycznie odcięte od Internetu. Specjaliści sądzą, że robak został stworzony za pomocą zaawansowanych narzędzi programistycznych, nad jego powstaniem pracował zespół ludzi o różnorodnych specjalizacjach informatycznych, a potencjał tego programu pozwalał zaatakować dowolną infrastrukturę krytyczną na świecie (na przykład elektrownię, rafinerię, fabrykę, sieć przesyłową gazu). Robak ten aktywuje się, gdy rozpoznaje oprogramowanie wykorzystywane w maszynach przemysłowych firmy Siemens. Sprawdza on co pięć sekund, czy maszyny takie zostały uruchomione i jeśli tak, to aktywuje podprogram mający za zadanie zniszczyć je w sposób fizyczny, zmuszając do destruktywnego działania. Według ekspertów w dziedzinie zabezpieczeń Stuxnet był bronią wymierzoną w określony cel, wskazują na to statystyki infekcji: zarażone maszyny przede wszystkim znajdują się w takich krajach jak Iran, Pakistan, Indie oraz Indonezja, a także Chiny. Cel ataku stanowi według analityków irańska infrastruktura krytyczna, między innymi reaktor atomowy w Bushehr[166].

Ataki polegające na odmowie usługi lub wykorzystaniu złośliwych programów stanowią realną groźbę dla internetowych systemów wyborczych. Dotychczas nie opracowano skutecznego remedium na nie, a samoobrona

---

[165] Zainteresowanym polecam przetestowanie narzędzia Virus Construction Set służącego do konstruowania wirusów z gotowych modułów. Do uruchomienia i obsługi wymaga ono zaledwie elementarnej wiedzy informatycznej. Program powstał w 1990 roku, nie jest niebezpieczny dla komputerów zaopatrzonych we współczesne programy antywirusowe: http://vx.netlux.org/vx.php?id=tv13.

[166] Patrz między innymi: E. Mills, *Expert: Stuxnet was built to sabotage Iran nuclear plant*, „InSecurity Complex", http://news.cnet.com/8301-27080_3-20017201-245.html, 21.09.2010; L. O'Murchu, *Last-minute paper: An indepth look into Stuxnet*, „Virus Bulletin", http://www.virusbtn.com/conference/vb2010/abstracts/LastMinute7.xml, 09.2010; Stuxnet worm hits Iran nuclear plant staff computers, „BBC News Middle East", http://www.bbc.co.uk/news/world-middle-east-11414483, 26.09.2010.

przed nimi jest często nieskuteczna. Wydaje się, że brak bezpieczeństwa stanowi podstawowy problem uniemożliwiający wprowadzenie systemów głosowania w najbliższej przyszłości[167].

Rozwiązanie problemów technicznych nie eliminowałoby barier na drodze do wdrożenia głosowania przez Internet. Nie mniej istotne są bariery o charakterze społecznym: brak zaufania obywateli do głosowania z użyciem Internetu, nadmiernie skomplikowany dla obywateli system głosowania oraz nierównomierny poziom informatyzacji społeczeństwa. Skrót WWW (*World Wide Web*) rozwijany jest czasem przez użytkowników Internetu żartobliwie jako *Wild West Web*, by dać wyraz przekonaniu, że Internet jest obszarem licznych zagrożeń i bezprawia, jak niegdyś Dziki Zachód. Doświadczenia użytkowników Internetu oraz docierające do nich wiadomości na temat licznych niebezpieczeństw tworzą barierę psychologiczną, która pomimo usunięcia problemów technicznych utrudniłaby wdrażanie internetowych systemów głosowania na odległość. Na niski poziom zaufania wpływają nieudane eksperymenty z wyborami przez Internet. Taka sytuacja miała miejsce podczas wyborów samorządowych w okręgu Boone (Stany Zjednoczone), gdzie wszystkich zaskoczyły wyniki uzyskane przy wykorzystaniu oprogramowania MicroVote: w miejscowości, gdzie uprawnionych do głosowania było 19 000 obywateli, system naliczył 144 000 oddanych głosów[168]. W 2000 roku ponad dwie trzecie Amerykanów uważało, że stworzenie bezpiecznego systemu głosowania z użyciem Internetu zajmie wiele lat lub nie zdarzy się nigdy[169]. Przeprowadzone w 2004 roku badania jakościowe metodą grupowych wywiadów zogniskowanych na zachodnioeuropejskich internautach wykazały, że poziom zaufania do Internetu, a w tym do bezpieczeństwa głosowania jest nadzwyczaj niski; badani zgłaszali przede wszystkim obawę, że głosowanie przez Internet stworzyłoby dla władzy nieodpartą pokusę wykorzystywania wiedzy o preferencjach politycznych obywateli[170]. Z kolei w Austrii po testach systemu elektronicznego głosowania przeprowadzono badania ilościowe, które wykazały wyższy, aczkolwiek nadal niezadowalający, stopień zaufania do głosowania z użyciem elektronicznych kanałów przekazu – jedna trzecia bada-

[167] F. Mendez, A.H. Trechsel, *The European Union and E-voting*…, [w:] A.H. Trechsel, F. Mendez (ed.), *The European Union and E-voting*…, s. 2; A.M. Oostveen, P. Besselaar van den, *Internet Voting*…, s. 65.

[168] D. Springer, *E-voting*…, strony nienumerowane.

[169] *A Report on the Feasibility*…,s. 36.

[170] A.M. Oostveen, P. Besselaar van den, *Internet Voting*…, s. 71.

nych nie wierzyła w anonimowość i poprawność testowanego systemu wyborczego[171].

W literaturze przedmiotu podkreśla się, że warunkiem zastosowania Internetu w procedurach wyborczych jest wysoki poziom zaufania społecznego; mówi się o konieczności prowadzenia kampanii zmieniających negatywny stereotyp Internetu[172]. Derrick de Kerckhove przekonuje, że najistotniejszym, niezależnie od kwestii technicznych, czynnikiem jest „przygotowanie publiczności"[173]. Brak zaufania może jednak, wbrew oczekiwaniom zwolenników głosowania z użyciem Internetu, przyczynić się do obniżenia frekwencji wyborczej na skutek wprowadzenia internetowych wyborów[174]. W tym miejscu należy wskazać istotny dylemat twórców oprogramowania przeznaczonego do prowadzenia wyborów z wykorzystaniem Internetu. Ujawnienie kodu źródłowego takiego programu czyniłoby zadość wymogowi transparencji; negatywnym efektem takiej decyzji byłoby zwiększenie niebezpieczeństwa odnalezienia luk w takim oprogramowaniu i wykorzystanie ich do swoich celów niekonieczne z pożytkiem dla dobra wspólnego. Z kolei nieujawnianie kodu źródłowego naraziłoby władze na krytykę i podejrzenia o chęć zatajenia możliwości informatycznej manipulacji wynikami wyborów[175].

Istotną barierą, łączącą się z kwestią zaufania do systemu głosowania przez Internet, jest problem złożoności działania oprogramowania i sieci komputerowych. Analizy wykazują, że w świadomości większości użytkowników Internetu i komputerów technika ta traktowana jest jak „czarna skrzynka" o niezrozumiałych procedurach i zasadach funkcjonowania, choć wiadomych efektach działania[176]. W teorii demokracji podkreśla się,

---

171 M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 50.

172 *A Report on the Feasibility*…, s. 6; D. Springer, *E-voting*…, strony nienumerowane.

173 D. de Kerckhove, *Powłoka kultury. Odkrywanie nowej elektronicznej rzeczywistości*, Warszawa 2001, s. 22.

174 A.M. Oostveen, P. Besselaar van den, *Internet Voting*…, s. 65.

175 E.A. Fischer, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues*, CRS Report for Congress, http://epic.org/privacy/voting/crsreport.pdf, 4.11.2003, s. 26. Warto zwrócić uwagę na fakt, że kwestia udostępniania źródeł oprogramowania użytkownikom jest przedmiotem zainteresowania oraz intensywnych działań społeczności użytkowników komputerów od lat osiemdziesiątych XX wieku. Jest to obecnie prężny ruch społeczny na rzecz Wolnego Oprogramowania. Ruch ten zapoczątkował Richard M. Stallman, legenda subkultury hakerów, programista z Massachusetts Institute of Technology.

176 R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 90; G. Schryen, *E-Democracy*…, strony nienumerowane.

że zaufanie obywateli do aktu wyborczego jest w znacznej mierze funkcją jego przejrzystości i klarowności. Tymczasem jest to jeden z najsłabszych punktów internetowych wyborów[177]. Warunkiem wdrożenia głosowania z użyciem Internetu jest zrozumiałość mechanizmów jego funkcjonowania (w tym zasad bezpieczeństwa głosu) dla przeciętnego wyborcy bez doświadczenia informatycznego i matematycznego. Ponadto system taki powinien umożliwiać łatwe wyrażenie swojej woli osobie o niskich umiejętnościach matematycznych i informatycznych[178]. Eksperymenty z głosowaniem w Internecie pokazują, że jest to warunek niemal niemożliwy do spełnienia ze względu na niepełnowartościowe wzorce behawioralne użytkowników Internetu. Spektakularnym przykładem jest test austriackiego systemu głosowania internetowego w 2006 roku, który wypadł niepomyślnie, bowiem żaden z testujących go wyborców nie zadał sobie trudu dokładnego przeczytania opisu technicznego oraz instrukcji obsługi systemu[179]. W efekcie system zabezpieczeń i szyfrowania może stać się absolutnie nieprzejrzysty i niezrozumiały dla przeciętnego użytkownika, co siłą rzeczy będzie skutkowało spadkiem zaufania, sceptycyzmem, zniechęceniem do podejmowania aktywności wyborczej za pośrednictwem Internetu[180]. Niska świadomość zasad działania systemu głosowania wśród obywateli może zachęcić partie polityczne do prób manipulacji wyborcami. Posłużyć się tu można analogią do stosowanego obecnie w Wielkiej Brytanii procederu (legalnego, choć wysoce nieetycznego) nazywanego *granny farming*. Praktyka prowadzona jest w domach starców i wykorzystuje ona nieuwagę ofiar oraz nieznajomość procedur wyborczych. Osoba dokonująca manipulacji dostarcza pensjonariuszom domu opieki wypełnione uprzednio karty głosowania i skłania do ich podpisania, a następnie wysyła. Pensjonariusze są przekonani, że składając podpis głosują na preferowanego kandydata, choć niekoniecznie tak musi być[181].

Czynnikiem uniemożliwiającym wdrożenie internetowego głosowania na szeroką skalę jest zjawisko nierównego dostępu różnych grup społecz-

---

177 P. Gomułkiewicz, *Wirtualne*… .

178 M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 14.

179 Tamże, s. 50.

180 M. Gajlewicz, *Demokracja a nowe technologie,* [w:] J. Adamowski (red.), *Demokracja a nowe środki komunikacji społecznej*, Warszawa 2004, s. 59; L. Pratchett, M. Wingfield, N.B. Fairweather, S. Rogerson, *Balancing Security and Simplicity in E-voting. Towards an Effective Compromise?*, [w:] A.H. Trechsel, F. Mendez (ed.), *The European Union and E-voting*…, s. 63.

181 L. Pratchett, M. Wingfield, N.B. Fairweather, s. Rogerson, *Balancing Security*…, s. 171.

nych i jednostek do Internetu; narusza ono podstawowe zasady demokracji – równość i powszechność wyborów[182]. Zjawisko niejednakowych możliwości korzystania z sieci nazywane jest w literaturze przedmiotu cyfrowym podziałem (*digital divide*)[183] i oznacza dychotomiczny podział na posiadających i nieposiadających dostępu do Internetu z powodów technicznych: braku właściwego sprzętu, oprogramowania i łącza telekomunikacyjnego[184]. Ten dychotomiczny podział został z czasem uzupełniony o nowe wymiary. Jako pierwsi wskazali je Manuel Castells oraz Eszter Hargittai. M. Castells mówi o różnicach w poziomie wiedzy[185], a E. Hargittai używa pojęcia cyfrowego podziału drugiego stopnia (*second level digital divide*) argumentując, że sam dostęp do Internetu jest konieczny, choć niewystarczający, bowiem niezbędne jest osiągnięcie określonego poziomu kompetencji w zakresie efektywnego i skutecznego wykorzystania Internetu[186]. Ponadto wymienia takie czynniki cyfrowego podziału drugiego stopnia jak: autonomia użycia rozumiana jako swoboda i względnie nieograniczony dostęp do posiadanego łącza internetowego oraz istnienie sieci społecznego wsparcia, dających możliwość skorzystania z pomocy innych, bardziej zaawansowanych użytkowników. Cyfrowy podział zaczął wykształcać się w połowie lat dziewięćdziesiątych XX wieku wraz z rozpoczętym dynamicznym procesem umasawiania Internetu[187];

---

[182] *Code of Good Practice in Electoral Matters*… s. 5.

[183] Dominik Batorski proponuje tłumaczenie pojęcia *digital divide* na język polski jako cyfrowe wykluczenie. Patrz: http://sna.pl/dbatorski/SocjologiaInternetu.html#Proble matyka. Debata na temat cyfrowego wykluczenia jest relatywnie nowa, jednak podziały społeczne wynikające z nierównego dostępu do rozmaitych technologii są względnie stare. Na przykład w XIX i XX wieku Amerykanie doświadczali podziału między wsią i miastem w dostępie do telegrafu. Następnie podział przesunął się na tych, którzy mieli dostęp do elektryczności i tych którzy nie mieli. Kolejne dotyczyły posiadania telefonu i telewizora. Patrz: R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 44.

[184] Athanasios I. Bozinis pisze o wyłanianiu się dwóch grup: *Elektronicznych Arystokratów* korzystających z dostępu do Internetu w dowolnym wymiarze czasowym i *Elektronicznych Metysów* nieposiadających możliwości korzystania z tego medium: A.I. Bozinis, *Internet Politics and Digital Divide Issues: The Rising of a New Electronic Aristocrats and Electronic Meticians*, „Journal of Social Sciences" 2007, nr 3 (1), s. 24–26.

[185] M. Castells, *Galaktyka Internetu. Refleksje nad Internetem, biznesem i społeczeństwem*, Poznań 2003, s. 77–156.

[186] E. Hargittai, *Second-Level Digital Divide: Differences in People's Online Skills*, „First Monday. Peer-Reviewed Journal of the Internet", http://www.firstmonday.org/issues/issue7_4/hargittai/index.html, 1.04.2002.

[187] K. Pietrowicz, *Nowa stratyfikacja społeczna? 'Digital divide' a Polska*, [w:] L.H. Haber (red.), *Społeczeństwo informacyjne – wizja, czy rzeczywistość?: II ogólnopolska konferencja naukowa*, Kraków 2004, s. 255.

kwestią dyskusyjną pozostają tezy zarówno o jego zaniku, jak też rozwoju[188]. Istotną zmienną warunkującą cyfrowy podział stanowi wiek. Dużą grupę wykluczonych stanowią osoby w podeszłym i średnim wieku. Spośród Amerykanów, którzy przekroczyli 65 rok życia tylko co czwarty korzysta z Internetu (26 proc.), w porównaniu z 67 proc. korzystających w wieku 50–64 lata, 80 proc. w wieku 30–49 lat i 84 proc. w wieku 18–29 lat[189]. Testy kompetencji przeprowadzone przez E. Hargittai wykazały, że w grupie wiekowej 10–19 lat średni czas wykonania zadań związanych z użyciem Internetu jest ponad trzykrotnie krótszy niż w grupie siedemdziesięciolatków i dwukrotnie krótszy w grupie czterdziestolatków. Również stopień poprawnej realizacji powierzonych zadań wykazuje znaczną przewagę osób w wieku 10–19 lat nad starszymi użytkownikami Internetu[190]. Wykształcenie także stanowi ważną zmienną przy opisie cyfrowego podziału. Osoby z wykształceniem średnim (*college degree*) radziły sobie znacznie gorzej w teście kompetencji obsługi Internetu niż osoby z wykształceniem wyższym (*graduate degree*) i bez wykształcenia średniego (*no college degree*)[191]. Z kolei płeć nie warunkuje cyfrowego podziału aż tak drastycznie, jednak dają się zaobserwować pewne różnice. Kobiety nieco rzadziej używają Internetu, niż mężczyźni, korzystają z mniejszej liczby usług i mniej chętnie zdobywają informacje za pośrednictwem Internetu, a także rzadziej angażują się w Internetowe formy wspólnoty[192]. Konsekwencje cyfrowego podziału zaobserwowano podczas prób z elektronicznym głosowaniem. Na przykład testy amerykańskiego systemu *Threeballot* wykazały, że grupa wyborców w Stanach Zjednoczonych miała poważne problemy z dokonaniem w nim dość prostych czynności związanych

---

188 W. Chen, B. Wellman, *Charting and Bridging Digital Divides: Comparing Socio-economic, Gender, Life Stage, and Rural-Urban Internet Access and Use in Eight Countries*, Centre for Urban and Community Studies, University of Toronto, http://www.amd.com/us-en/assets/content_type/DownloadableAssets/FINAL_REPORT_CHARTING_DIGI_DIVIDES.pdf, 10.2003 oraz J.E. Katz, R.E. Rice, *Social Consequences of Internet Use. Access, Involvement, and Interaction*, Cambridge, Londyn 2002, s. 39–55.

189 S. Fox, *Digital Divisions*, http://www.pewinternet.org/pdfs/PIP_Digital_Divisions_Oct_5_2005.pdf, 05.10.2005. Badanie zostało przeprowadzone metodą wywiadów telefonicznych wspomaganych komputerowo (CATI) w dniach 4 maja–7 czerwca 2005 na próbie dorosłych Amerykanów liczącej N=2001 respondentów.

190 E. Hargittai, *Second-Level Digital Divide*…, strony nienumerowane

191 Tamże, strony nienumerowane.

192 Patrz obszerne opracowanie: T. Kennedy, B. Wellmanm K. Klement, *Gendering the Digital Divide*, „IT&Society", http://www.stanford.edu/group/siqss/itandsociety/v01i05/v01i05a05.pdf, 2003, s. 72–96.

z prawidłowym oddaniem głosu[193]. Negatywne konsekwencje cyfrowego podziału dla wykluczonych grup będą tym bardziej widoczne, w im większym zakresie podejmowane będą próby implementacji internetowego głosowania, bez jednoczesnych usiłowań przezwyciężenia nierówności. Cyfrowy podział może powodować większe rozłamy i zniekształcenie woli powszechnej niż głosowanie tradycyjne, a w efekcie skutkować spadkiem frekwencji wyborczej, wytworzeniem się negatywnych postaw wobec polityki i polityków, rozwojem pozawyborczych kanałów ekspresji woli przez społeczeństwo[194].

Wdrożenie głosowania przez Internet napotyka szereg barier o charakterze politycznym. Najistotniejsze z nich to zagrożenie utratą bezpośredniej kontroli nad procesem wyborczym przez państwo i obywateli, ryzyko handlu głosami, globalizacja aktu głosowania, groźba naruszania wolności głosowania, ryzyko banalizacji aktu głosowania, a także problem ogniskowania się polityki na problemach internetowego głosowania w sieci jako wygodnym temacie zastępczym oraz potencjalna możliwość nieprzewidywalnych zmian na scenie politycznej.

Głosowanie internetowe może powodować utratę bezpośredniej kontroli nad procesem wyborczym przez państwo i obywateli. W wyborach z użyciem Internetu nadzorowanie procesu wyborów skupia się w rękach nielicznych jednostek – administratorów i programistów obsługujących system informatyczny, dla których podstawowym kryterium dopuszczenia do obsługi są kompetencje techniczne, a nie kwalifikacje moralne. Z kolei w tradycyjnym systemie głosowania struktura ta jest rozproszona w obwodowych komisjach wyborczych, gdzie odpowiedzialność spoczywa na instytucji mężów zaufania, zachodzi zjawisko wzajemnej, krzyżowej kontroli podmiotów obsługujących wybory. Badacze wyrażają obawy, że w scentralizowanym systemie internetowego głosowania na odległość dojść może do nadużyć ze strony technokratów działających na rachunek własny lub siły politycznej wywierającej presję[195]. Jeśli twórcą oprogramowania systemu głosowania jest podmiot drugiego sektora, to dochodzi do sytuacji, w której kluczowy dla funkcjonowania systemu demokratycznego proces jest kontrolowany przez instytucję komercyjną, nastawioną na zysk, działającą wedle logiki wolnego rynku, która

[193] G. Belote, H. Jones, J. Juang, *Threeballot in the Field,* http://theory.lcs.mit.edu/classes/6,857/projects/threeBallotPaper.pdf, 2006; M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 7–8.

[194] R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 12.

[195] A.M. Oostveen, P. Besselaar van den, *Internet Voting*…, s. 65; P. Gomułkiewicz, *Wirtualne*… .

niekoniecznie musi podpowiadać to, co jest słuszne z punktu widzenia dobra państwa[196]. Ryzyko autonomizacji podsystemu informatycznego jest realne. Niemiecki Federalny Trybunał Konstytucyjny uznał w 2009 roku wybory z użyciem Internetu za niekonstytucyjne między innymi ze względu na brak możliwości kontroli obywateli i państwa nad procesem zbierania i zliczania głosów, co zahamowało prace nad wdrażaniem tych systemów[197].

Poważnym problemem związanym z wyborami internetowymi na odległość jest potencjalnie łatwiejsze dokonanie sprzedaży głosu, niż w wyborach tradycyjnych[198]. Głosowanie z użyciem Internetu pozwala uniknąć odpowiedzialności za sprzedanie głosu, bowiem transakcja może dokonać się za pomocą oprogramowania, które przejmuje kontrolę nad komputerem użytkownika, a głosujący może tłumaczyć się nieświadomością faktu działania na jego komputerze takiego programu. Ponadto może uniknąć odpowiedzialności karnej, gdy procedura sprzedaży głosów odbywa się na serwerze znajdującym się poza jurysdykcją danego państwa, nie ma więc możliwości ścigania. Jest to realne niebezpieczeństwo – według estońskich analityków w systemie SERVE możliwe i opłacalne byłoby kupowanie i sprzedaż głosów na dużą skalę[199]. Z kolei w estońskim EstEVS sprzedaż głosów stała się nieopłacalna dzięki umożliwieniu wyborcy głosowania wielokrotnego, ponieważ rozwiązanie takie znacznie ogranicza pewność kupującego co do wywiązania się sprzedającego z umowy[200].

W literaturze przedmiotu podkreśla się, że Internet jest czynnikiem erozji politycznej granic państwowych, bowiem funkcjonuje niezależnie od państw i z technicznego punktu widzenia trudno jest ograniczyć jego autonomię[201]. Wdrażający głosowanie muszą liczyć się z faktem, że za sprawą Internetu wpływ na funkcjonowanie infrastruktury informatycznej mogą mieć również podmioty znajdujące się poza granicami państwa. Zapewnienie prawidłowego, niezakłóconego przebiegu wyborów przyjmuje wskutek tego wymiar międzynarodowy, zwielokrotnia konieczność zapewnienia właściwych środków bezpieczeństwa. Ma to szczególne znaczenie na obecnym etapie rozwoju Internetu, w którym widoczną tendencją jest

---

196 *Stanowisko Stowarzyszenia Internet Society*…, s. 11–12.

197 M. Chmielewski, *Wybory elektroniczne*… .

198 A.M. Oostveen, P. Besselaar van den, *Internet Voting*…, s. 65.

199 M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 63.

200 P. Gomułkiewicz, *Wirtualne*…; M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 50.

201 P. Maj, *Internet i demokracja. Ewolucja systemu politycznego*, Rzeszów 2009, s. 35.

rosnące upolitycznienie działań rozmaitych podmiotów, odkrywanie, że Internet staje się potężnym narzędziem mogącym służyć do prowadzenia skutecznej gry politycznej. Najnowszymi poznanymi przejawami tego rodzaju działań jest opisany wyżej robak Stuxnet, a także odkryta w marcu 2009 roku sieć, której publicyści nadali nazwę GhostNet[202]. Podejrzewa się, że jest to narzędzie skonstruowane i wykorzystywane przez Chiny w celu zdobywania informacji na całym świecie. Dotychczas wykryto infekcję 1 295 komputerów w 103 krajach, zostały one zarażone przez wirus o nazwie GhostRat, który „podłączył" je do sieci GhostNet. Sieć GhostNet przejmuje całkowitą (choć niezauważalną) kontrolę nad komputerem, może przechwytywać wszelkie przychodzące i wychodzące z niego informacje, a także wykorzystywać urządzenia peryferyjne podłączone do komputera – takie, jak mikrofony i kamery[203]. Potencjalnie sieć GhostNet mogłaby zostać wykorzystana do manipulacji lub uniemożliwienia przeprowadzenia wyborów internetowych na odległość.

Głosowanie internetowe stwarza groźbę naruszenia zasady wolności głosowania. Nie można mieć pewności, czy takie głosowanie będzie wolne od presji osób trzecich – członków rodziny lub przełożonych w zakładzie pracy[204]. Problem ten jednak można rozwiązać tak jak uczyniono to w Estonii, dzięki wprowadzeniu możliwości wielokrotnego głosowania[205].

Istnieje też ryzyko banalizacji aktu głosowania przez Internet. Obecność w lokalu wyborczym i oddawanie głosu jest w demokracjach rodzajem rytuału symbolicznie legitymizującego ten system, potwierdzającym jego wartość i cementującym obywateli[206]. Sprowadzenie głosowania do wpisania swojego kodu i kliknięcia w określonym miejscu strony internetowej redukuje wymiar symboliczny i wartość uczestnictwa, sprowadza wybory i demokrację do *game-show*[207].

Jako mniej istotne potencjalne bariery wdrożenia internetowego głosowania można wskazać ryzyko zogniskowania się polityki na problemach

---

[202] Obszerny raport na temat GhostNet: *Tracking GhostNet. Investigating a Cyber Espionage Network*, „Information Warfare Monitor", http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network, 29.03.2009, s. 1–53.

[203] *China accused over global computer spy ring*, „The Guardian", http://www.guardian.co.uk/world/2009/mar/30/china-dalai-lama-spying-computers, 30.03.2009; Major cyber spy network uncovered, „BBC News", http://news.bbc.co.uk/2/hi/americas/7970471.stm, 29.03.2009.

[204] M. Usidus, *Czyj jest*… .

[205] M. Kutyłowski, P. Kubiak, Z. Gołębiewski, F. Zagórski, *Elektroniczne systemy*…, s. 50.

[206] R.K. Gibson, *Internet Voting*…, s. 40.

[207] Tamże, s. 40; M. Nowina-Konopka, *Elektroniczna*…, s. 4–5.

internetowego głosowania w sieci, jako wygodnym temacie zastępczym[208]. Inną przeszkodą może być obawa dominujących sił politycznych przed zmianą *status quo*; modyfikacja sposobu głosowania wywoła zapewne określone przemiany elektoratu (na przykład będą głosowali ci, którzy dotychczas tego nie czynili) i wyniki wyborów mogą być nieprzewidywalne dla obecnych elit[209].

D. de Kerckhove podkreślał, że ludzkość jest nieprzerwanie tworzona i przetwarzana przez jej własne wynalazki[210]. Wprowadzenie głosowania przez Internet może stać się katalizatorem zmian społecznych i politycznych. Wyniki przeprowadzonych analiz skłaniają do refleksji nad możliwymi scenariuszami przyszłości w efekcie zastosowania techniki głosowania internetowego we współczesnych demokracjach.

Badacze wskazują, że głosowanie z użyciem Internetu będzie wzmacniać demokrację przedstawicielską głównie poprzez zintensyfikowanie zaangażowania w politykę grup już w niej działających i wciągnięcie do uczestnictwa nowych grup nieuczestniczących dotychczas w polityce. Wielu badaczy zakłada, że zmiany (o ile nastąpią) będą powolne. Taki sposób myślenia określa się mianem technorealizmu[211], teorii minimalnej zmiany (*minimal effect theories*)[212] lub teorii normalizacji (*normalizaton theory*)[213]. Ten sposób myślenia silnie identyfikuje się z udowodnioną empirycznie, klasyczną hipotezą Paula Lazarsfelda, głoszącą, iż media wzmacniają istniejące zachowania polityczne, lecz ich nie zmieniają[214]. Umiarkowany optymizm badaczy reprezentujących ten nurt oparty jest przede wszystkim na wynikach badań ilościowych i jakościowych prowadzonych w Internecie na szerszą skalę od drugiej połowy lat dziewięćdziesiątych XX wieku. Badacze zaliczani do tego nurtu na ogół wskazują, że Internet wzmacnia instytucje demokracji przedstawicielskiej

---

[208] Problem ten dostrzegł: M. Usidus, *Czyj jest…* .

[209] Barierę tę, choć nie w kontekście wyborów przez Internet, wskazał: P. Skwiecieński, *Społeczeństwo radosnych dzieciaków*, „Rzeczpospolita" 10.03.2010.

[210] D. de Kerckhove, *Powłoka kultury…*, s. 23.

[211] A.G. Wilhelm, *Democracy in the Digital Age. Challenges to Political Life in Cyberspace*, Nowy Jork, Londyn 2000, s. 14–23.

[212] P. Norris, J. Curtice, *The News Media and Civic Engagement*, http://ksghome.harvard.edu/~pnorris/ACROBAT/ECPR98.PDF, 23–28.03.1998, s. 3 oraz K. Newton, *Politics and the News Media: Mobilization or Videomalaise?*, [w:] R. Jowell (red.), *British Social Attitudes: the 14th Report, 1997/8,* Ashgate 1998.

[213] R. Gibson, S.J. Ward, *U.K. Political Parties and the Internet: 'Politics as Usual' in the New Media?*, „The Harvard International Journal of Press/Politics" 1998, nr 3, s. 14–38.

[214] Cyt. za: P. Norris, J. Curtice, *The News Media…*, s. 3.

oraz intensyfikuje partycypację polityczną[215]. Nie należy oczekiwać, by scenariusz e-demokracji przedstawicielskiej rozwijał się żywiołowo, istotne jest wieloaspektowe wsparcie i stymulacja ze strony władz państwowych lub organizacji trzeciego sektora, a także czynne poparcie obywateli.

Niektórzy badacze uznają Internet za medium o większym potencjale wpływu na zmiany socjopolityczne i podkreślają, że dzięki niemu możliwe jest przekształcenie współczesnych demokracji przedstawicielskich w elektroniczną demokrację bezpośrednią (e-demokrację bezpośrednią). Wizja ta zaczęła się kształtować wraz z rozwojem technologii komputerowych, upowszechnieniem się komputerów osobistych i pojawieniem pierwszych usług sieciowych dla cywilów w pierwszej połowie lat dziewięćdziesiątych. W skrajnie optymistycznym ujęciu ten sposób myślenia określony został przez Benjamina R. Barbera mianem scenariusza Panglossa (*Panglossian Scenario*)[216]. Wizję tę wiąże B.R. Barber z samozadowoleniem oraz uproszczoną i fałszywą projekcją występujących obecnie trendów; nazywa ten scenariusz naiwnym i ahistorycznym, pełnym złudzeń odnośnie ludzkich zachowań w sferze polityki. Scenariusz Panglossa tkwi w przekonaniu, że skoro Internet umożliwia demokrację bezpośrednią, to jest to warunkiem wystarczającym do tego, aby ona zaistniała, wstępem do jej ziszczenia jest wdrożenie wyborów z użyciem Internetu. Scenariuszem bardziej stonowanym mieszczącym się jednak w wizji e-demokracji bezpośredniej jest scenariusz Jeffersona (*Jeffersonian Scenario*). B.R. Barber podkreśla, że demokracja jest formą rządów, która opiera się na informacji i komunikacji. Jest dlań oczywiste, że nowe technologie informacji i komunikacji mogą być korzystne dla demokracji i rozwijać ją, jednak w granicach ściśle zakreślonych przez instytucje państwa, poprzestając na konsultacjach społecznych oraz debatach z użyciem Internetu[217]. Dick Morris wyraża pogląd, że utopijna wizja Tomasza Jeffersona bazująca na zgromadzeniach obywateli i bezpośredniej partycypacji jest bliska ziszczeniu właśnie dzięki Internetowi. Badacz ten jest przekonany, że stopniowo do praktyki politycznej zaczną wkraczać cykliczne referenda, początkowo niewiążące, a kiedy przekroczona zosta-

[215] J. Corrales, *Lessons…*, [w:] *Democracy and the Internet*. .., s. 35.

[216] Doktor Pangloss to postać niepoprawnego optymisty ze sztuki *Kandyd* Voltaira (wł. Françoisa-Marie Arouet). Przypuszcza się, że pierwowzorem dla Panglossa był filozof Gottfried Wilhelm Leibniz, który w swojej *Teodycei* argumentował, że żyjemy w najlepszym z możliwych światów.

[217] B.R. Barber, *Three Scenarios for the Future Technology and Strong Democracy*, „Political Science Quarterly" 1998–1999, nr 113 (4), s. 584.

nie określona bariera liczebności biorących w nich udział będą miały one nie tylko konsultacyjny, lecz decydujący charakter, zastępując instytucje demokracji pośredniej. Zmiany takie są nieuniknione, a internetowe referenda staną się dla obywateli tak zwyczajne, jak czynność codziennego czytania gazety lub używanie poczty elektronicznej; zmiany te, zajdą zarówno na szczeblu lokalnym, jak i ogólnopaństwowym[218]. Wielu badaczy demokracji krytykuje jednak te poglądy uważając, że wdrożenie demokracji bezpośredniej, w której katalizatorem zmian miałoby się stać umożliwienie obywatelom głosowania z użyciem Internetu jest niemożliwe, bowiem każda zmiana socjopolityczna wynika z realnej potrzeby, a tej u obywateli nie ma[219].

Niektórzy badacze ostrzegają przed rozwojem demokracji bezpośredniej, uznając, że może ona mieć negatywne skutki dla demokracji, gdy obywatele i władze wpadną w „pułapkę referendów" czyniąc je podstawowym mechanizmem podejmowania decyzji politycznych[220]. Elektroniczna demokracja bezpośrednia przerodzić może się łatwo w elektroniczną demokrację plebiscytarną (e-demokrację plebiscytarną) lub elektroniczny populizm (e-populizm)[221]. Demokracja plebiscytarna to forma demokracji opierająca się na instytucjach demokracji bezpośredniej i całkowitym lub częściowym – ale znacznym – zlikwidowaniu instytucji pośredniczących w tworzeniu prawa i sprawowaniu władzy. Badacze wskazują, że ten negatywny typ demokracji może być z technicznego punktu widzenia łatwo wdrożony w wielomilionowych społeczeństwach dzięki Internetowi[222]. Wprowadzenie instytucji demokracji plebiscytarnej może skutkować poważnymi zakłóceniami ładu politycznego, doprowadzić do specyficznej

---

[218] D. Morris, *vote.com. How big-money lobbyists and the media are losing their influence, and the Internet is giving power back to the people*, Los Angeles 1999, s. 27–33, 141, 146.

[219] A. Malina, *Perspectives on citizen democratisation and alienation in the virtual sphere*, [w:] B.N. Hague, B.D. Loader (ed.), *Digital Democracy. Discourse and Decision Making in the Information Age*, Londyn, Nowy Jork 1999, s. 38; E. Milner, *Electronic government: more than just a 'good thing'? A question of 'ACCESS'*, [w:] tamże, s. 70; P. Nixon, H. Johansson, *Transparency through technology: the internet and political parties*, [w:] tamże, s. 147–148; T. Locke, *Participation, inclusion, exclusion and netactivism: how the internet invents new forms of democratic activity*, [w:] tamże, s. 219.

[220] R.M. Alvarez, T.E. Hall, *Point, Click & Vote…*, s. 15.

[221] Pojęcie demokracji plebiscytarnej szeroko omawia i porównuje z innymi formami demokracji: B.R. Barber, *Which Technology and Which Democracy?*, http://web.mit.edu/m-i-t/articles/barber.html, 6.12.1998.

[222] I. Budge, *The New Challenge of Direct Democracy*, Cambridge 1996, s. 59–74; D. Morris, *Direct Democracy and the Internet*, „Loyola of Los Angeles Law Review" 2001, nr 40 (3), s. 1033–1053.

formy totalitaryzmu polegającej na tyranii większości[223]. Największym zagrożeniem demokracji jawi się w tym kontekście zagarnięcie władzy przez większość i niedopuszczenie do głosu mniejszości. Zagadnienie to rozpatrywane jest na gruncie filozofii politycznej. Do współczesnej myśli politycznej pojęcie tyranii większości wprowadził Jan Stuart Mill. Autor ten uznaje ją za budzącą większą grozę, niż inne tyranie, pomimo tego, że nie szafuje ona tak srogimi karami. Tyrania większości pozostawia mniej dróg ucieczki jednostce, jest bardziej wszechogarniająca i sięga o wiele dalej w życie prywatne obywateli[224]. Obywatele tworzą wówczas w toku cyklicznych referendów prawa korzystne, co prawda dla każdego z osobna, lecz destrukcyjne z punktu widzenia całości politycznych i społecznych[225]. Wizję możliwej patologizacji demokracji wskutek powstania i utrzymywania się tyranii większości analizuje Richard K. Moore. Jeśli lud ulegnie kuszącej wizji bezpośredniego sprawowania władzy politycznej, wówczas efektem będzie nie tylko chaos polityczny, lecz również poważne naruszanie i niszczenie ładu społecznego i ekonomicznego[226]. E-demokracja plebiscytarna przypomina stan, w którym pozbawiono władzy oficerów na statku i o jego kursie decydują głosujący pasażerowie[227].

Część autorów wyraża obawy, że wdrożenie internetowego głosowania mogłoby stać się czynnikiem atrofii demokracji przedstawicielskiej. Coraz bardziej skomplikowane procedury głosowania, nierównomierny poziom informatyzacji społeczeństwa, niepewne bezpieczeństwo i tajność głosu, banalizacja aktu głosowania oraz utrata bezpośredniej kontroli nad procesem wyborczym przez państwo i obywateli doprowadzić może do zniechęcenia do uczestnictwa w wyborach, politycznego cynizmu i obojętności, odmowy podejmowania jakichkolwiek wysiłków w sferze polityki, a więc do elektronicznej apatii (e-apatii).

Najbardziej pesymistyczny scenariusz przewiduje, że Internet może zostać wykorzystany w celu prowadzenia systematycznej i tajnej inwigilacji obywateli przez władzę, doprowadzając do powstania elektronicznego totalitaryzmu (e-totalitaryzm). Już teraz badacze przestrzegają przed pułapką interaktywnej polityki – zjawiskiem polegającym na doskona-

[223] F. Spagnoli, *Homo Democraticus. On the Universal Desirability and the Not So Universal Possibility and Human Rights*, Londyn 2003, s. 319.

[224] J.S. Mill, *O wolności*, Warszawa 1999.

[225] B.E. Cain, *The Internet in the (Dis)Service of Democracy*, „Loyola of Los Angeles Law Review" 2001, nr 40 (3), http://llr.lls.edu/volumes/v34-issue3/cain.pdf, s. 1005–1021.

[226] R.K. Moore, *Democracy and cyberspace*, [w:] *Digital Democracy*…, s. 50.

[227] M.L. Dertouzos, *What Will Be. How The New World of Information Will Change Our Lives*, Nowy Jork 1997, s. 216.

łym rozpoznaniu wyborcy dzięki jego uczestnictwie w sieci i dzięki temu możliwości manipulowania nim[228]. W literaturze przedmiotu często przywołuje się model Panoptykonu stworzony przez brytyjskiego myśliciela Jeremy'ego Benthama. Panoptykon to architektoniczny projekt budowli mieszczącej idealne więzienie, tak pomyślane, by strażnik mógł obserwować więźniów, sam nie będąc przez nich widziany[229]. Model ten dostarcza inspiracji współczesnym badaczom Internetu. Podobieństwo pomiędzy Panoptykonem a systemami nadzoru bezpośredniego wykorzystującymi Internet przedstawił między innymi Tom Bringall; głosi on nadejście Nowego Panoptykonu, nazwanego nowym ze względu na możliwość niezauważalnego śledzenia dowolnie wybranych użytkowników Internetu[230]. Z kolei David Lyon[231] oraz Mark Poster[232] nazywają przewidywany, przyszły stan rzeczy Superpanoptykonem. Według tych badaczy wizja wszechogarniającego nadzoru może się ziścić, ponieważ zniknęły bariery technologiczne, które dotychczas stały temu na przeszkodzie. Ciągłe i wszechstronne, monitorowanie życia obywateli przypuszczalnie, zdaniem D. Lyona, doprowadzi do powstania państwa nadzoru (*surveillance state*). Instytucja państwa na przestrzeni wieków zawsze rościła sobie pretensje do wszechwiedzy, lecz dopiero obecnie nowoczesne technologie pozwalają na praktyczną realizację tej wizji[233]. Autorzy wyróżniają dwie grupy zagrożeń, które w niedługim czasie mogą stać się fundamentem dla sprawowania totalitarnej kontroli nad społeczeństwem dzięki zastosowaniu internetowej technologii. Po pierwsze, są to programy monitorujące bieżącą działalność obywateli w Internecie, a po drugie – bazy

---

[228] K. Krzysztofek, *Polityka i demokracja w społeczeństwie informacyjnym. Wizje 'cyberdemokracji'*, [w:] J. Lubacz (red.), *W drodze do społeczeństwa informacyjnego*, Warszawa 1999, s. 87.

[229] Panoptykon został opisany przez J. Benthama w serii listów opublikowanych w 1791 roku: J. Bentham, *Panopticon or the Inspection House*, [w:] M. Bozovic (ed.), *The Panopticon Writings*, Londyn 1995, s. 29–95. Więcej na temat historii powstania koncepcji Panoptykonu oraz inspiracji nim współczesnych badaczy: C. Pease-Watkin, *Bentham's Panopticon and Dumont's Panoptique*, „Panoptikoa", http://eprints.ucl.ac.uk/archive/00000656/01/9.3cpwpan.pdf, 2002, s. 25–36 oraz s. Werret, Potemkin and the Panopticon: Samuel Bentham and the Architecture of Absolutism in Eighteenth Century Russia, http://eprints.ucl.ac.uk/archive/00000648/01/4.Potemkin_and_the_Panopticon.pdf, 1999.

[230] T. Bringall III, *The New Panopticon: The Internet Viewed as a Structure of Social Control*, „Theory & Science", 2002.

[231] D. Lyon, *The Electronic Eye. The Rise of Surveillance Society*, Minneapolis 1994, s. 37.

[232] M. Poster, *Critical Theory and Poststructuralism: In Search of a Context*, Nowy Jork 1989 oraz tenże, *The Mode of Information*, Cambridge 1990.

[233] D. Lyon, *The Electronic Eye…*, s. 31.

danych, do których trafiają informacje o wszelkich sferach ich życia[234]. W odniesieniu do pierwszej grupy zagrożeń można mówić o *omniprezencji* państwa, czyli jego wszechobecności dzięki systemowi elektronicznych oczu i uszu, zaś drugą grupę można określić mianem *omniscjencji*, to jest wszechwiedzy państwa o obywatelach, uzyskiwanej dzięki obrazowi każdego obywatela w elektronicznych bazach danych. Wyróżnione rodzaje zagrożeń nie wyczerpują potencjalnie istniejącego pola kontroli politycznej wskutek zastosowania nowych technologii[235]. Zagrożenia te Roger Clarke określa mianem *dataveillance*. Pojęcie to jest zestawieniem dwóch słów dane (*data*) oraz nadzór (*surveillance*) i oznacza nadzór sprawowany nad obywatelami za pomocą zbieranych o nich danych[236].

Groźba ziszczenia się scenariuszy pesymistycznych – e-demokracji plebiscytarnej, e-apatii, e-totalitaryzmu – skłaniałby do natychmiastowego zaprzestania prac nad głosowaniem z użyciem Internetu i jednocześnie zaniechaniem rozwijania innych form uczestnictwa obywateli w polityce za pośrednictwem tego medium. Z drugiej strony obietnice wzmocnienia demokracji przedstawicielskiej, a nawet wdrożenie na szerszą skalę form demokracji bezpośredniej sprawiają, że ryzyko wydaje się warte podjęcia. Eksperci próbując odnaleźć się między dwiema skrajnymi wizjami – wdrożenia lub zakazania głosowania za pośrednictwem Internetu – proponują, by rozwijać tę technologię, ale w sposób ściśle ograniczony, na niewielką skalę[237]. Rozwiązanie to nazywają „trzecią drogą" rozwoju internetowego głosowania. Polega ona na tym, by głosowanie z użyciem Internetu wdrażać w niewielkim zakresie – testować je na grupach takich jak niewidomi, znajdujący się za granicą, chorzy przebywający stale w domach[238]. Stosowanie eksperymentów o niewielkim zasięgu i w wyborach o mniejszym znaczeniu politycznym, w ściśle kontrolowanych warunkach, pozwoliłoby na wyeliminowanie odkrytych i poznanie jeszcze nieujawnionych zagrożeń. Warto przy tym pamiętać o istotnych

[234] A. Giddens, *The Nation State and Violence*, Berkeley 1987, s. 14–15, 175 i n. Podobny podział zaproponowali polscy badacze w artykule: P. Mazurek, J.M. Zając, K. Rakocy, *Między inwigilacją a uwiedzeniem. Użytkownicy Internetu wobec praktyk gromadzenia i przetwarzania danych*, „Studia Socjologiczne" 2007, nr 3 (186), s. 147–148.

[235] Potencjalne, przyszłe zagrożenia związane z nowoczesnym technologiami identyfikuje w raporcie dla Parlamentu Europejskiego: S. Wright, *An Appraisal of Technologies of Political Control*, http://www.statewatch.org/news/2005/may/steve-wright-stoa-rep.pdf, 6.01.1998.

[236] R. Clarke, *The Resistable Rise of the National Personal Data System*, „Software Law Journal" 1992, nr 5, s. 29–59.

[237] R.M. Alvarez, T.E. Hall, *Point, Click & Vote*…, s. 14.

[238] Tamże, s. 27.

cechach Internetu, które warunkują powodzenie tego typu przedsięwzięć – wdrażanie nowych rozwiązań powinno odbywać się siłami nie tylko państwa (tzw. strategia *top-down*), ale również obywateli i organizacji trzeciego sektora (strategia *bottom-up*), ze szczególnym uwzględnieniem zaawansowanych użytkowników Internetu.

Streszczenie

W niniejszym artykule podjęto próbę oceny wpływu głosowania przez Internet na demokrację przedstawicielską. We wstępie dokonano przeglądu występujących w literaturze przedmiotu pojęć związanych z elektronicznym głosowaniem, a także przeprowadzono analizę eksperymentów nad internetowym głosowaniem oraz ocenę ich efektów. Następnie przedstawiono argumenty wykorzystywane przez zwolenników tego sposobu głosowania. W kolejnej części artykułu omówiono bariery rozwoju wyborów z użyciem Internetu na trzech płaszczyznach: technicznej, społecznej i politycznej. Wyróżniono pięć scenariuszy ewolucji głosowania internetowego: elektroniczną demokrację przedstawicielską (e-demokrację przedstawicielską), elektroniczną demokrację bezpośrednią (e-demokrację bezpośrednią), elektroniczną demokrację plebiscytarną (e-demokrację plebiscytarną), elektroniczną apatię (e-apatię) i elektroniczny totalitaryzm (e-totalitaryzm).

Daniel Mider

Internet voting and democracy

Internet voting prospects of development and its' influence on representative democracy is the aim of analysis in hereby paper. In preface main terms and concepts of electronic voting used in the literature is ordered and defined. The first part of the article consists of Internet voting experiments review by country and evaluation of its effects. Analysis of arguments and expectations of remote Internet voting zealots is the main theme of the second part of the article. Subsequently the most important barriers for development of this way of voting is discussed on technical, social and political areas. Article ends with considerations about future of democracy in remote Internet voting context. Following types of possible long-term scenarios are marked out: representative electronic democracy (*representative e-democracy*), direct electronic democracy (*direct e-democracy*), electronic plebiscitary democracy (*plebiscitary e-democracy*), electronic apathy (*e-apathy*) and electronic totalitarianism (*e-totalitarianism*).