Daniel Mider, Olgierd Borówka

Internet – medium bez cenzury?

Słowa kluczowe:
socjologia Internetu, komunikowanie polityczne, cenzura polityczna, typologia cenzury politycznej, wolność słowa

W prezentowanym artykule przeanalizowano przebieg i efekty walki o wolny dostęp do informacji i komunikowanie się w Internecie. Walka o wpływy rozgrywa się pomiędzy obywatelami, organizacjami trzeciego sektora i ruchami społecznymi – z jednej strony, a państwami – z drugiej. W tym kontekście konieczne wydaje się postawienie następujących pytań badawczych: w jakim więc stopniu i w jakich formach podstawowa demokratyczna wartość, jaką jest wolność słowa, podlega w Internecie ograniczeniom? Jakie podmioty nakładają ograniczenia i jakie treści oraz kanały komunikacji tym ograniczeniom podlegają? Jakie pojawiły się metody oporu użytkowników Internetu wobec prób ograniczania wolności słowa w Internecie? Tak sformułowane pytania lokują problem w ramach rodzącej się subdyscypliny socjologii – socjologii Internetu[1].

Zastosowanie Internetu w sferze komunikowania politycznego rozbudziło wprawdzie nadzieje na wdrożenie ładu politycznego nowego typu – wyeliminowanie słabości współczesnych demokracji, stworzenie systemu rządów opartego na równorzędności stosunków pomiędzy rządzonymi i rządzącymi, zwiększeniu uczestnictwa obywateli w sprawowaniu rządów, a przede wszystkim transparencji władzy[2]. Andrew L. Shapiro

[1] R. Kling, *The Internet for Sociologists*, „Contemporary Sociology", 1997, nr 26 (4), s. 434–444.

[2] B.R. Barber, *Three Scenarios for the Future Technology and Strong Democracy*, „Political Science Quarterly", 1998–1999, nr 113 (4), s. 581–582; M. Castells, *Galaktyka Internetu. Refleksje nad Internetem, biznesem i społeczeństwem*, Poznań 2003; R.K. Moore, *Democracy*

ogłosił entuzjastyczną tezę o „rewolucji kontroli" (*control revolution*) – wskazywał, że dzięki potencjałowi komunikacyjnemu Internetu władza się rozprasza i przekazywana jest od elit do „końcowych użytkowników", czyli obywateli[3]. Internet pozwala przeciwstawiać się władzy, umożliwia agregację i mobilizowanie podobnie myślących, wspomaga tworzenie i dystrybucję niezależnej od władzy informacji, daje obywatelom poczucie mocy, słowem – istotnie narusza dotychczasową asymetrię sił pomiędzy władzą państwową a obywatelami[4]. Wielu badaczy wyraża obawy, że istnieją trwałe tendencje do monopolizacji każdego medium masowego przez elity rządzące ze względu na fakt, że media te stanowią istotne źródło dochodów oraz władzy; to w początkach istnienia nowożytnej demokracji środki masowego przekazu nazwano czwartą władzą[5]. Wszystkie media masowe podlegają – w jakimś stopniu – kontroli, nawet w systemie demokratycznym[6]. Koncepcję dotyczącą uzależniania i stopniowego zagarniania środków masowego przekazu przez elity władzy rozwinięto na gruncie ekonomii neoklasycznej[7]. Wraz z rozwojem różnych sposobów zapisu i rozpowszechniania myśli wykształciła się w społeczeństwach europejskich cenzura – praktyka kontrolowania i ograniczania informacji. Oznacza ona systematyczną kontrolę treści masowego medium komunikacyjnego za pomocą środków prawnych, administracyjnych, finansowych, kulturowych lub przemocy fizycznej. Na ogół współistnieje i jest wspomagana przez system propagandy; zazwyczaj cenzury dokonują rządzący lub elity polityczne, mogą też jej dokonywać inne podmioty. Cechą konstytutywną pojęcia cenzury jest sformułowanie *systematyczna* – na jego podstawie orzekamy, czy mamy do czynienia z cenzurą[8]. W literaturze przedmiotu istnieją dwa sposoby rozumienia pojęcia cenzury – wąskie

and cyberspace, [w:] B.N. Hague, B.D. Loader (eds.), *Digital Democracy. Discourse and Decision Making in the Information Age*, Routledge, Londyn, Nowy Jork 1999; A. Rothert, *Technopolis. Wirtualne sieci polityczne*, Warszawa 2003, s. 22.

3 A.L. Shapiro, *The Control Revolution*, Nowy Jork 1999, s. 13.

4 P. Gulda, *Internet w stosunkach między władzą a obywatelami*, [w:] P. Żuk (red.), *Media i władza*, Warszawa 2006, s. 280–293.

5 Pojęcie czwartej władzy wprowadził szkocki pisarz i historiozof Tomasz Carlyle nawiązując do wypowiedzi Edmunda Burke'a podczas debaty parlamentarnej w Izbie Gmin w 1787 roku: J. Schultz, *Reviving the fourth estate*, Cambridge 1998, s. 49.

6 T. Goban-Klas, *Granice wolności mediów*, [w:] Z. Bauer, E. Chudziński (red.), *Dziennikarstwo i świat mediów*, Warszawa 2008, s. 411.

7 M.E. Price, *Television: The Public Sphere and National Identity*, Nowy Jork 1995.

8 K.H. Youm, Hasło: *Freedom of the Press*, [w:] *International Encyclopedia of the Social and Behavioral Sciences*, N.J. Smelser, P.B. Baltes (eds.), Amsterdam 2001, s. 5775.

i szerokie. W węższym rozumieniu pojęcie to oznacza wyłącznie działania instytucji państwowych, natomiast rozumienie szersze – przyjęte na potrzeby niniejszego artykułu – obejmuje każde ograniczenie wolności słowa, niezależnie od podmiotu, który go dokonuje[9].

Słowo *cenzura* pochodzi z sanskrytu, w którym oznaczało 'wyliczać, odczytywać listę, ogłaszać, oznajmiać, zawiadamiać'; zaadaptowano je w postaci łacińskiego *censēre* w znaczeniu 'oceniać, szacować' lub 'osądzać'. W starożytnym Rzymie, od 443 roku p.n.e., funkcjonował obieralny i kadencyjny urząd cenzora (*censor*). Cenzor odpowiedzialny był za wykonywanie spisów ludności, szacowanie majątku obywateli oraz czuwanie nad ładem moralnym i obyczajowym (tzw. *regimen morum*)[10]. Cenzurę można określić mianem prawdy selektywnej. Jest to zjawisko odmienne od kłamstwa, bowiem kłamstwo wprowadza w błąd poprzez kreowanie fałszywych faktów. Natomiast prawda selektywna jest bardziej subtelna, polega na manipulowaniu kontekstem informacji oraz odpowiednio dobranymi i uporządkowanymi prawdami cząstkowymi[11]. W teorii demokracji przyjmuje się powszechnie, że pojęciem korelatywnym dla pojęcia cenzury jest pojęcie wolności słowa[12].

W literaturze przedmiotu spotyka się rozmaite typologie cenzury. Najczęściej rozróżnia się **cenzurę prewencyjną** i **cenzurę *post facto***[13]. Cenzura prewencyjna (uprzednia) oznacza ingerowanie w informację przed jej upowszechnieniem (*formal prepublication review*). Krytyczne dane są eliminowane, zanim zostaną udostępnione odbiorcom[14]. Jest to bardzo skuteczny sposób ograniczania wolności ekspresji, jednak ze względu na liczbę wytwarzanych we współczesnych społeczeństwach informacji, ta forma kontroli wolności słowa jest niemal niemożliwa do wdrożenia. Cenzura prewencyjna może być jednak stosowana efektywnie w odniesieniu do informacji z wąskich tematycznie obszarów. Ma ona swoją długą

---

[9] C. Munro, Hasło: *Censorship*, [w:] *The Blackwell Encyclopedia of Political Institutions*, V. Bogdanor (ed.), Oxford 1987, s. 78.

[10] *The Encyclopedia of Censorship*, J. Green (ed.), Nowy Jork, Oxford, Sydney 1990, s. 7.

[11] T. Strzyżewski, *Matrix czy prawda selektywna. Antycenzorskie retrospekcje*, Wrocław 2006, s. 16–17.

[12] C. Munro, *Censorship*, [w:] *The Blackwell Encyclopedia of Political Intuitions*, V. Bogdanor (ed.), Oxford 1987, s. 78.

[13] H.J. Abraham, *Censorship*, [w:] *International Encyclopedia of the Social Sciences*, W.A. Darity (ed.), Nowy Jork 1968, s. 356.

[14] G.T. Marx, hasło: *Censorship and Secrecy: Legal Perspectives*, [w:] *International Encyclopedia of the Social and Behavioral Sciences*, N.J. Smelser, P.B. Baltes (eds.), Amsterdam 2001, s. 1584–1585.

tradycję, praktykowano ją już w starożytności. Współcześnie korzysta się z niej doraźnie i wówczas motywuje się jej użycie zagrożeniem ładu społecznego, tzw. *clear and present danger*. W Stanach Zjednoczonych zasada ta została na gruncie prawa sformułowana w 1919 roku przez Sąd Najwyższy. Jest to usprawiedliwienie zakazu rozpowszechniania publikacji, jeśli państwo uzna je za niebezpieczne[15]. Amerykański system prawny przewiduje również możliwość utajniania przez państwo informacji. Tę kwestię reguluje prezydencki *Dekret 13526 o tajnych informacjach bezpieczeństwa narodowego* z 2009 roku[16]. Utajnienie informacji jest szczególnym rodzajem cenzury prewencyjnej, ponieważ podmiot rozpowszechniający naraża się nie tylko na wycofanie publikacji z obiegu, ale również na sankcje z zakresu prawa karnego. Istnieją również dwa inne sposoby dokonywania cenzury prewencyjnej: zmonopolizowanie kanałów przekazu przez rządzących, a także licencjonowanie i rejestracja kanałów przekazu lub jednostek zajmujących się obrotem informacji (redaktorów, dziennikarzy)[17]. Natomiast cenzura *post facto* obejmuje działania podejmowane po opublikowaniu informacji. Jej istotą jest negatywne sankcjonowanie podmiotów rozpowszechniających niedozwoloną informację. W państwach demokratycznych największe możliwości ograniczania treści prezentowanych w mediach zapewniają uregulowania dotyczące tajemnicy państwowej[18]. Kryterium sposobu dokonywania cenzury pozwala wyodrębnić **cenzurę bezpośrednią** i **pośrednią**. W pierwszym przypadku mamy do czynienia z jawną ingerencją w treść przekazu lub z jego blokowaniem. W przypadku cenzury pośredniej na przekaz wpływa się za pomocą miękkich technik oddziaływania – przykładem mogłoby być subsydiowanie prasy[19]. Tego typu cenzurę T. Goban-Klas nazywa pozacenzuralnymi

---

15 T. Goban-Klas, *Granice wolności mediów*, [w:] Z. Bauer, E. Chudziński (red.), *Dziennikarstwo i świat mediów*, Warszawa 2008, s. 412, 414.

16 *Executive Order – Classified National Security Information*, http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information, 01.09.2011.

17 G.T. Marx, *Censorship and Secrecy: Legal Perspectives*, [w:] *International Encyclopedia of the Social and Behavioral Sciences*, N.J. Smelser, P.B. Baltes (eds.), Amsterdam 2001, s. 1584–1585; K.H. Youm, *Freedom of the Press*, [w:] *International Encyclopedia of the Social and Behavioral Sciences*, Elsvier Science, N.J. Smelser, P.B. Baltes (eds.), Amsterdam 2001, s. 5776.

18 T. Goban-Klas, *Granice wolności mediów…*, s. 419.

19 K.H. Youm, *Freedom of the Press…*, s. 5776. Niektórzy badacze wskazują, że zjawisko to nosi znamiona cenzury, jednak doświadczenia szwedzkie wykazały, że istnieje nikła zależność pomiędzy subsydiowaniem prasy przez rząd, a niechęcią do jego krytykowania przez tę prasę.

formami kontroli mediów. Wskazuje, że są one zazwyczaj skuteczniejsze i w większym stopniu niż cenzura bezpośrednia obecne w państwach demokratycznych. Typowymi jej przejawami są naciski zorganizowanych grup (politycznych, wyznaniowych, kulturalnych) mające się prezentować jako spontaniczne oburzenie, lecz faktycznie będące zorganizowaną, uporządkowaną akcją. Może także przyjmować formę uzależniania mediów poprzez reklamodawców – szantażowanie wycofaniem drogich reklam. Tę drogę przyjmują najczęściej wielkie korporacje[20]. Rolę cenzury pośredniej odgrywają często przepisy dotyczące zniesławienia (*libel law*); badacze zauważają, że około 2/3 pozwów do sądów z tego tytułu dotyczy mediów masowych[21].

Z punktu widzenia potrzeb analizy zjawiska cenzury w Internecie najbardziej adekwatne wydaje się kryterium podmiotowe klasyfikacji cenzury. Według tego kryterium można wyróżnić **cenzurę publiczną** i **prywatną** (**państwową** i **pozapaństwową**)[22]. W pierwszym przypadku podmiotem dokonującym ingerencji w informację dystrybuowaną przez środki komunikowania masowego są instytucje państwowe w postaci specjalnie powołanych do tego wyspecjalizowanych organów lub instytucji sądowych i organów ścigania. W Polskiej Rzeczpospolitej Ludowej instytucją dokonującą cenzury wstępnej był Główny Urząd Kontroli Prasy, Publikacji i Widowisk funkcjonujący od 1945 do 1990 roku[23]. Cenzury drugiego typu dokonują podmioty prywatne: podmioty drugiego sektora – firmy, podmioty trzeciego sektora – stowarzyszenia oraz jednostki. Można wyróżnić trzy grupy tych podmiotów: dystrybutorów informacji dokonujących cenzury, twórców informacji dokonujących cenzury oraz odbiorców informacji dokonujących cenzury. Ze względu na podmiot dokonujący cenzury istotne jest także rozróżnienie między ingerencją w treści dokonywaną z zewnątrz (przez instytucję państwa, grupy społeczne, inne jednostki, etc.) a sytuacją, w której jednostka sama dokonuje ograniczenia swoich wypowiedzi w kanałach masowego przekazu z obawy przed możliwymi sankcjami prawnymi, politycznymi, społecznymi lub finansowymi. Takie zjawisko możemy nazwać **autocenzurą**.

[20] T. Goban-Klas, *Granice wolności mediów*…, s. 419.
[21] K.H. Youm, Hasło: *Freedom of the Press*…, s. 5777.
[22] H.J. Abraham, *Censorship*…, s. 356.
[23] T. Goban-Klas, *Granice wolności mediów*…, s. 417–418.

Metody ograniczania wolności słowa w Internecie

Szacuje się, że około jednej czwartej populacji internautów (25,3 proc., 1,72 miliarda) na całym świecie podlega jakimś formom cenzury[24]. Cenzura Internetu jest przede wszystkim praktykowana przez państwa totalitarne i autorytarne, jednak niektóre formy ograniczania wolności słowa występują również w demokracjach. Doroczny raport Reporterów Bez Granic (*Reporters Sans Frontiers*, *Reporters Without Borders*) dotyczący cenzury Internetu wymienia dwie kategorie krajów. Pierwszą kategorię nazywa wrogami Internetu, zaliczając do nich reżimy niedemokratyczne: Arabię Saudyjską, Birmę, Chiny, Egipt, Iran, Koreę Północną, Kubę, Syrię, Tunezję, Turkmenistan, Uzbekistan i Wietnam). Druga kategoria to kraje, w których społeczeństwa są nadzorowane (*under surveillance*), zaliczono do nich w 2010 roku także niektóre państwa uznawane za demokratyczne; społeczeństwa nadzorowane znajdują się w Australii, Bahrajnie, Białorusi, Erytrei, Korei Południowej, Malezji, Rosji, Sri Lance, Tajlandii, Turcji oraz Zjednoczonych Emiratach Arabskich[25]. Organizacja Reporterzy Bez Granic stosuje od 2002 roku Indeks Wolności Prasy (*Press Freedom Index*), przy tworzeniu którego cztery spośród 43 wskaźników poświęca Internetowi: stopień kontroli dostawców Internetu pośrednio lub bezpośrednio przez władze, odnotowane przypadki blokowania dostępu do stron lub interwencji w mechanizmy filtrowania w Internecie, przypadki zatrzymań twórców informacji w Internecie (blogerów, niezależnych dziennikarzy) oraz występowanie ataków lub kampanii dezinformacyjnych w stosunku do stron niezależnych i blogów[26].

---

[24] A. Lupetti, *Internet Censorship Report*, http://woorkup.com/2010/06/27/internet-censorship-report/, 07.2011.

[25] *Enemies of the Internet – Countries Under Surveillance*, Reporterzy Bez Granic, http://en.rsf.org/IMG/ pdf/ Internet_enemies.pdf, dostęp: lipiec 2011, s. 4, 39–62.

[26] Indeks Wolności Prasy (*Press Freedom Index*) mierzony jest na skali od 0 do 100, wartość najniższa oznacza najwyższą wolność prasy, a najwyższa – całkowite ograniczenie tej wolności. Indeks tworzony jest przez organizacje zrzeszone i korespondentów, obejmuje 178 państw świata. Indeks ten opiera się na subiektywnych odczuciach badaczy, dlatego mogą występować znaczne różnice w corocznych pomiarach. W ciągu ośmiu lat prowadzenia pomiarów średnia wyniosła 10,34 punktu; najlepszy wynik Polska uzyskała w 2003 roku (6,17 pkt.), najgorszy – w 2007 roku (18,50). W 2010 roku Polska uzyskała 8,88 pkt. Sytuację w Polsce uważa się za „satysfakcjonującą" pod względem wolności mediów. Reporters Without Borders, *Europe Falls From Its Pedestal, No Respite in the Dictatorships*, http://en.rsf.org/press-freedom-index-2010,1034.html, 07.2011; Reporterzy Bez Granic, *Questionnaire for Compiling the 2010 Press Freedom Index*, http://en.rsf.org/IMG/ pdf/cm_questionnaire_2010_gb.pdf, 07.2011.

Najbardziej rozpowszechnioną formą cenzury w Internecie jest cenzura instytucjonalna – państwowa[27]. Dokonuje się ona poprzez bezpośrednią ingerencję instytucji państwa w Internet, jak również ingerencję pośrednią – z użyciem rozmaitych sankcji. Obejmuje zarówno cenzurę prewencyjną, jak i cenzurę *post facto*. Analiza przypadków cenzury w Internecie pozwala na stworzenie klasyfikacji obejmującej następujące formy cenzury: 1) techniczne ograniczanie dostępu do Internetu (polegające na całkowitym lub częściowym zablokowaniu dostępu do Internetu); 2) penalizacja korzystania z określonych internetowych usług lub kanałów przekazu oraz zakaz rozpowszechniania określonych treści; 3) tworzenie finansowych, biurokratycznych i polityczno-społecznych barier dostępu do Internetu (poprzez wymóg rejestracji treści zamieszczanych przez użytkowników, zawyżanie cen dostępu do Internetu, a także działania pozaprawne – włamania na strony internetowe i blokowanie lub kasowanie ich treści oraz zastraszanie aktywnych użytkowników Internetu – blogerów, niezależnych dziennikarzy). Należy podkreślić, że cenzura w Internecie ma charakter przede wszystkim techniczny, znacznie mniejszą rolę odgrywają ograniczenia prawne oraz bariery finansowe, biurokratyczne i polityczno-społeczne oraz działania bezprawne, jak na przykład zastraszanie.

Spośród technicznych sposobów ograniczania dostępu do Internetu najmniejszych nakładów wymaga **całkowite zablokowanie dostępu do Internetu**. Jest to forma cenzury o najwyższym natężeniu[28]. Najgłośniejszym tego typu przypadkiem było odcięcie dostępu do egipskiego Internetu przez Muhammada Hosni Saida Mubaraka w czasie osiemnastodniowych protestów Egipcjan rozpoczętych Dniem Gniewu na przełomie stycznia i lutego 2011 roku przeciwko sytuacji społecznej i politycznej w kraju. Internet został odcięty na pięć dni, począwszy od 26 stycznia 2011 roku. Całkowite odcięcie dostępu do Internetu okazało się nieskuteczne, bowiem Egipcjanie użyli alternatywnych, starszych, niewymagających pod względem technicznym kanałów przekazu – Sieci 1.0[29]. Podobną tak-

---

[27] Porównaj: *Press Freedom on the Internet*, materiały zaprezentowane na *A Groundbreaking Conference Examining Issues of Press Freedom in the Internet Age*, 26–28 czerwca 2003, Nowy Jork, http://www.wpfc.org/site/docs/pdf/Publications/Working%20Papers-Conf%20Booklet.pdf, 07.2011, s. 1–39.

[28] K.H. Youm, hasło: *Freedom of the Press*…, s. 5775.

[29] E. Rauhalam, *Did Egypt Really 'Shut Off' the Internet?*, „Time NewsFeed", http://newsfeed.time.com/2011/01/28/did-egypt-really-shut-off-the-internet, 28.01.2011; R. Singel, *Egypt Shut Down Its Net With a Series of Phone Calls*, „Threat Level. Privacy, Crime And Security Online", http://www.wired.com/threatlevel/2011/01/egypt-isp-shutdown/,

tyką posłużył się rząd chiński w czerwcu 2009 roku, odcinając dostęp do Internetu autonomicznemu regionowi Xinjiang w północno-zachodnich Chinach[30]. Analogiczny sposób postępowania wobec społeczeństwa stosuje Erytrea, gdzie całkowicie odcina się dostęp do Internetu w sytuacjach zaburzeń ładu politycznego. Przypadki takie odnotowano także w Syrii – w trwających od marca zmaganiach, rząd zdecydował się 3 czerwca 2011 roku na odcięcie wszystkich usług internetowych[31]. Tymczasowe blokowanie dostępu do sieci może przerodzić się w stan permanentnego oddzielenia danej sieci od ogólnoświatowego Internetu. Takie tendencje występują w Korei Północnej. Jest ona praktycznie odcięta od Internetu, dostęp do niego mają poprzez łącza satelitarne tylko wysocy rangą uprzywilejowani urzędnicy. Na potrzeby studentów funkcjonuje Intranet, odcięty jednak od ogólnoświatowej sieci. Korea Północna nie wykorzystuje połączeń z ogólnoświatowym Internetem – pomimo że ICANN[32] asygnowała dla tego kraju kilkadziesiąt adresów IP i domenę .kp, to nie jest ona używana, nawet hosting strony rządowej Korei odbywa się na serwerze jednej z amerykańskich firm. Z analogiczną sytuacją mamy do czynienia na Kubie, gdzie istnieją równolegle dwie sieci: pierwsza z nich to niewielki, kubański (znajdujący się w domenie .ca) i składający się z nielicznych stron rządowych oraz internetowej encyklopedii Intranet, a druga to ogólnoświatowy Internet. Dostęp do ogólnoświatowej sieci możliwy jest na terenie zaledwie kilku hoteli (poprzez sieć bezprzewodową) oraz dla niektórych zaufanych funkcjonariuszy systemu. Podobna sytuacja dotyczy także Chin – chiński Internet jest fizycznie częściowo odcięty od reszty świata; funkcjonuje system przekierowań, który utrudnia użytkownikom korzystanie z zasobów zewnętrznych[33]. Tego typu zjawisko określa

28.01.2011; R. Szpunar, *Egipt blokuje Internet, aktywiści szukają alternatyw*, „IDG News Service", http://www.idg.pl/news/366773/egipt.blokuje.internet.aktywisci.szukaja.alternatyw. html, 31.01.2011; W. Szpunar, *Mubarak odszedł. Ile było w tym Facebooka?*, „IDG News Service", http://www.idg.pl/news/367157/mubarak.odszedl.ile.bylo.w.tym.facebooka.html, 14.02.2011.

30 R. Heacock, *China shuts down Internet in Xinjiang region after riots*, „OpenNet Initiative", http://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots, dostęp: 06.07.2009.

31 M. Chrobot, *Syria kolejnym krajem „wolnym od Internetu"*, „Komputer Świat", http://www.komputerswiat.pl/nowosci/wydarzenia/2011/22/syria-kolejnym-krajem-wolnym-od-internetu-internet!po-prostu-wyciagnieto-wtyczke.aspx, 04.06.2011.

32 *The Internet Corporation for Assigned Names and Numbers* – Internetowa Korporacja ds. Nadawania Nazw i Numerów zajmująca się przyznawaniem nazw domen internetowych.

33 Reporterzy Bez Granic, *Enemies of the Internet – Countries Under Surveillance*, http://en.rsf.org/IMG/ pdf/Internet_enemies.pdf, 07.2011, s. 11, 13, 22, 45.

się w literaturze przedmiotu mianem splinternetu (ang. *splinter* – 'rozszczepiać, rozłupywać'), a więc Internetu podzielonego pod względem technicznym, politycznym lub społecznym. W tym kontekście używa się także określenia wirtualnej kontrrewolucji lub bałkanizacji Internetu[34]. Jako przyczynę takiego podziału wskazuje się na ogół czynniki kulturowe, przede wszystkim niedostosowanie, w przeważającym stopniu anglojęzycznego Internetu, do potrzeb użytkowników używających alfabetów innych niż łaciński, przede wszystkim pisma chińskiego, w mniejszym stopniu alfabetu arabskiego oraz cyrylicy[35]. Potrzeby te to przede wszystkim zapisy nazw domen w wymienionych językach oraz brak znajomości przeważającego w Internecie języka angielskiego (87 proc. informacji zawartej w Internecie zostało zapisane w tym języku), a także zróżnicowane potrzeby techniczne oraz odmienne style użytkowania usług internetowych. Kraje takie jak Arabia Saudyjska, Bahrajn, Katar, Kuwejt i Zjednoczone Emiraty Arabskie opracowały eksperymentalne sieci niedostępne przez ogólnoświatowy Internet[36]. Na przykład Chiny oraz członkowie Ligi Państw Arabskich, a także Turcja utworzyły swoje własne domeny internetowe, których nazwy zapisywane są w alfabetach narodowych, przez co sieci te nie są dostępne dla przeciętnego europejskiego użytkownika. Podziały kulturowe są często tylko pretekstem – jak w wyżej opisanych przypadkach. Decydującą rolę odgrywają względy polityczne i ideologiczne. Jednakże, niezależnie od przyczyn podziału Internetu na mniejsze części, jednym z jego skutków jest utrata jednej z ważnych cech Internetu – transgraniczności. Efektem rozwoju tego zjawiska może być bałkanizacja całkowita, polegająca na podziale Internetu na odizolowane od siebie, zupełnie niezależne i wzajemnie niedostępne sieci. Techniczne ograniczanie dostępu do Internetu może polegać także na **blokowaniu kanałów przekazu, pojedynczych stron internetowych (konkretnych adresów), a także manipulowaniu słowami kluczowymi internetowych wyszukiwarek**. Taka forma cenzury ma bardziej subtelny

---

[34] *A virtual counter-revolution*, „The Economist", http://www.economist.com/node/16941635, 02.09.2010; R. Cichowlas, *Bałkanizacja Internetu*, „Gazeta.pl", http://www.kapitalizm.org/?action=show_article&art_id =472, 11.10.2011.

[35] D. Kulbaka, *Internet może się rozpaść na mniejsze sieci?*, „Webinside.pl", http://webmade.org/wiadomosci/ rozlam-internetu-onz.php, 12.10.2006. Wskazuje się także na politykę Stanów Zjednoczonych Ameryki Północnej w zakresie administrowania siecią jako przyczynę możliwego rozpadu Internetu: S. Butler, *The Evolution of Internet Interconnections*, http://www.2sparrows.org/Sean/rit/final%20thesis.pdf, 2000, s. 49 i nast.

[36] A. Mitraszewska, *Jak zapobiec bałkanizacji sieci*, „Gazeta.pl", http://gospodarka.gazeta.pl/gospodarka/1,33211,3125403.html, 22.01.2006.

charakter, jest mniej dostrzegalna i przez to stwarza większe możliwości do nadużyć ze strony państw. Jest ona nazywana cenzurą selektywną lub częściową (*selective*)[37]. Tego typu ograniczeń wolności słowa używają nie tylko państwa totalitarne i autorytarne, lecz także demokratyczne. Takie ograniczanie wolności słowa w Internecie może odbywać się na trzy sposoby[38]. Pierwsza z metod polega na uniemożliwieniu korzystania użytkownikom z wybranych kanałów internetowej komunikacji (na przykład z mikroblogów). Drugi sposób jest o wiele mniej zauważalny dla użytkowników – blokowane są pojedyncze strony internetowe lub fora dyskusyjne. Trzeci sposób jest niemal niewidoczny dla użytkownika i polega na takim filtrowaniu określonych haseł i słów kluczowych, w efekcie którego użytkownik nie otrzymuje w wynikach wyszukiwania żadnych danych na interesujący go temat lub uzyskuje nieadekwatne, spreparowane przez cenzorów.

Blokowanie kanałów internetowej komunikacji stosują w głównej mierze reżimy totalitarne i autorytarne. Działania takie polegają na uniemożliwieniu korzystania z określonego kanału komunikacji internetowej. Najczęściej blokowane są tak zwane serwisy społecznościowe oraz inne kanały komunikacji klasyfikowane jako Sieć 2.0, rzadziej fora internetowe. Wybór kanałów komunikowania nie jest przypadkowy – niektórych kanałów, a w szczególności mikroblogów oraz serwisów społecznościowych reżimy niedemokratyczne obawiają się ze względu na ich duży potencjał więziotwórczy i komunikacyjny. Irańskie protesty wywołane reelekcją Mahmouda Ahmadinejada zyskały swój niezwykły potencjał mobilizacyjny właśnie dzięki tym kanałom komunikacji; wydarzenia te określane są w świecie arabskim mianem „twitterowej rewolucji". Tego typu blokady zastosował także rząd egipski podczas protestów w Egipcie w styczniu 2011 roku. Zablokowane wówczas zostały: mikroblog Twitter, portal społecznościowy Facebook oraz usługa poczty elektronicznej dostępna przez strony www – Hotmail, co miało utrudnić lub nawet uniemożliwić – w zamyśle władz – sprawną mobilizację uczestników

[37] K.H. Youm, *Freedom of the Press…*, s. 5775.

[38] W literaturze przedmiotu najczęściej stosuje się techniczną klasyfikację sposobów blokowania treści i kanałów komunikacyjnych w Internecie (wyróżnia się najczęściej: blokowanie adresów IP, filtrowanie DNS i przekierowania, filtrowanie adresów URL, filtrowanie pakietów, resetowanie połączeń), jednak z punktu widzenia celów analizy postawionych w niniejszym artykule takie porządkowanie zjawisk uznano za nieprzydatne, proponując własne. Global Internet Freedom Consortium (GIFC), *Internet Censorship: Overview of Advanced Technologies and Products*, http://www.internetfreedom.org/…/Defeat_Internet_Censorship_ White_ Paper.pdf, 21.10.2007, s. 3–4.

protestów[39]. W Chinach cyklicznie zdarzają się blokady określonych usług, głównie masowe odcinanie dostępu do wszystkich czatów i forów dyskusyjnych, zazwyczaj w czasie rocznic rozmaitych wydarzeń politycznych i społecznych, które potencjalnie mogą zmobilizować do działania przeciwników systemu. Rząd chiński może w łatwy sposób kontrolować i blokować zamieszczane w chińskim Internecie treści. Udało się to uzyskać w wyniku wdrożenia w 2000 roku projektu Złota Tarcza (potocznie zwanego Wielką Chińską Ścianą Ogniową, *The Great Firewall of China*)[40]. Złota Tarcza uważana jest za najlepiej rozwinięty na świecie państwowy system blokowania i nadzoru sieci Internet. Sporadycznie zjawisko blokowania internetowych kanałów przekazu zdarza się w demokracjach. Na przykład niemiecka sieć telefoniczna T-Mobile ogłosiła zablokowanie usługi Skype, grożąc klientom, którzy spróbują z niej korzystać, zerwaniem umowy[41]. Jednak działanie to nie miało podłoża politycznego, lecz było podyktowane chęcią operatora do osiągania wyższych zysków. Jednym ze sposobów ograniczania dostępu do niektórych usług, szczególnie usług Sieci 2.0, wymagającej większej przepustowości łączy, jest obniżanie przez rządy szybkości łącz internetowych. Taka sytuacja miała miejsce w Iranie, gdzie obniżono szybkości łącza internetowego do zaledwie 256 kbit/s[42].

Częściej stosowanym zabiegiem jest **blokowanie stron internetowych**. W przypadku takich zabiegów użytkownikom trudniej rozpoznać manipulację ze strony władzy. Pierwsze przypadki blokowania dotyczą

---

[39] E. Rauhalam, *Did Egypt Really 'Shut Off' the Internet?*, „Time NewsFeed", http://newsfeed.time.com/2011/01/28/did-egypt-really-shut-off-the-internet/,28.01.2011; R. Singel, *Egypt Shut Down Its Net With a Series of Phone Calls*, „Threat Level. Privacy, Crime And Security Online", http://www.wired.com/threatlevel/2011/01/egypt-isp-shutdown/, 28.01.2011; R. Szpunar, *Egipt blokuje Internet, aktywiści szukają alternatyw*, „IDG News Service", http://www.idg.pl/news/366773/egipt.blokuje.internet.aktywisci.szukaja.alternatyw. html, 31.01.2011; W. Szpunar, *Mubarak odszedł. Ile było w tym Facebooka?*, „IDG News Service", http://www.idg.pl/news/367157/mubarak.odszedl.ile.bylo.w.tym.facebooka.html, 14.02.2011.

[40] Potoczna nazwa Złotej Tarczy – Wielka Chińska Ściana Ogniowa pochodzi od skojarzenia urządzenia nazywanego *Firewall* (zapora lub ściana ogniowa) stanowiącego rodzaj systemu obronnego dla sieci i systemów komputerowych z Wielkim Murem Chińskim. Więcej na temat tego projektu: G. Walton, *China's Golden Shield. Corporations and the Development of Surveillance Technology in the People's Republic of China*, http://www.dd-rd.ca/site/_PDF/publications/globalization/CGS_ENG.PDF, 2011.

[41] *T-Mobile blokuje Skype'a*, http://tech.wp.pl/kat,1009781,title,T-Mobile-blokujeSkypea,wid,11008032, wiadomosc.html?ticaid=180ce&_ticrsn=5, 03.04.2009.

[42] P. Drabik, *Cenzura w Internecie – tak to wygląda na świecie*, „Wiadomości24.pl", http://www.wiadomosci24.pl/artykul/cenzura_w_internecie_tak_to_wyglada_na_swiecie_124081-2--1-d.html, 07.2011.

Chin i zaistniały pod koniec lat dziewięćdziesiątych XX wieku. Obecnie blokowane są między innymi serwisy Voice of America i BBC News. Blokowane są także setki tysięcy stron internetowych należących do rządowej opozycji[43]. W Arabii Saudyjskiej zablokowano dotąd około pół miliona stron internetowych dotyczących religii oraz praw człowieka, w Turcji – blisko cztery tysiące. Z kolei w Syrii blokowane są strony pornograficzne, kurdyjskie oraz izraelskie[44]. Analogiczne praktyki stosują Zjednoczone Emiraty Arabskie oraz Egipt. Irańscy internauci nie mają dostępu do wielu serwisów, między innymi Amazon.com i IMDB.com[45]. Zdarzają się także przypadki blokowania pojedynczych stron. Na przykład w Turcji zablokowano serwis YouTube w maju 2008 roku wskutek rozpowszechniania przez ten kanał materiałów obrażających Mustafę Kemala Atatürka. Z kolei w Rosji zablokowano stronę Partii Narodowych Bolszewików (Nazbol.ru). W grudniu 2009 roku odcięta została czasowo strona rosyjskiego Ruchu Solidarność (www.rusolidarnost.ru)[46]. Na mocy prawa ustanowionego w 2008 roku australijski rząd przekazał swojej agencji Australian Communications and Media Authority (ACMA) pieczę nad treściami znajdującymi się w Internecie. Prowadzona jest konsekwentna polityka blokowania stron „na rzecz poprawy bezpieczeństwa w Internecie dla rodziny"[47]. Cenzurowane są informacje na temat dobrowolnej eutanazji, gry wideo (blokowane są strony z grami *online flash* oraz możliwość zakupu gier o zbyt dużej skali przemocy), a także inne treści. Prowadzony jest rejestr zakazanych stron[48]. Najczęstszym argumentem przemawiającym za blokowaniem poszczególnych stron internetowych jest hasło walki z terroryzmem. Podobnymi uzasadnieniami posługują się politycy europejscy. Komisarz sprawiedliwości i bezpieczeństwa Unii Europejskiej Franco Frattini w 2007 roku wezwał dostawców usług internetowych, by blokowali dostęp do stron, które uczą, jak konstruować

[43] Ze względu na liczbę stron internetowych i blogów blokowanych przez chiński rząd utworzono wyszukiwarki tych zablokowanych. Dzięki stronie http://www.greatfirewall.biz/ można sprawdzić, czy dana strona jest w Chinach blokowana. Patrz także: Global Internet Freedom Consortium (GIFC), *Defeat Internet Censorship: Overview of Advanced Technologies and Products…*; P. Drabik, *Cenzura w Internecie – tak to wygląda na świecie*, „Wiadomości24.pl", http://www.wiadomosci24.pl/artykul/cenzura_w_internecie_tak_to_wyglada_na_swiecie_124081-2--1-d.html, 07.2011.

[44] Reporterzy Bez Granic, *Enemies of the Internet – Countries Under Surveillance*, http://en.rsf.org/IMG/pdf/ Internet_enemies.pdf, 07.2011, s. 24, 26, 58.

[45] P. Drabik, *Cenzura w Internecie…*

[46] Reporterzy Bez Granic, *Enemies of the Internet…*, s. 5, 49, 58.

[47] P. Drabik, *Cenzura w Internecie…*

[48] Tamże.

bomby, a w Wielkiej Brytanii minister spraw wewnętrznych Jacqui Smith wezwała do zwalczania stron terrorystycznych[49].

Najtrudniejszym do wykrycia sposobem cenzurowania treści zamieszczanych w Internecie jest **zjawisko manipulowania słowami kluczowymi internetowych wyszukiwarek**. Ocenzurowane w ten sposób treści istnieją, nie są blokowane, lecz wyniki wyszukiwarek nie pokazują ich. Użytkownik, który nie zna ich adresu, nie może w żaden sposób zapoznać się z ich treścią[50]. Tego typu cenzurę rozwija Chińska Republika Ludowa. Liczne słowa kluczowe, wyszukiwane w chińskim Internecie, nie zwracają żadnych wyników lub zwracają niewłaściwe. Niektóre ze słów blokowane przez władze Chin to: demokracja, prawa człowieka, dyktatura, despotyzm, antykomunizm, bandyci komunistyczni, genocyd, czerwony terror, Dalai Lama, Tiananmen[51]. Analogiczne rozwiązania techniczne stosuje Iran[52]. Eksperci uważają, że technologie cenzury Internetu proliferują pomiędzy krajami niedemokratycznymi. Za głównego ich eksportera uważa się Chiny, które zaopatrują w oprogramowanie między innymi Białoruś, Kubę i Zimbabwe[53]. Za główną przyczynę takiego stanu rzeczy uważa się jednak współpracę pomiędzy chińskim rządem a amerykańskimi koncernami, które sprzedając ChRL nowoczesne technologie, umożliwiają rozwijanie coraz skuteczniejszych narzędzi cenzorskich. Tego rodzaju zarzuty stawia się od lat między innymi firmie Cisco Systems. Najnowsze oskarżenia pojawiły się w sierpniu 2011 roku. Wysunięte zostały przez pełnomocnika chińskiego dysydenta Du Daobina. Powód zarzuca korporacji współudział w tworzeniu systemu Złota Tarcza. Radca prawny firmy odpiera te zarzuty, twierdząc, że urządzenia sprzedawane przez Cisco do Chin w żaden sposób nie różnią się od tych, które oferowane są klientom w innych krajach[54].

---

[49] P. Kościński, *Czy w Internecie grozi nam cenzura*, „Rzeczpospolita", http://www.rp.pl/artykul/153063.html, 24.06.2008.

[50] J. Zittrain, B. Edelman, *Empirical Analysis of Internet Filtering in China*, http://cyber.law.harvard.edu/ filtering/china, 20.03.2003.

[51] Zainteresowany Czytelnik może się zapoznać z obszerniejszą, aczkolwiek nieenumeratywną listą słów filtrowanych przez system chińskiej internetowej cenzury pod adresem: *List of blacklisted keywords discovered by ConceptDoppler*, [w:] http://www.conceptdoppler.org/badwords.html, 19.09.2007.

[52] Reporterzy Bez Granic, *Enemies of the Internet*…, s. 18.

[53] C. Voeux, J. Pain, *Going Online in Cuba: Internet Under Surveillance*, http://www.rsf.org/IMG/pdf/rapport _gb_md_1.pdf, 07–08.10.2006, s. 1–6.

[54] J. Moe, *Suit says Cisco is helping China commit crimes*, http://marketplace.publicradio.org/display/web/2011/08/29/tech-report-lawsuit-says-cisco-helping-china-commit-crimes, 01.09.2011.

Rozpowszechnionym sposobem cenzurowania Internetu przez państwa jest **penalizacja używania określonych form internetowej komunikacji**. Z tego rozwiązania korzystają niemal wyłącznie reżimy autorytarne i totalitarne. Na przykład obowiązujące w Chinach prawo zakazuje użytkownikom Internetu korzystania z zagranicznych serwisów informacyjnych, dozwolone jest przeglądanie tych tylko stron internetowych, które są przez władze licencjonowane, ponadto chiński internauta nie może też założyć konta użytkownika na mikroblogu Twitter. Chińskie prawo nakłada też obowiązki na dostawców informacji w Internecie – są oni odpowiedzialni za zapewnienie zgodności z prawem wszelkich rozpowszechnianych informacji[55]. Z kolei w Birmie zakazane jest używanie usług poczty elektronicznej innych niż dostarczane przez rząd, w Syrii nie wolno korzystać z Facebooka, w Tunezji natomiast niedozwolone jest używanie takich serwisów, jak Youtube czy Dailymotion[56].

Innym sposobem ograniczania wolności słowa jest **zakaz rozpowszechniania informacji na określone tematy lub w określonej formie**. W tym przypadku trudno jest nakreślić granicę, po przekroczeniu której ochrona wartości kulturowych, religijnych oraz bezpieczeństwa państwa staje się cenzurą. Wydaje się, że z ewidentną sytuacją mamy do czynienia w Chinach i Egipcie. W ChRL liczba uwięzionych internautów w 2010 roku wyniosła 72 osoby; zostali oni oskarżeni o dywersję lub naruszenie tajemnicy państwowej. Z kolei w Egipcie nastąpiły w 2008 roku masowe aresztowania blogerów – do więzień trafiło ponad pięciuset internautów na podstawie ustawy o bezpieczeństwie państwa. Większość aresztowanych została zwolniona, jednak w więzieniu pozostaje znany bloger Abdel Kareem Suleiman posługujący się nickname'em Kareem Amer. Z kolei w Iranie w 2006 roku uchwalono prawo przeciwko przestępczości w Internecie, poddając penalizacji wypowiedzi godzące w islam, inne uznane przez państwo religie bądź pogwałcające wartości rodzinne. W Malezji obowiązuje drakońskie prawo pozwalające na przetrzymywanie podejrzanego bez procesu do dwóch lat na podstawie prawa o bezpieczeństwie wewnętrznym. Ponadto przewidywane są wysokie grzywny za naruszenie dóbr osobistych w Internecie – jest to równowartość około trzech tysięcy dolarów amerykańskich[57]. Na całym świecie odnotowywane są przypadki ograniczania wolności słowa wskutek **nadinterpretacji przepisów prawa lub mechanizmów postępowania sądowego**. Na przykład

[55] P. Drabik, *Cenzura w Internecie…*

[56] Reporterzy Bez Granic, *Enemies of the Internet…*, s. 5, 58.

[57] Tamże, s. 11, 15, 48.

w Tunezji w 2005 roku prawnik Mohamed Abbou został skazany na trzy i pół roku więzienia za opublikowanie w Internecie raportu, w którym oskarżył rząd tunezyjski o torturowanie więźniów[58]; na Kubie natomiast podjęto działania przeciwko „nieprawomyślnemu" blogerowi Orlando Luisowi Prado[59]. Z kolei prawo australijskie (na szczeblach lokalnych) nakazuje podpisywanie się pod komentarzami zamieszczanymi w Internecie imieniem i nazwiskiem – w przeciwnym razie orzekana jest grzywna w wysokości równej od tysiąca do prawie pięciu tysięcy dolarów amerykańskich[60]. W tym kontekście niepokój polskich internautów wzbudziło powołanie na początku lutego 2011 roku Parlamentarnego Zespołu ds. Promocji Wolności Przekazu i Poszanowania Zasad Dialogu Społecznego w Komunikacji. Użytkownicy Internetu obawiają się, że instytucja ta służy cenzurze w Internecie[61]. Według regulaminu Zespół ma na celu przeciwdziałanie ograniczaniu wolności słowa i swobody prezentowania opinii oraz ograniczenie agresji w Internecie i innych mediach. Członkowie zespołu będą powiadamiać organy ścigania o wypowiedziach internautów naruszających prawo; ochronie będą podlegać nie tylko politycy, lecz także na przykład lekarze i przedsiębiorcy. Tak spreparowana formuła działania zespołu jest w istocie próbą skuteczniejszego egzekwowania obowiązującego w Polsce prawa obecnego na gruncie konstytucji oraz kodeksu cywilnego[62]. Jednym ze sposobów ograniczania wolności słowa w Internecie jest **wymóg rejestracji treści zamieszczanych przez użytkowników**. Działania takie umożliwiają sprawowanie kontroli nad internautami i zapobiegają wywarzaniu się poczucia anonimowości. Skrajny wymóg rejestracji wprowadzono na przykład w Bahrajnie; od 2007 roku należy rejestrować wszystkie strony internetowe. Szczególny niepokój internautów wzbudzają próby regulowania przez państwo zasad

---

58 P. Drabik, *Cenzura w Internecie…*

59 Reporterzy Bez Granic, *Enemies of the Internet…*, s. 14.

60 Według badań niemal wszyscy Australijczycy (96 proc.) nie akceptują wprowadzonego w 2009 roku prawa. W dniach 28–29 stycznia 2010 roku odbył się masowy protest w australijskim Internecie przeciwko tym uregulowaniom – nastąpiło „zaćmienie Internetu". Reporterzy Bez Granic, *Enemies of the Internet…*, s. 39–40.

61 K. Jasiołek, *Posłowie ocenzurują Internet*, http://www.komputerswiat.pl/nowosci/internet/2011/05/poslowie-ocenzuruja-internet.aspx, 03.02.2011; L. Kolarska-Bobińska, *Jak PiS chce uporządkować Internet*, http://www.tokfm.pl/Blogi/1,110587,9040503,Jak_PiS_chce_porzadkowac_Internet.html, 02.02.2011.

62 *Regulamin Zespołu Parlamentarnego ds. Promocji Wolności Przekazu i Poszanowania Zasad Dialogu Społecznego w Komunikacji*, http://orka.sejm.gov.pl/opinie6.nsf/nazwa/dialog spoleczny/$file/dialogspoleczny.pdf, 07.2011.

funkcjonowania jednostek i grup w Internecie; postrzegane są na ogół jako formy cenzurowania. Tak zinterpretowane zostały przez polskich internautów zmiany wprowadzone w nowelizacji ustawy o radiofonii i telewizji nazywanej potocznie ustawą medialną[63]. Szczególny niepokój wzbudził nowy przepis głoszący, że każdy użytkownik prowadzący działalność gospodarczą i zamieszczający w Internecie materiały audiowizualne musi zarejestrować je w Krajowej Radzie Radiofonii i Telewizji (KRRiT). Polscy internauci podjęli protest przeciwko temu prawu na początku 2011 roku. Obrońcy zmian w ustawie twierdzą, że zakres podmiotowy obowiązywania przepisu jest bardzo wąski i obejmuje wyłącznie dostawców programów telewizyjnych na żądanie (tzw. *Video on Demand*, VOD), a nie wszystkich, którzy zamieszczają materiały wideo[64].

Za formę cenzury państwowej uważa się także **zawyżanie cen dostępu do Internetu**. Zabieg ten stosują przede wszystkim Chiny oraz Kuba. Opłata za godzinę korzystania z cyberkafejki z dostępem do Intranetu narodowego wynosi na Kubie ponad półtora dolara amerykańskiego, a sieci międzynarodowej około sześciu dolarów amerykańskich przy średniej miesięcznej pensji nieprzekraczającej dwudziestu jeden dolarów amerykańskich[65].

W ramach działań pozaprawnych stosowane są **włamania na strony internetowe i usuwanie lub zmiana ich treści**. Reporterzy Bez Granic donoszą o stosowaniu takich praktyk w Federacji Rosyjskiej. W styczniu 2010 roku dokonano ataku na stronę ingushetiyaru.org po tym, jak zamieszczono na niej ostatni wywiad z zamordowaną w lipcu 2009 roku aktywistką na rzecz praw człowieka Natalią Estemirową. Pojawiają się też informacje o przejmowaniu adresów e-mail dysydentów, a treści wiadomości przekierowywane są na nieznane adresy. Również w Chinach odnotowano tego typu przypadki – zlikwidowano wszelkie informacje na temat chińskiego dysydenta Liu Xiabao, po tym, gdy została przyznana mu Pokojowa Nagroda Nobla[66]. Innym sposobem ograniczania wolności słowa jest **zastraszanie aktywnych użytkowników Internetu – blogerów i niezależnych dziennikarzy**. O praktyki zastraszania internautów

---

63 *Ustawa o radiofonii i telewizji z dnia 29 grudnia 1992 r. o radiofonii i telewizji*, Dz.U. z 1993 r., Nr 7, poz. 34.

64 Szczegóły na stronie: *Wszystko o polityce w Polsce. Podziękuj premierowi*, http://www.podziekuj premierowi.pl/, 24.01.2011.

65 Reporterzy Bez Granic, *Enemies of the Internet*…, s. 8, 13.

66 ga, PAP, *Z chińskiego Internetu znika Liu Xiabao. W prasie propaganda*, http://wiadomosci.gazeta.pl/Wiadomosci/1,80569,8492635,Z_chinskiego_internetu_znika_Liu_Xiaobo__W_prasie.html, 11.10.2010.

oskarża się Rosję, Sri Lankę oraz Uzbekistan[67]. Jako próbę zastraszania odebrała internetowa społeczność Finlandii sytuację, w której internauta krytykujący działania fińskich organów ścigania i uregulowania prawne dotyczące ograniczeń w Internecie został umieszczony na policyjnej liście zakazanych stron internetowych zawierającej dystrybutorów pornografii dziecięcej[68].

Cenzura w Internecie dokonywana jest nie tylko przez instytucje państwa, lecz także przez dystrybutorów informacji (administratorów portali i wortali internetowych, forów dyskusyjnych, czatów, etc.), twórców informacji (blogerów, niezależnych dziennikarzy, aktywnych uczestników forów i czatów) oraz konsumentów internetowej informacji. Niektóre kanały internetowego przekazu podlegają cenzurowaniu przez administratorów, są to przede wszystkim moderowane (regulowane) fora i grupy dyskusyjne; w mniejszym stopniu takiej zdecentralizowanej regulacji podlegają treści zamieszczane w serwisach społecznościowych oraz na serwerach stron www. Moderacja oznacza, że administrator (moderator) ma prawo i obowiązek dokonywania ingerencji w treść komunikatów zamieszczanych przez dyskutujących. Ingerencja ta może się odbywać przed lub po opublikowaniu wypowiedzi użytkownika. W pierwszym przypadku wypowiedź nie jest udostępniana dyskutującym, dopóki nie zostanie zaakceptowana przez moderatora, a w drugim przypadku zmiany dokonywane są *ad hoc* na upublicznionym już materiale. Zakres moderacji w Internecie ogranicza rolę administratora do egzekwowania zasad przestrzegania tak zwanej netykiety[69] oraz regulaminu danego forum dyskusyjnego, grupy dyskusyjnej czy serwisu społecznościowego. Zasady dokonywania ingerencji w wypowiedzi użytkowników są ściśle określone na mocy wzorów subkultury Internetu: użytkownicy danego forum muszą być poinformowani, kto moderuje daną grupę, jakie są zasady jej moderowania (kryteria merytoryczne i formalne, jakie muszą spełniać zamieszczane informacje) oraz jakie są ewentualne przyczyny niezamieszczenia wypowiedzi lub

---

[67] Reporterzy Bez Granic, *Enemies of the Internet*…, s. 11, 35, 49.

[68] P. Kościński, *Czy w Internecie grozi nam cenzura*, http://www.rp.pl/artykul/153063.html, 24.06.2008.

[69] Netykieta stanowi zbiór zasad technicznych i wzorców kulturowych obowiązujących w interakcjach pomiędzy użytkownikami Internetu. Jest ona niezbyt konsekwentnie przestrzegana, rozmaicie interpretowana, częściowo tylko sformalizowana. Szerzej na ten temat: S. Hambridge, *RFC 1855. Netiquette Guidelines*, http://www.stanton.dtcc.edu/stanton/cs/rfc1855.html, 10.2010, strony nienumerowane; M. Moares, M. Horton, *Rules for posting to Usenet*, http://www.faqs.org/faqs/usenet/posting-rules/part1, 07.2010, strony nienumerowane.

ukazania się jej w formie okrojonej. W sytuacji, gdy moderator przekracza tak zdefiniowaną rolę, działa ekspansywnie – na przykład jako redaktor treści lub wychowawca użytkowników – wówczas można mówić o cenzurze. Motywacją takiego postępowania mogą być własne poglądy moderatora lub obawa przed poniesieniem sankcji rozproszonych lub formalnych, w szczególności ze strony państwa. Zwykli użytkownicy serwisów społecznościowych również mogą dokonywać swoistej cenzury. Takie wydarzenia miały miejsce na polskim Facebooku w przypadku konta blogerki Kataryny (Katarzyny Sadło) oraz kont krytycznych wobec prezydenta Bronisława Komorowskiego – „Wtopa Bronka", „Nie dla prezydentury Bronisława Komorowskiego", a także konta „Gówno prawda – nie czytam Gazety Wyborczej". Przeciwnicy zamieszczanych na wymienionych kontach treści masowo skorzystali z mechanizmu „Zgłoś nadużycie" i doprowadzili do ich zablokowania lub skasowania.

Zjawisko autocenzury dotyka również twórców informacji w Internecie; bardzo trudno określić jest jego skalę. Powstrzymywanie się od ekspresji swoich poglądów dotyczy wszystkich przejawów aktywności publicznej we współczesnych społeczeństwach – nie ogranicza się ono tylko do Internetu. Zjawisko autocenzury w demokracjach jest problemem nowym. W klasycznych teoriach demokracji nie brano pod uwagę tej kwestii, bowiem za głównego wroga wolności słowa uważano państwo; uważa się je za zagrożenie wolności słowa w demokracjach: „Cenzura może przybrać całkiem inną formę. Może odzywać się w nas echem, może się zagnieździć w nas, szpiegować nas niby prywatny, piszący pod dyktando sekretarz, który przypomina, aby nie posunąć się za daleko. Wewnętrzny cenzor ostrzega nas, że zbyt wiele ryzykujemy – naszą reputacją, rodziną, karierą, pracą czy postępowaniem prawnym przeciwko naszej firmie"[70]. We współczesnych demokracjach zjawisko autocenzury manifestuje się w ortodoksyjnie, dogmatycznie pojmowanych i często doprowadzanych *ad absurdum* działaniach społecznych określanych mianem politycznej poprawności (*political correctness*)[71], niekiedy

[70] J. Keane, *Media a demokracja*, Londyn 1992, s. 31, 33.

[71] Wprowadzenie do języka dyskursu publicznego i analiz politycznych pojęcia *polityczna poprawność* przypisywane jest w literaturze przedmiotu wielu autorom: Leaf Van Boen przyznaje pierwszeństwo Bolszewikom, u których politycznie poprawny oznaczało zgodny z linią partii, następnie zostało przyswojone w świecie zachodnim, zyskując przy tym wydźwięk ironiczny (określano nim ortodoksyjnych działaczy politycznych), aby w końcu zostać w latach osiemdziesiątych i dziewięćdziesiątych XX wieku przyswojone już w całkowicie poważnym znaczeniu przez ruch społeczny przeciwdziałający dyskryminacji ze względu na płeć, rasę i orientację seksualną. Patrz: L. Van Boven, *Pluralistic*

też nazywanych kulturową wrażliwością (*cultural sensitivity*)[72]. Polityczna poprawność, początkowo jako forma ruchu społecznego, a następnie jako konsekwentnie wdrażana polityka, pojawiła się w Stanach Zjednoczonych Ameryki Północnej w latach osiemdziesiątych i dziewięćdziesiątych dwudziestego wieku. Szczególnego znaczenia nabrała ona na politycznym forum publicznym oraz w środowisku akademickim, wpływając silnie również na inne dziedziny życia społecznego[73]. Polityczna poprawność jest rozumiana przede wszystkim jako pewien zbiór reguł użycia języka na forum publicznym[74], ale także jako zachowania i postawy wobec mniejszości narodowych, etnicznych, religijnych, seksualnych i innych[75]. Polityczna poprawność ma na celu wyeliminowanie określeń i zachowań znieważających lub poniżających wymienione grupy społeczne. Radykalna polityczna poprawność prowadzi do zjawiska, które określane jest mianem pluralistycznej ignorancji (*pluralistic ignorance*), to znaczy przecenienia jednomyślności otoczenia społecznego w zakresie oceny danej kwestii społecznej, podczas gdy dany pogląd podziela zaledwie mniejszość[76].

Ignorance and Political Correctness: The Case of Affirmative Action, „Political Psychology", 2000, nr 21 (2), s. 268. Odmienny pogląd na historię powstania tego pojęcia prezentują Jacek Bartyzel, a także Jadwiga Witek i Zbigniew Żmigrodzki, uważając za autora tego pojęcia antropologa kulturowego Franza Boasa, a popularyzatora (w znaczeniu ironicznym) – Dinesh D'Souza. Patrz: J. Bartyzel, *Polityczna poprawność*, http://konserwatyzm.pl/archiwum/index2.php?option=com_ content&do_pdf=1&id=1592, 07.2010, strony nienumerowane, a także J. Witek, Z. Żmigrodzki, *Polityczna poprawność w III Rzeczypospolitej*, Radom 2003, s. 12.

72 E. Andrews, *Cultural Sensitivity and Political Correctness: The Linguistic Problem of Naming*, „American Speech", 1996, nr 71 (4), s. 389.

73 C.R. Sunstein, *Sprzeciw w życiu społeczeństw*, Warszawa 2006, s. 159–161.

74 Słowniczki politycznie poprawnych słów i ich niepoprawnych politycznie odpowiedników zawierają artykuły: C. Ardelean, *The Challenge of Political Correctness in the Translation of „Sensitive" Texts*, „Nauczni trudowie na Rusenskija Uniwiersitet", 2008, nr 47 (5.3), http://conf.ru.acad.bg/bg/docs/cp/5.3/5.3-4.pdf, 07.2009, s. 27–28; L.N. Szapina, *Efemizmy w socialnych sfierach dejatelnosti: politkorrektonst' i «dieriewiannyj jazyk» (na primierie francuzkowo jazyka)*, „Bulletin of Adyghe State University: Internet Scientific Journal", 2008, nr 2 (677), http://vestnik.adygnet.ru/files/2008.2/677/Shapina2008_2.pdf, 07.2009, strony nienumerowane; E. Andrews, *Cultural Sensitivity and Political Correctness: The Linguistic Problem of Naming*, „American Speech", 1996, nr 71 (4) s. 389.

75 A. Szahaj, *E pluribus unum? Dylematy wielokulturowości i politycznej poprawności*, Universitas, Kraków 2004; C.R. Sunstein, *Sprzeciw w życiu społeczeństw*, Warszawa 2006, s. 159–161; J. Cohen, *Freedom of Expression*, „Philosophy and Public Affairs", 1993, nr 22 (3).

76 L. Van Boven, *Pluralistic Ignorance and Political Correctness: The Case of Affirmative Action*, „Political Psychology", 2000, nr 21 (2), s. 268.

Powstawanie zjawiska pluralistycznej ignorancji może zostać przedstawione według następującego schematu: 1) w ramach danej społeczności jej członkowie pragną pozostawać w dobrych relacjach i cieszyć się dobrą reputacją swoich współziomków; 2) zasadą realizowaną w danej społeczności jest wykluczanie lub pozbawianie dobrej reputacji tych jej członków, którzy wspólnie podzielane wartości podważają; 3) zatem jeśli dana jednostka oceni, że dany pogląd może być niepopularny, a więc pozbawić ją dobrej reputacji, to pomimo posiadania skrystalizowanych poglądów na daną kwestię nie wypowie ich[77]. Schemat procesu autocenzury jest tożsamy z konkluzjami płynącymi z klasycznych eksperymentów przeprowadzonych przez Salomona E. Ascha, a także Muzafera Sherifa, dotyczących informacyjnego konformizmu grupowego. Mechanizm działania radykalnej politycznej poprawności polega na stosowaniu etykietowania *ad hominem* – na podstawie wypowiedzi jednostki wnioskujemy, kim jest, a więc na przykład przeciwnik afirmatywnej akcji to zapewne rasista, niezależnie od tego, czy jego argumenty przeciw mają charakter racjonalny czy nieracjonalny, rasistowski czy nierasistowski, nie ma on prawa uczestniczyć w dyskursie[78]. Jednostki w obawie przed utratą reputacji, przed etykietowaniem, nie biorą udziału w publicznej dyskusji, autocenzurują swoje wypowiedzi, oddzielają publicznie prezentowane poglądy od tych wypowiadanych prywatnie. Opisany wyżej mechanizm doprowadza do atrofii sfery publicznej, upadku dyskursu, niszczy więź społeczną i kulturę zaufania w społeczeństwie, a także doprowadza do stanu, w którym nie widać głębokich być może podziałów i polaryzacji, bo nie są one ujawniane w trakcie publicznej debaty w danym społeczeństwie[79].

Metody oporu wobec ograniczeń wolności słowa w Internecie

Cenzura prowadzona w Internecie przez państwa wywołuje żywe reakcje internautów. Społeczność użytkowników Internetu stara się na różne sposoby odzyskać kontrolę nad wolną ekspresją i przepływem informacji w Internecie. Wyróżnić można trzy grupy podejmowanych działań:

---

77 S. Morris, *Political Correctness*, „The Journal of Political Economy", 2001, nr 2, s. 233.

78 G.C. Loury, *Self-Censorship in Public Discourse: A Theory of 'Political Correctness' and Related Phenomena*, http://www.econ.brown.edu/fac/Glenn_Loury/louryhomepage/teaching/Ec%20137/Ec%20137%20new%20material/material_2004/Ratsocty.pdf, 07.2009, s. 8.

79 C.R. Sunstein, *Sprzeciw w życiu społeczeństw*…, s. 159–161.

po pierwsze, tworzenie i rozpowszechnianie narzędzi informatycznych umożliwiających łamanie cenzury Internetu oraz bezpieczną i efektywną wymianę poglądów i informacji; po drugie, tworzenie w Internecie miejsc umożliwiających zamieszczanie i przechowywanie niecenzurowanych informacji oraz łamanie ograniczeń wolności słowa poprzez ujawnianie cenzurowanych informacji oraz – po trzecie – działania o charakterze propagandowym i edukacyjnym, promującym wolność słowa w Internecie, ujawniającym przypadki cenzury i innych nadużyć ograniczających wolność słowa. Podstawowym sposobem łamania cenzury w Internecie jest tworzenie i rozpowszechnianie narzędzi informatycznych umożliwiających znoszenie blokad informacyjnych oraz umożliwiających anonimową i efektywną wymianę poglądów i informacji. Do tego celu służą przede wszystkim programy zapewniające bezpieczeństwo użytkowników, pozwalające na ukrycie tożsamości i szyfrowanie danych. Istnieje wiele tego typu narzędzi – większość z nich jest dedykowana przez ich twórców społeczeństwom znajdującym się w państwach autorytarnych i totalitarnych. Jednym z najbardziej godnych zaufania narzędzi jest Freenet. Jest to darmowe oprogramowanie, które pozwala na anonimowe udostępnianie i ściąganie plików, publikowanie stron i blogów dostępnych wyłącznie dla użytkowników Freennetu (to znaczy niedostępnych w otwartym Internecie) oraz używanie czatów bez obawy przed cenzurą. Zasada działania Freenetu polega na udostępnianiu własnej przepustowości łącza i miejsca na dysku innym użytkownikom. Sieć jest całkowicie zdecentralizowana i nie ma żadnych instancji administracyjnych; dzięki temu jest ona odporna na próby identyfikacji użytkowników i ich lokalizacji. Ponadto jest ona niewrażliwa na zagrożenia wewnętrzne – uczestnik sieci Freenet nie jest w stanie stwierdzić, jakiego rodzaju treści przechowuje na swoim twardym dysku, oraz czego dotyczą transmisje przechodzące przez jego komputer. Sieć Freenet mogą zainstalować i obsługiwać nawet początkujący użytkownicy Internetu, jej obsługa nie wymaga zaawansowanych umiejętności informatycznych; tryb instalacji opatrzony został licznymi komentarzami pozwalającymi użytkownikowi uniknąć błędów grożących utratą bezpieczeństwa. Zasoby informacyjne dostępne we Freenecie nie są dostępne przez popularne wyszukiwarki lub katalogi internetowe, jak na przykład Google lub Yahoo. Freenet jest oprogramowaniem o otwartym źródle – jego kod źródłowy jest w całości dostępny[80]. Obecnie może on

[80] I. Clarke, *The Philosphy Behind Freenet*, http://www.meetopia.net/virus/pdf-ps_db/freenet-project_philosophy.pdf, 17.09.2008.

działać w dwóch trybach: Opennet i Darknet[81]. W pierwszym przypadku połączenia dokonywane są przez dowolnych użytkowników należących do sieci – zarówno tych znanych, jak i nieznanych użytkownikowi nawiązującemu połączenie, a droga przekazu wybierana jest automatycznie. Specyficznym trybem działania Freenetu jest Darknet polegający na ograniczeniu kontaktów wyłącznie do zaufanych, znanych uczestników; połączenia konfiguruje sam użytkownik i dlatego taka aktywność jest bardzo trudna do wykrycia. Sieć Darknet jest odizolowana od reszty sieci Freenetu; wymaga jednak co najmniej pięciu użytkowników, by ją utworzyć; wszelkie przekazy podlegają szyfrowaniu za pomocą mechanizmów kryptografii asymetrycznej. W tym celu łączące się ze sobą węzły muszą przed podjęciem komunikacji posiadać swoje wzajemne klucze publiczne oraz dane dotyczące położenia i konfiguracji; połączenia zarządzane są ręcznie, a nie automatycznie. Dzięki takiemu rozwiązaniu możliwe jest ukrycie faktu funkcjonowania Freenetu na danym komputerze. Freenet jest programem skutecznym, jak dotąd z powodzeniem używany jest on przez chińskich dysydentów; rząd chiński nie znalazł sposobu na monitorowanie takich połączeń. Jedynym sposobem zablokowania transmisji z użyciem Freenetu jest fizyczne odcięcie dróg przekazu. Podobnym programem, kompatybilnym z Freenetem (aczkolwiek stanowiącym odrębną sieć i niedzielącym z nim danych), był program Entropy[82]. Miał on większe możliwości techniczne i był szybszy w działaniu od Freenetu. Projekt ten nie jest już jednak rozwijany. Innym tego typu programem jest TOR (*The Onion Routing*) początkowo finansowany przez rząd Stanów Zjednoczonych; w 2004 roku pracę nad nim przekazano organizacjom pozarządowym – Electronic Frontier Foundation, a następnie Tor Poject. Program TOR minimalizuje ryzyko podsłuchu oraz ujawnienia tożsamości użytkowników. Informacje przesyłane są losowymi drogami z użyciem mechanizmu zacierania śladów; nie jest to jednak w pełni bezpieczny mechanizm – niektóre sposoby komunikacji zwiększają ryzyko zlokalizowania użytkowników[83]. Program ten jest szeroko stosowany przez dysydentów w państwach autorytarnych i totalitarnych na całym świecie,

---

[81] Omówienie technicznych aspektów funkcjonowania Freenetu zawierają artykuły: P. Bijata, *Odkryj tajny Internet*, „PC Format", http://www.pcformat.pl/Odkryj-tajny-internet,a,1736,strona,1, 07.06.2011; I. Clarke, S.G. Miller, T.W. Hong, O. Sandberg, B. Wiley, *Protecting Free Expression Online with Freenet*, IEEE Internet Computing, styczeń-luty 2002, s. 40–49; M. Mahdian, *Fighting Censorships with Algorithms*, http://www.mahdian.org/censorship.pdf, 07.2011.

[82] Nazwa Entropy jest to akronim *Emerging Network To Reduce Orwellian Potency Yield*.

[83] *The Onion Router (TOR)*, https://www.torproject.org/about/overview.html.pl, 08.2011.

używany jest też przez Stany Zjednoczone jako narzędzie prowadzenia białego wywiadu, a także – coraz częściej – w celach przestępczych[84]. Inne, niekiedy polecane programy i sposoby szyfrowania danych i ukrywania swojej tożsamości, nie są tak bezpieczne jak wyżej wymienione. Na przykład popularny i prosty sposób łączenia komputerów poprzez tunelowanie VPN (*Virtual Private Network*), co prawda utrudnia znacznie podsłuchiwanie danych, ale ujawnia ilość, chronologię komunikacji oraz geolokalizację użytkowników. Wśród licznych narzędzi służących do zapewniania bezpieczeństwa i dostępu do cenzurowanych informacji w sieci można wymienić również programy i sieci takie jak Gnunet, I2P, MUTE Network czy Triangle Boy (w tym ostatnim przypadku władze chińskie opracowały sposób jego blokowania) oraz co najmniej kilkanaście innych programów anonimowych serwerów *proxy*. Na uwagę zasługuje w tym kontekście także projekt rządu amerykańskiego rozpowszechniania systemu alternatywnych połączeń z Internetem omijających cenzurę miejscowych sieci telekomunikacyjnych. Opracowano niewielkich gabarytów, przenośne zestawy umożliwiające przekazywanie szyfrowanych danych poza systemem sieci nadzorowanym przez dane państwo[85].

Ważnym aspektem walki z cenzurą jest **możliwość dostarczania informacji bez ujawniania tożsamości i lokalizacji nadawcy**. Można tego dokonać dzięki wykorzystaniu programów nazywanych anonimowymi remailerami, jak na przykład Cypherpunk, Mixmaster, Mixminion lub pseudoanonimowymi remailerami, jak na przykład Penet. Programy te zapewniają twórcy możliwość całkowitej lub częściowej anonimowości (przesyłanie lub publikowanie pod pseudonimem) przy przesyłaniu informacji i publikacji pocztą e-mail.

W walce z cenzurą wykorzystywane są także **techniki ukrywania informacji w przesyłanych przekazach**: fotografiach, plikach dźwiękowych i filmach. Niewidoczny komunikat może być w zasadzie umieszczony w każdym przekazie cyfrowym[86]. Technika ukrywania komunika-

---

[84] Przestępcze zastosowania sieci TOR były przyczyną interpelacji skierowanej do Ministerstwa Spraw Wewnętrznych i Administracji przez posła Platformy Obywatelskiej Krzysztofa Brejzę: K. Brejza, *Interpelacja (nr 13631) do ministra spraw wewnętrznych i administracji w sprawie przeciwdziałania rozpowszechnianiu dziecięcej pornografii w Internecie*, https://pibn3ueheubjxv2z.tor2web.org/wiki/index.php/Interpelacja_Brejzy, 25.11.2009.

[85] prot, PAP, *„NYT": Internet w walizce oszuka cenzorów w krajach dyktatorskich*, http://www.tokfm.pl/Tokfm/1,103086,9771618,_NYT___Internet_w_walizce_oszuka_cenzorow_w_krajach.html, 12.06.2011.

[86] Krótkie wprowadzenie do techniki steganografii prezentuje Dorothy E. Denning: D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 355–359.

tów w przekazach wizualnych nazywana jest steganografią (gr. *steganos* – 'ukryty' oraz gr. *graphos* – 'piszę'), a w przekazach dźwiękowych – steganofonią[87]. Deszyfrowanie takich komunikatów nazywane jest steganalizą, przez analogię do kryptoanalizy. Istnieją w sieci Internet liczne darmowe i odpłatne programy służące do szyfrowania i deszyfrowania tego typu informacji, jednak ich funkcjonalność jest niezadowalająca w porównaniu z innymi narzędziami zapewniającymi bezpieczeństwo.

Omijanie blokad nakładanych przez państwa na określone usługi i witryny stanowi popularny sposób walki z cenzurą w Internecie. W najprostszy sposób można tego dokonać za pomocą programu Web2Mail. Program ten pełni funkcję pośrednika pomiędzy zakazaną stroną internetową a użytkownikiem. Użytkownik wysyła list elektroniczny na adres serwera Web2Mail z wpisanym w treści listu adresem zakazanej strony oraz specjalną instrukcją. Stronę internetową o podanym adresie otrzymuje w liście zwrotnym. Program ten oparty został na założeniu, że o ile zablokowanie dostępu do strony internetowej jest łatwe, o tyle przeskanowanie zawartości poczty elektronicznej i tam wykrycie blokowanych informacji jest o wiele trudniejsze, bardziej pracochłonne i czasochłonne. Drugi sposób polega na dostępie do blokowanych stron internetowych za pośrednictwem neutralnych (to jest nieblokowanych) adresów internetowych. Wiele organizacji oferuje taką możliwość z myślą o walce z cenzurą informacji w Internecie. Najpopularniejsze są programy Peekabooty oraz Psiphon. Program Peekabooty został udostępniony społeczności internautów w lipcu 2001 roku przez cenione postacie subkultury hakerów – członków grupy Cult of the Dead Cow: pomysłodawcy programu OxBlooda Ruffina oraz programistów Paula Baranowskiego i Joey'a De Villa. Zasada działania Peekaboty opiera się na zdecentralizowanej sieci dobrowolnych uczestników, którzy na swoich komputerach uruchamiają specjalne oprogramowanie. Droga przesyłania informacji pomiędzy uczestnikami takiej sieci wybierana jest losowo, a informacje dotyczące drogi przepływu informacji nie są w przesyłanych danych przechowywane. Taki system zapewnia anonimowość wszystkich użytkowników – zarówno pobierających daną informację, jak też uczestniczących w ich przekazywaniu oraz uniemożliwia rozpoznanie, z jakich zasobów Internetu korzystają końcowi jej użytkownicy (tę właściwość zapewnia system

[87] Warto wspomnieć o polskim wkładzie w rozwój tej techniki. Inżynierowie z Instytutu Telekomunikacji Politechniki Warszawskiej Krzysztof Szczypiorski i Wojciech Mazurczyk opracowali oryginalny sposób ukrywania treści w komunikatach VoIP (*Voice over Internet Protocol*). M. Minta-Kobus, *Sposób na tajne rozmowy w sieci*, http://nauka.dziennik.pl/hitech/artykuly/129063,sposob-na-tajne-rozmowy-w-sieci.html, 04.06.2008.

szyfrowania danych). Rozwiązania techniczne zastosowane w programie Peekabooty uniemożliwiają również blokowanie programów przez stosujących cenzurę, ponieważ program ten wykorzystuje porty używane przez popularne usługi internetowe. Ich zablokowanie byłoby tożsame z całkowitym odcięciem od Internetu[88]. Peekabooty od początku swego istnienia budził wielkie nadzieje na złamanie cenzury w krajach, w których Internet jest blokowany. Z kolei Psiphon działa na podobnych zasadach. Ideą jego twórców – Citizen Lab działającego na Uniwersytecie w Toronto było stworzenie darmowego, łatwego w instalacji oprogramowania zapewniającego użytkownikowi bezpieczeństwo, anonimowość i możliwość omijania filtrów nakładanych na treści w Internecie. Zasada działania programu Psiphon opiera się na mechanizmie pośrednika, to jest komputera, na którym zainstalowany jest specjalny program. Zainteresowani uzyskaniem anonimowego połączenia łączą się z tym komputerem i za jego pomocą uzyskują dostęp do dowolnych zasobów sieci. Połączenie jest szyfrowane, zatem cenzorzy wiedzą tylko, że dany komputer jest połączony z innym, nie wiedzą natomiast, jakie treści są pobierane[89].

Innym sposobem zwalczania ograniczeń wolności słowa w Internecie jest **tworzenie w nim miejsc umożliwiających bezpieczne zamieszczanie i przechowywanie niecenzurowanych informacji**. Takie miejsca określane są mianem rajów informacyjnych lub cyberrajów (*data haven, cyberhaven*) przez analogię do rajów podatkowych lub rajów korporacyjnych. W raju informacyjnym użytkownicy mogą bezpiecznie przechowywać swoje dane niezależnie od przepisów prawa obowiązujących w ich własnych krajach. Najczęściej służy on do przechowywania treści politycznych zakazanych przez władze państwowe, a także produktów informatycznych (programów użytkowych i gier) lub artystycznych (filmów, zdjęć) chronionych prawami autorskimi, względnie innej działalności uznawanej za nielegalną na określonym obszarze (na przykład wirtualne gry hazardowe lub pornografia). Raj informacyjny może być wykorzystywany zarówno w celach działalności politycznej, jak też celach przestępczych (terroryzm, pranie brudnych pieniędzy, handel narkotykami, pornografia dziecięca, łamanie praw autorskich). Raj informacyjny musi się charakteryzować trzema parametrami: bezpieczeństwem fizycznym, bezpieczeństwem prawno-politycznym oraz bezpieczeństwem informatycznym. Bezpieczeństwo fizyczne oznacza takie ulokowanie serwerów raju informacyjnego, które uniemożliwia fizyczny dostęp do nich organom

[88] *Cult of the Dead Cow*, http://w3.cultdeadcow.com/cms/, 07.2011.

[89] *Psiphon*, http://psiphon.ca/, 07.2011.

ścigania, oddziałom wojskowym lub sabotażystom. Z kolei stworzenie bezpieczeństwa prawno-politycznego wymaga ulokowania raju informacyjnego w miejscu, w którym istnieją uregulowania prawne umożliwiające gromadzenie i przechowywanie określonego rodzaju informacji, a także wystarczający stopień odporności na naciski dyplomatyczne. Osiągnięcie bezpieczeństwa informatycznego wymaga odpowiedniego poziomu zabezpieczeń czyniącego serwery raju informacyjnego niewrażliwymi na ataki lub infiltrację. Przykładem raju informacyjnego jest mikropaństwo Sealandia utworzone 2 września 1967 roku na opuszczonej platformie na Morzu Północnym u wybrzeży Wielkiej Brytanii przez emerytowanego majora armii brytyjskiej Roya Batesa. Państwo to, nieuznawane przez żadne inne, służyło jako raj informacyjny dzięki współpracy właściciela amerykańskiej firmy HavenCo Seana Hastingsa i Michaela Batesa – syna R. Batesa. Taka lokalizacja Sealandii – poza jurysdykcją państw związanych umowami międzynarodowymi – umożliwiła firmie oferowanie na serwerach treści o tematyce erotycznej, hazardowej oraz swobodne działanie społeczności hakerów[90]. Na przełomie 2006 i 2007 roku grupa Piratebay.org negocjowała zakup Sealandii w celu ominięcia obowiązującego w innych krajach – ich zdaniem nieadekwatnego dla doby Internetu – prawa autorskiego. Transakcja ta nie doszła do skutku. Sealandia została jednak sprzedana w 2007 roku, planowane jest wykorzystanie jej jako wirtualnego kasyna[91].

Wyjątkowy przykład raju informacyjnego stanowi serwis-organizacja WikiLeaks. Jej celem jest wspieranie idei jawności działań rządów i innych instytucji, w tym korporacji ponadnarodowych. Swoje działanie opiera na anonimowej skrzynce odbiorczej, z której skorzystać może każdy, kto ma dostęp do niejawnych dokumentów i informacji, które powinny, jego zdaniem, zostać upublicznione ze względu na szczególną wagę dla spo-

[90] Warto wspomnieć, iż na zaproszenie władz Sealandii na serwerach umieściła swoje strony organizacja Tibet Online, co tworzy interesującą sytuację z punktu widzenia prawa międzynarodowego. Żądania kierowane do Wielkiej Brytanii ze strony Chińskiej Republiki Ludowej nie odnoszą skutku, bowiem Sealandia leży poza jej terytorium. Z kolei oficjalne naciski skierowane do Sealandii uczyniłyby ją *de facto* państwem w rozumieniu prawa międzynarodowego. Więcej na ten temat: L.K. Talko, *Sealandia. Królestwo za koniak*, http://serwisy.gazeta.pl/df/1,34467,1811006.html, 08.12.2003 oraz tenże, *Raj cyberanarchistów*, http://serwisy.gazeta.pl/swiat/1,34174,1814216.html, 07.12.2003, a także oficjalna strona Księstwa Sealandii: http://www.sealandgov.org/, 07.2011.

[91] B. Hansen, *Sealand seeks to cash in on online casino bonanza. Fictitious nation to thumb nose at Cheney administration*, http://www.theregister.co.uk/2007/08/02/sealand_online_casino/, 02.08.2007; Ch.W. Moore, *Sealand Launches Offshore Online Casino*, http://www.applelinks.com/index.php/more/sealand_launches_offshore_online_casino/, 03.08.2007.

łeczeństwa. WikiLeaks sprawdza ich autentyczność, dokonuje obróbki danych, a następnie, przy pomocy dziennikarzy z przychylnych organizacji redakcji, tworzy na ich podstawie raporty, które pozwalają zwykłemu odbiorcy, to jest takiemu, który nie posiada fachowej wiedzy, zrozumieć czego dotyczą i dlaczego są istotne. Domena wikileaks.org zarejestrowana została w 2006 roku. Pomysłodawcą i głównym inicjatorem powstania WikiLeaks był australijski haker Julian Assange. Wiadomo o tym od 2007 roku, choć twórcy serwisu dbają o własną anonimowość na równi z anonimowością swych informatorów. Archiwa WikiLeaks zawierają w znacznej mierze dokumenty obnażające działania rządów, agencji wywiadowczych oraz wielkich koncernów. Upubliczniane przez organizację raporty niejednokrotnie stawały się przyczyną skandali politycznych i dyplomatycznych, a także katalizatorami rozwoju ruchów pacyfistycznych.

Do najgłośniejszych publikacji należy zaliczyć: nagranie z 12 lipca 2007 roku, ukazujące atak powietrzny na Bagdad, w którym śmierć poniosło wielu cywilów i dwóch dziennikarzy agencji Reutera, zbiór dokumentów *Dziennik z wojny afgańskiej* (*Afgan War Diary*), prezentujący przekrój działań militarnych podejmowanych przez amerykańskie wojska w tym kraju, analogiczny zbiór dotyczący wojny w Iraku, zatytułowany *Iraq War Logs,* na podstawie którego dziennikarze śledczy „The Guardian" stworzyli tak zwaną „mapę śmierci" (*death map*) oraz upubliczniane stopniowo, począwszy od listopada 2010 roku, archiwa amerykańskiej korespondencji dyplomatycznej wykradzionej z Departamentu Stanu, demaskującej negatywny lub lekceważący stosunek amerykańskiej dyplomacji względem sojuszników (tzw. *Cablegate*). WikiLeaks jest szczególnym przykładem cyberraju, ponieważ charakterystyczne dla tego typu miejsc parametry uzyskane zostały tu wyłącznie za sprawą szeregu działań w świecie wirtualnym oraz zabiegów prawnych, nie zaś, jak w przypadku Sealandii, dzięki fizycznemu istnieniu miejsca niepodlegającego jurysdykcji żadnego z państw. Warto bliżej się przyjrzeć, w jaki sposób WikiLeaks udało się spełnić kryteria definicyjne. O WikiLeaks jako cyberraju mówić można od 1 grudnia 2010 roku, kiedy archiwa organizacji przeniesiono z ulokowanych na terytorium Stanów Zjednoczonych serwerów firmy Amazon. Bezpieczeństwo fizyczne uzyskano dzięki lokalizacji danych na serwerach firmy Bahnhof, ulokowanych w bunkrze przeciwlotniczym Pionen na terytorium Szwecji. Status tego państwa na arenie międzynarodowej, głęboko zakorzeniona w jego polityce zewnętrznej idea neutralności oraz położenie geograficzne to najistotniejsze czynniki gwarantujące fizyczne bezpieczeństwo przechowywanych i upublicznianych informacji. Bezpieczeństwo prawno-polityczne osiągnięto również w konsekwencji

fizycznej lokalizacji danych na szwedzkich serwerach. W myśl zasad obowiązywania prawa wewnątrzkrajowego, działalność WikiLeaks regulowana jest przez prawo Królestwa Szwecji, w którego systemie normatywnym wolność słowa zajmuje szczególną pozycję – aż dwa z czterech aktów składających się na konstytucję tego kraju poświęcono swobodzie wypowiedzi. Są to: *Akt o wolności druku* z 1949 roku oraz *Akt o wolności wypowiedzi* z 1991 roku. Nie wynika z tego jednak, że Szwecja sama w sobie jest cyberrajem. Kraj ten ma bowiem bardzo restrykcyjne regulacje dotyczące ochrony praw autorskich i własności intelektualnej. Obostrzenia tego rodzaju nie mają jednak wpływu na działalność WikiLeaks, która nie zajmuje się piractwem komputerowym. Bezpieczeństwo informatyczne serwisu jest zaś efektem dwóch czynników. Pierwszy stanowi fakt, że założyciele i administratorzy wikileaks.org to w większości hakerzy, osoby doskonale znające się na zagrożeniach bezpieczeństwa danych, a zatem również na metodach walki z nimi. J. Assange już jako nastolatek włamywał się na serwery Pentagonu. Drugim czynnikiem jest z kolei ogromna liczba rozsianych po świecie kopii całych archiwów – tak zwanych *mirrors* – dzięki którym, w razie uszkodzenia serwerów z Pionen, dane pozostają dostępne w sieci.

Brak podmiotowości prawnomiędzynarodowej WikiLeaks może rodzić zastrzeżenia co do słuszności twierdzenia, że jest to cyberraj. Spełnianie kryteriów bezpieczeństwa oraz charakter działalności prowadzonej przez organizację zdają się być jednak mocnymi argumentami przemawiającymi za tą tezą.

Przyszłość WikiLeaks jest niepewna ze względu na wewnętrzny rozłam, jaki miał miejsce w szeregach organizacji. Część współpracowników J. Assange'a z byłym rzecznikiem WikiLeaks – Danielem Domscheit-Bergiem na czele postanowiła kontynuować działalność demaskatorską na własną rękę. Zarzucają oni J. Assange'owi zbyt duże zaangażowanie polityczne. Uważają, że uczynił on z WikiLeaks narzędzie gry politycznej, przy pomocy którego realizuje interesy własne i sprzyjających mu podmiotów. D. Domscheit-Berg założył na początku 2011 roku konkurencyjny dla WikiLeaks serwis – OpenLeaks[92]. Jest także autorem książki *Inside WikiLeaks: My time with Julian Assange at the World's Most Dangerous Website*. Niezależnie jednak od dalszych losów WikiLeaks, tendencja do

[92] H. Blodget, *WikiLeaks Defector Explains What's Wrong With WikiLeaks And Why He's Creating A New Site Called "OpenLeaks"*, http://www.businessinsider.com/wikileaks-defector-explains-whats-wrong-with-wikileaks-and-why-hes-creating-a-new-site-called-openleaks-2011-1, 08.2011.

powstawania podobnych cyberrajów jest wyraźnie zauważalna i pozwala przypuszczać, że ta forma walki o wolność słowa w Internecie nie stanowiła jednostkowego fenomenu.

Innym sposobem ochrony wolności słowa jest **dokonywanie ataków w proteście przeciwko cenzorom Internetu**. Najczęściej celem ataków stają się instytucje państwowe i korporacje. Najbardziej znanymi grupami działającymi na rzecz wolności słowa w Internecie w taki sposób są Anonymous oraz Lulz Security (LulzSec). Anonymous powstał w 2006 roku, należy traktować go jako swoisty ruch protestu, obecny w internetowych kanałach przekazu, który wykształcił własną, specyficzną subkulturę. Jego wartości ogniskują się przede wszystkim na wolności przepływu informacji w Internecie. Działania przyjmują przede wszystkim formę ataków typu odmowa dostępu usługi – DDoS (*Distributed Denial of Service*), włamań na serwery www i podmian stron internetowych (*web defacements*), kradzieży i rozpowszechniania wykradzionych informacji. Najpoważniejszymi ze względu na konsekwencje działaniami była rozpoczęta przez Anonymous w grudniu 2010 roku akcja poparcia na rzecz WikiLeaks. Początkowo działania odbywały się w ramach operacji „Odpłata" (*Payback*), a następnie pod kryptonimem „Pomścić Assange'a" (*Operation Avenge Assange*) w postaci ataków DDoS przeciwko serwisom Amazon, PayPal, MasterCard, Visa oraz szwajcarskiemu bankowi PostFinance[93]. Cele zostały wybrane ze względu na politykę tych firm wobec J. Assange. Na skutek ataków serwisy MasterCard i Visa przestały czasowo funkcjonować. Anonymous grozili także podjęciem działań przeciwko personelowi Quantico, gdy w tym więzieniu został osadzony w lipcu 2010 roku amerykański żołnierz Bradley E. Manning, prawdopodobnie odpowiedzialny za udostępnienie tajnych danych wojskowych serwisowi WikiLeaks[94]. 15 czerwca 2011 roku Anonymous zaatakowała blisko sto stron internetowych malezyjskiego rządu w odwecie za zablokowanie stron WikiLeaks i The Pirate Bay[95]. Celem ataku stały się także strony Zimbabwe i Tunezji na przełomie grudnia 2010 roku

[93] Oświadczenie zawierające wyjaśnienie motywów postępowania grupy znajduje się w: *Operation Avenge Assange*, https://uloadr.com/u/4.png, 08.2011.

[94] A. Greenberg, *Anonymous Hackers Target Alleged WikiLeaker Bradley Manning's Jailers*, http://blogs.forbes.com/andygreenberg/2011/03/07/anonymous-hackers-target-alleged-wikileaker-bradley-mannings-jailers/, 07.03.2011; S. Ragan, *Anonymous plans defense for Bradley Manning – promises a media war*, http://www.thetechherald.com/article.php/201109/6905/Anonymous-plans-defense-for-Bradley-Manning-promises-a-media-war?page=1, 04.03.2011.

[95] Ch. Albanesius, *Hackers Target Malaysian Government Sites*, „PC Magazine", 16 czerwca 2011, [w:] http://www.pcmag.com/article2/0,2817,2387108,00.asp, 07.2011.

i stycznia 2011 roku[96]. Zablokowanie stron rządowych w Zimbabwe było odpowiedzią na pozew żony prezydenta Grace Mugabe, która zażądała od miejscowej gazety odszkodowania za opublikowanie pochodzących z WikiLeaks materiałów na temat nadużyć finansowych pochodzących z WikiLeaks[97]. G. Mugabe zażądała od gazety „The Standard" 15 milionów dolarów zadośćuczynienia za szkody, jakie miał ponieść jej wizerunek wskutek postawienia jej fałszywych zarzutów. Pełnomocnik żony prezydenta określił oskarżenia padające na łamach gazety jako „fałszywe, skandaliczne i złośliwe"[98]. W tym miejscu warto zwrócić uwagę na fakt, że w rankingu Press Freedom Index z 2010 roku, Zimbabwe znajduje się na 123 pozycji (spośród 178 uwzględnionych państw), a gazeta „The Standard" była już przez lokalne władze represjonowana[99]. Anonymous byli również aktywni podczas wydarzeń na Bliskim Wschodzie określanych mianem arabskiej wiosny rozgrywających w 2011 roku. W ramach „Operacji Tunezja", 5 stycznia 2011 roku, za pomocą DDoS zaatakowano

[96] Ataki typu DDoS wykorzystują nieusuwalną słabość sieci Internet – 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. Sieć komputerów służąca do dokonywania tego typu działań, a uprzednio przejęta w sposób nieuprawniony, nazywana jest *botnetem* (jest to zbitek angielskich słów *bot* od robot oraz *net* od sieć). Pojedyncze 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. 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 znaczne straty. Potencjalnie atak DDoS jest łatwy do przeprowadzenia nawet przez średniozaawansowanego użytkownika za pomocą darmowego programu – na przykład LOIC autorstwa Praetox Technologies (*Loic Orbit Ion Cannon*) lub wersji tego programu, na przykład JS LOIC. Program dostępny jest pod adresem: *LOIC*, https://github.com/NewEraCracker/LOIC/, dostęp: lipiec 2011. Więcej na temat ataków typu DDoS: 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, 02.10.2007, s. 3.

[97] W. Szpunar, *Grupa Anonymous atakuje strony rządowe*, http://www.idg.pl/news/365763/grupa.anonymous.atakuje.strony.rzadowe.html, 05.01.2011.

[98] BBC, *Wikileaks: Grace Mugabe sues over diamond claims*, http://www.bbc.co.uk/news/world-africa-12007142, 02.09.2011.

[99] Tamże.

tunezyjski rząd. W efekcie wielu Tunezyjczyków przyłączyło się do cyberataków podczas tak zwanej jaśminowej rewolucji. Grupa ta jest także odpowiedzialna za ataki na egipskie strony rządowe podczas protestów na przełomie stycznia i lutego 2011 roku. Spośród innych aktywności Anonymous warto wymienić przyłączenie się do protestów przeciwko nadużyciom wyborczym w Iranie w czerwcu 2009 roku. Wraz z irańskimi hakerami oraz grupą The Pirate Bay umożliwili wolną od cenzury wymianę informacji pomiędzy Iranem a resztą świata na temat protestów, które wystąpiły po ogłoszeniu wyników wyborów. Podjęto także działania przeciwko wprowadzeniu cenzury Internetu w Australii – w lutym 2010 roku zaatakowano strony australijskiego parlamentu oraz niektórych ministerstw. Atak ten nie był tak silny jak typowe ataki DDoS, miał znaczenie przede wszystkim symboliczne. Aktywność Anonymous ma przede wszystkim charakter polityczny, ale podejmowane są również działania o charakterze społecznym, na przykład 20 maja 2009 roku grupa zorganizowała happening YouTube Porn Day, podczas którego w odwecie za usunięcie plików muzycznych z serwisu zamieściła w nim liczne filmy pornograficzne oznaczone jako przeznaczone dla dzieci, w 2008 roku zaatakowano Kościół Scjentologiczny a rok wcześniej doprowadzono za pomocą działań w cyberprzestrzeni do aresztowania pedofila Chrisa Forcanda. W czerwcu 2011 aresztowano w Hiszpanii trzech członków Anonymous, jednak nie przerwało to działalności ruchu[100] – 21 lipca zgłoszono, że Anonymous zaatakowali serwery Narodowej Agencji Bezpieczeństwa Stanów Zjednoczonych, wchodząc w posiadanie tajnych danych Paktu Północnoatlantyckiego[101], a na początku sierpnia grupa Anonymous w odwecie za aresztowanie swoich członków włamała się na strony internetowe kilkudziesięciu instytucji rządowych w Stanach Zjednoczonych, wykradając jednocześnie dane[102].

Grupa Lulz Security powstała w efekcie opuszczenia grupy Anonymous przez jednego z jej członków Ryana Cleary'ego; jest to jej domniemany lider i założyciel. LulzSec deklarują obronę praw człowieka, w tym przede wszystkim obronę wolności słowa, występują przeciwko korupcji i nadużyciom rządów państw oraz korporacji. Formuła działań grupy

[100] A. Steliński, *Trzech hakerów z grupy Anonymous w areszcie*, http://www.networld.pl/news/371871/ Trzech.hakerow. z.grupy.Anonymous.w.areszcie.html, 13.06.2011.

[101] OneIndia News, *Hacker group Anonymous attacks NASA servers*, http://news.oneindia.in/2011/07/21/tech-hacker-group-anonymous-attacks-nasa-servers-aid0102.html, 21.07.2011.

[102] POg, PAP, *USA: atak hakerów na 70 agencji i służb*, http://wiadomosci.onet.pl/swiat/usa-atak-hakerow-na-70-agencji-i-sluzb,1,4815000,wiadomosc.html, 07.08.2011.

zgodnie z jej nazwą przyjmuje charakter żartobliwy[103]. W swojej działalności skupiają się głównie na włamaniach na strony internetowe rozmaitych instytucji i podmianie ich treści, a także kradzieży informacji. Zamieszczane treści mają charakter surrealistycznych parodii. W mniejszym stopniu korzystają z ataków typu DDoS. Ofiarą ich ataków padły między innymi systemy informatyczne Senatu Stanów Zjednoczonych, Centralnej Agencji Wywiadowczej (CIA), Federalnego Biura Śledczego (FBI), tunezyjskiego i brazylijskiego rządu oraz brytyjskich instytucji państwowych: policji oraz Urzędu Statystycznego, a także licznych korporacji (m.in. Sony, HBGary). LulzSec nawiązali współpracę z Anonymous i innymi grupami w obronie J. Assange'a, tworząc koalicję Anti-Sec (*Operation Anti-Security*)[104]. Niektóre grupy subkultury hakerów postrzegają LulzSec nie jako obrońców wolności słowa, lecz jako zagrożenie dla tej wartości. Grupa TeaMp0isoN uważa, że LulzSec niepotrzebnie drażni władze państwowe, co może doprowadzić do ograniczenia swobody wymiany danych i działalności w Internecie. Lulz Security ogłosiła zakończenie swojej działalności po kilkudziesięciu dniach aktywności – w czerwcu 2011 roku[105]. Okazało się to jednak nieprawdą – działalność została wznowiona; włamano się na stronę internetowego wydania „The Sun" i zamieszczono tam w formie artykułu informację o śmierci właściciela koncernu medialnego Ruperta Murdocha[106].

Istotną rolę w walce z ograniczeniami wolności słowa w Internecie odgrywają **działania o charakterze propagandowym i edukacyjnym, promującym wolność słowa w Internecie, ujawniającym przypadki nadużyć**. Można mówić o wyłanianiu się swoistej kontestacyjnej, kontrkulturowej

[103] Źródłosłów nazwy Lulz Security to modyfikacja skrótu LOL – *Laughing Out Loud* – 'śmiać się na głos' lub *Lots of Laughs* – 'kupa śmiechu', a *for lulz* oznacza 'dla śmiechu'.

[104] A. Golański, *Z frontu cyberwojny: LulzSec przeciwko władzy, hakerskie podziemie przeciwko LulzSec, niewinnym się dostaje*, http://webhosting.pl/Z.frontu.cyberwojny.LulzSec.przeciwko.wladzy.hakerskie.podziemie.przeciwko.LulzSec.niewinnym.sie.dostaje?page=1, 22.06.2011; K. Jaskuła, *Grupa hakerska Lulz Sec zaatakowała stronę CIA*, http://www.pcworld.pl/news/372103/Grupa.hakerska.Lulz.Sec.zaatakowala.strone.CIA.html, 16.06.2011; kaien, *USA: hakerzy z LulzSec znów atakują*, http://tvp.info/informacje/swiat/usa-hakerzy-z-lulzsec-znow-atakuja/4764198, 25.06.2011.

[105] J. Weisenthal, *Notorious Hacker Group LulzSec Just Announced That It's Finished*, http://www.webcitation.org/5ziS1EJcn, 25.06.2011, patrz także: *Mowa końcowa LulzSec*, http://hacking.pl/pl/news-16482-Mowa_koncowa_LulzSec.html, 08.2011.

[106] M. Gajewski, *Lulzsec włamali się do 'The Sun', sfabrykowali informacje o śmierci Ruperta Murdocha*, http://www.chip.pl/news/bezpieczenstwo/monitorowanie-i-szyfrowanie-danych/2011/07/lulzsec-wlamali-sie-do-the-sun-sfabrykowali-informacje-o-smierci-ruperta-murdocha, 19.07.2011.

wobec wszelkich sił próbujących dokonać regulacji, subkultury Internetu. Najczęściej przyjmuje ona charakter organizacji, wokół której skupia się liczne, masowe grono sympatyków mobilizujące się na jej wezwanie. Najdłużej istniejącą tego typu organizacją jest Electronic Frontier Foundation (EFF). Założona została w 1990 roku przez Mitcha Kapora, Johona Gilmore'a i Johna Perry'ego Barlowa. Obecnie zrzesza kilkadziesiąt tysięcy członków i sympatyków; angażuje się w działania na rzecz wolności obywatelskich, prawa do anonimowości, prywatności i wolności słowa w Internecie; na przykład w 2005 roku wydała podręcznik dla blogerów umożliwiający im orientację w kwestiach prawnych związanych z publikacją wypowiedzi. Organizacja uczestniczy w licznych działaniach, w tym prawno-sądowych, na rzecz wolności słowa, w szczególności przeciwko korporacjom i rządowi Stanów Zjednoczonych. W grudniu 2010 roku wyraziła poparcie dla WikiLeaks i zaoferowała pomoc finansową oraz techniczną, sponsorowała również prace nad oprogramowaniem umożliwiającym bezpieczne komunikowanie się i omijanie cenzury[107]. Prawnicy EFF oraz ACLU (*American Civil Liberties Union*) chcieli dowieść, że pozbawianie konkretnej strony domeny internetowej stoi w sprzeczności z 1. poprawką do konstytucji USA. Znaczącą organizacją jest OpenNet Initiative – przeciwdziała ona cenzurze w sieci oraz nadzorowaniu internautów. Zrzesza liczne instytucje akademickie, głównie amerykańskie. Finansuje narzędzia służące do bezpiecznego zdobywania i rozpowszechniania informacji w Internecie, prowadzi działalność edukacyjną i promocyjną oraz analityczną. Organizacja ta sfinansowała wykonanie opisanego wcześniej w tekście narzędzia Psiphon, efektem jej działalności analitycznej są zaś publikacje na tematy związane z cenzurą w sieci[108]. Na uwagę zasługuje polska inicjatywa – powstała w 2009 roku Fundacja Panoptykon. Działa ona na rzecz ochrony praw człowieka, przeciwstawiając się obecnemu i nasilającemu się współcześnie zjawisku społeczeństwa nadzorowanego (*surveillance society*). Według statutu organizacja stawia sobie za cel podejmowanie debaty publicznej na temat mechanizmów i technologii umożliwiających nadzorowanie społeczeństwa, a także prowadzenie badań nad trendami rozwojowymi społeczeństwa nadzorowanego oraz analiz społecznych konsekwencji tego procesu.

[107] Więcej na temat EFF: *Electronic Frontier Foundation*, https://www.eff.org/, 08.2011.

[108] Są to następujące dzieła: *Access Denied – The Practice and Policy of Global Internet Filtering*, R.J. Deibert, J.G. Palfrey, R. Rohozinski, J. Zittrain (eds.), Cambridge 2008; *Access Controlled – The Shaping of Power, Rights, and Rule in Cyberspace*, R.J. Deibert, J.G. Palfrey, R. Rohozinski, J. Zittrain (eds.), Cambridge 2010. Więcej na temat organizacji: *OpenNet Initiative*, http://opennet.net/, 08.2011.

Istotnymi elementami działań Panoptykonu są działania edukacyjne służące podniesieniu poziomu świadomości społecznej na temat zagrożeń związanych z nowymi technologiami w kontekście nadzoru i inwigilacji. Wymienione cele realizowane są w postaci przygotowywania ekspertyz, analiz i opracowań, monitorowania prawa, uregulowań prawnych, a także propozycji zmian legislacyjnych i pomocy prawnej. Organizacja Panoptykon podejmuje liczne przedsięwzięcia – warto wymienić działania przeciwko projektom blokowania stron internetowych, rozmowy z rządem na temat regulacji Internetu i inne[109].

* * *

Cenzura treści internetowych przekazów dokonywana jest zarówno w państwach demokratycznych, jak i niedemokratycznych. W przypadku państw niedemokratycznych – autorytarnych i totalitarnych – stosowane są przede wszystkim techniki, które można określić mianem twardych. Polegają one na odcinaniu lub utrudnianiu dostępu do Internetu oraz blokowaniu niedozwolonych i niebezpiecznych zdaniem cenzurujących treści, a także penalizacji poszukiwania niektórych informacji w Internecie lub korzystania z określonych kanałów przekazu. Natomiast w systemach demokratycznych dominuje cenzura, którą można określić mianem miękkiej. Polega ona na tym, że użytkownicy Internetu sami nakładają na siebie ograniczenia, nie całkiem zdając sobie z tego sprawę – jest to autocenzura. Zjawisko tego typu niebezpieczne stanowi niebezpieczeństwo przede wszystkim dlatego, że jest ono trudne do dostrzeżenia. Internauci nie zauważają go, skupiając swoją aktywność na obronie przed „twardymi" formami cenzury. Nasilanie się tego trendu doprowadzić może w demokracjach do swoistego paradoksu – z jednej strony nieskrępowanych technicznych możliwości wyrażania opinii, a z drugiej – autocenzury na gruncie ideologicznym. Problem autocenzury wykracza poza komunikowanie polityczne w Internecie, obejmuje wszelkie formy komunikacji we współczesnych społeczeństwach. Pierre Bourdieu, analizując to zjawisko, wprowadził kategorię przemocy symbolicznej (*symbolic violence*, *la violence symbolique*), oznaczającą władzę narzucania członkom danej wspólnoty wzorców kulturowych jako niekwestionowanych, uniwersalnych, obowiązujących i to w taki sposób, że ukrywają one faktyczne układy sił[110]. Przemoc symboliczna manifestuje się poprzez działania socjalizacyjne i komunikacyjne, jej efektem jest kształtowanie i wdrażanie jako bez-

[109] Więcej na temat organizacji: *Fundacja Panoptykon*, http://panoptykon.org/, 08.2011.

[110] P. Bourdieu, J.-C. Passeron, *Reprodukcja. Elementy teorii systemu nauczania*, tłum. E. Neyman, Warszawa 2006, s. 73, 118.

alternatywnych określonych wzorców kulturowych: wartości, symboli, obyczajów, postaw. Władza kształtuje i narzuca posłuszeństwo nie w sposób mechaniczny, lecz manipulując siatką ludzkiej percepcji, kształtując miary, jakimi się posługujemy, interpretując to, co postrzegamy, w szczególności świat społeczny. Władza, ustanawiając taką matrycę percepcyjną, wpływa na system naszych ocen i utrwala go, a jednocześnie pozostaje niewidzialna i niekwestionowana przez obywateli. Tworzy ona pewien system, swoistą przestrzeń symboliczną, która pełni funkcję narzędzia służącego do narzucania i legitymizowania dominacji[111].

Internet zwielokrotnił możliwości komunikacji i wpływu zarówno rządzących, jak i rządzonych. Z jednej strony rządzeni uzyskali dzięki Internetowi nieposiadany dotąd i trudny do ograniczenia potencjał wymiany informacji, ekspresji myśli i mobilizacji. Efekty arabskiej wiosny 2011 roku i osłabiania chińskiego oraz kubańskiego reżimu to zasługa w dużej mierze Internetu. Z drugiej strony Internet wyposaża współczesne państwa i inne organizacje w niespotykany dotąd potencjał kontroli i inwigilacji jednostki. Wielu współczesnych badaczy rozwija tezę Michela Foucaulta, że nowoczesne państwo rezygnuje z przemocy fizycznej wobec obywateli na rzecz ich nadzorowania[112]. Wskazują oni, że Internet jest narzędziem, które mogłoby zaspokoić największe apetyty władzy na wszechwiedzę o obywatelach. W tym kontekście rozwijane są w literaturze przedmiotu alarmujące koncepcje państwa nadzoru czy Superpanoptykonu[113]. Odsłania się janusowe oblicze Internetu: jest jednocześnie narzędziem służącym realizacji wolności słowa i ograniczania tej wolności.

Streszczenie

W prezentowanym artykule przeanalizowano przebieg i efekty walki o wolny dostęp do informacji i komunikowanie się w Internecie. Walka o wpływy rozgrywa się pomiędzy obywatelami, organizacjami trzeciego sektora, i ruchami społecznymi

[111] P. Bourdieu, L.J.D. Wacquant, *Zaproszenie do socjologii refleksyjnej*, tłum. A. Sawisz, Warszawa 2001, s. 167.

[112] M. Foucault, *Nadzorować i karać*, tłum. T. Komendant, Warszawa 1998.

[113] T. Bringall III, *The New Panopticon: The Internet Viewed as a Structure of Social Control*, http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN003570.pdf, 07.2011; N. Chomsky, *Necessary Illusions. Thought Control in Democratic Societies*, Londyn 1989; D. Lyon, *The Electronic Eye. The Rise of Surveillance Society*, Minneapolis 1994, s. 37; E. Morozov, *The Net Delusion. The Dark Side of Internet Freedom*, Nowy Jork 2011; M. Poster, *Critical Theory and Poststructuralism: In Search of a Context*, Nowy Jork 1989 oraz tenże, *The Mode of Information*, Cambridge 1990.

– z jednej strony, a państwami – z drugiej. W pierwszej części tekstu oceniono, w jakim stopniu, w jakich formach i wskutek działań jakich podmiotów podstawowa demokratyczna wartość – wolność słowa – podlega w Internecie ograniczeniom. Druga część artykułu zawiera analizę metod służących użytkownikom Internetu do stawiania oporu ograniczaniu wolności słowa. Przeprowadzona analiza wykazała, że rywalizacja pomiędzy tymi dwoma rodzajami podmiotów ma charakter dynamiczny i ewolucyjny. Rola inicjatorów działań przypada głównie państwom, z kolei obywatele na ogół jedynie reagują na wprowadzane ograniczenia. Obydwie strony podejmują przede wszystkim działania o charakterze technicznym: instytucje państwa wdrażają rozwiązania umożliwiające filtrowanie i blokowanie treści, a obywatele konstruują oprogramowanie pozwalające bezpiecznie wykorzystywać informacje niedostępne wskutek zabiegów cenzorskich. Państwa ponadto posiłkują się w ograniczaniu wolności słowa rozwiązaniami legislacyjnymi, takimi jak cenzura prewencyjna oraz inne pośrednie i bezpośrednie formy nacisku lub ograniczeń. Obywatele, broniąc się przed cenzurą, podejmują działalność o charakterze edukacyjnym, która realizowana jest zwykle przez organizacje pozarządowe.

Daniel Mider, Olgierd Borówka

INTERNET – MEDIUM WITHOUT CENSORSHIP?

In this article the process and consequences of the struggle for influences on the Internet that takes place between citizens (individuals, NGO's, social movements) and government institutions were analyzed. In the first part of the text, the degree to which basic democratic values such as freedom of speech are subject to Internet restrictions was investigated. The second part of the reading constitutes an analysis of the methods which are used to resist Internet limits on freedom of speech. It can be concluded from the analysis conducted that the rivalry between these two types of subjects is of a dynamic character. Governments usually take action whereas citizens react solely to the introduced restrictions. Both sides undertake action of a technical character which is based on implementing the solutions enabling filtering and blocking the content or allowing safe browsing and use of information which because of censorship has become unavailable. Moreover, governments make use of legislative solutions to restrict freedom of speech such as preventative censorship or other direct and indirect forms of repression. Society, however while defending itself from censorship, undertakes activities of an educational character which are implemented by NGO's.

KEY WORDS: *sociology of the Internet, political communication, political censorship, typology of political censorship, freedom of speech*