Zeszyty **PRASOZNAWCZE**

Kraków 2014, T. 57, nr 2 (218), s. 337–354

doi:10.4467/2299-6362PZ.14.019.2340

www.ejournals.eu/Zeszyty-Prasoznawcze/

LOSY SWOBODNEGO PRZEPŁYWU INFORMACJI W KONTEKŚCIE PROJEKTÓW ACTA ORAZ ITR

MICHAŁ OLĘDZKI

Uniwersytet Warszawski
Wydział Dziennikarstwa i Nauk Politycznych

ABSTRACT

Future of free flow of information in the context of ACTA and IRT projects

The idea of free flow of information, for which after II world war developed democratic countries fought on the United Nations and UNESCO forums, was primarily based on the American concept of freedom of the press and the belief that the source of human progress is unrestricted activity of individuals and free competition, uninhibited by state authorities intervention. Today, with the Internet we finally have free access to information and freedom of passing it on to others. However, frequently there are more cases of limiting access to certain information on the network, not only from authoritarian countries, but also democratic. Under the legal names of projects such as European Commissions' ACTA or ITR (International Telecommunications Regulations) operated by the International Telecommunication Union (ITU – the specialized organization of United Nations) there are smuggled provisions that main goal is to better control the Internet, and thus the flow of information in the world. Citizens of many countries recognize this as a desire to limit their rights and freedoms, so they loudly oppose such regulations. There is a war for control over information. This war has already started decades ago and on its course not only politicians, big business and the media have an impact, but also to the fore come Internet users – citizens of free countries.

Key words: flow of information, ACTA, IRT, new media

Idea swobodnego przepływu informacji, o której realizację walczyły po II wojnie światowej na forum ONZ i UNESCO rozwinięte kraje demokratyczne, opierała się przede wszystkim na amerykańskiej koncepcji wolności prasy i przekonaniu,

✉ Adres do korespondencji: Wydział Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego, Instytut Dziennikarstwa, ul. Nowy Świat 69, 00-927 Warszawa

że źródłem postępu ludzkości jest niczym nieograniczona działalność jednostek oraz swobodna walka konkurencyjna, niekrępowana ingerencją organów państwowych. Przez niemal pół wieku toczyły się rozmowy na poziomie międzynarodowym, co należy zrobić, aby każdy obywatel miał swobodny dostęp do informacji. Podkreślano, że człowiek, aby się rozwijał i zdobywał wiedzę o otaczającym go świecie, powinien mieć nieograniczony dostęp do wszystkich źródeł informacji. Powszechna Deklaracja Praw Człowieka, Międzynarodowe Pakty Praw Obywatelskich i Politycznych czy Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności gwarantowały, że demokratyczne rządy zapewnią realizację tych podstawowych wartości i praw człowieka.

Dzisiaj ta idea nie ma już takiego znaczenia jak niemal w całym XX wieku, gdy dostęp do różnych baz danych i źródeł informacji był mocno ograniczony czy to ze względu na brak technologii, czy też z powodu uwarunkowań politycznych i ideologicznych. Internet, a w szczególności wyszukiwarki internetowe ułatwiają obecnie niemal powszechny dostęp do informacji, wciąż jednak mamy do czynienia z barierami, takimi jak konieczność posiadania odpowiedniego urządzenia i podłączenia do Internetu, a w krajach o systemach totalitarnych lub monopartyjnych państwowa kontrola dostępu do sieci bądź do określonych serwisów. Zatem o ile narodziny i szybki rozwój Internetu stały się wielką szansą zrealizowania marzeń ludzi o likwidowaniu barier ograniczających poznanie świata poprzez dostęp do wielu źródeł informacji, o tyle w wielu miejscach na świecie mieszkają miliony ludzi, którzy nie mają szans na korzystanie z sieci. Wciąż jeszcze możemy też mówić o uzależnieniu technologicznym większości państw świata od takich potęg przemysłowych jak Stany Zjednoczone, które dysponują największym potencjałem intelektualnym i możliwościami produkcyjnymi dającymi im nieograniczone możliwości generowania nowych technologii internetowych, ale także dzięki temu sprawowania kontroli nad całym przepływem informacji w świecie.

Wystarczy zauważyć, że zdecydowana większość z nas korzysta z jednego systemu (Windows), jednej przeglądarki (Internet Explorer) oraz jednej wyszukiwarki (Google). Zawarte w misji Google słowa o „uporządkowaniu światowych zasobów informacji, tak by stały się powszechnie dostępne i użyteczne" są właściwą ilustracją ekonomicznych i politycznych prób wykorzystania tych informacji oraz tego, jak ważne w dzisiejszym społeczeństwie są wyszukiwarki internetowe. Umożliwiają one jednak wielu rządom i zaawansowanym technologicznie użytkownikom z odpowiednimi zdolnościami rozwój różnych narzędzi i mechanizmów, które pozwalają uzyskać określone korzyści i promować swoje interesy gospodarcze, militarne oraz polityczne.

Dzisiaj za pomocą Internetu mamy wreszcie do czynienia ze swobodnym dostępem do informacji, jak i swobodą jej przekazywania. Coraz częstsze są jednak przypadki chęci ograniczenia dostępu do pewnych informacji w sieci, nie tylko ze strony państw autorytarnych, ale również demokratycznych. Pod przykrywką projektów prawnych ACTA Komisji Europejskiej lub ITR (Międzynarodowe Przepisy Telekomunikacyjne) prowadzonym przez Międzynarodowy Związek

Telekomunikacyjny (ITU – organizacja wyspecjalizowana ONZ) przemyca się przepisy, które mają na celu większą kontrolę Internetu, a tym samym przepływu informacji w świecie. Obywatele wielu państw uznają to za chęć ograniczenia ich praw i swobód, więc głośno sprzeciwiają się tym przepisom. Trwa wojna o kontrolę nad informacją. Wojna ta rozpoczęła się już dziesiątki lat temu i na jej przebieg mają wpływ nie tylko politycy, wielki biznes i media, ale do głosu dochodzą też użytkownicy Internetu – obywatele wolnych krajów.

Przykłady ograniczania wolności w Internecie

Jedną ze strukturalnych cech Internetu jest jego niezawisłość. Wolność słowa i swoboda komunikacji są wpisane w istotę sieci od jej samych początków. John Gilmore, współtwórca Electronic Frontier Foundation – międzynarodowej organizacji *non profit* zajmującej się prawem cyfrowym, stwierdził w 1993 roku: „Sieć interpretuje cenzurę jako usterkę i ją omija”[1]. Początkowo zarządzaniem Internetem zajmowały się nie państwa, lecz związek dobrowolnych ciał standaryzacyjnych oraz organizacje obywatelskie złożone z informatyków, naukowców i pasjonatów. Jest to swoisty system obejmujący wielu interesariuszy.

Powszechnie znana jest jednak prawda, że dostęp do informacji daje władzę, dlatego też rządy starają się ją kontrolować. Przykładów takiej kontroli nie trzeba długo szukać. Przy Radzie Praw Człowieka w Organizacji Narodów Zjednoczonych działa Specjalny Sprawozdawca, który zgodnie z rezolucją 7/36 otrzymał mandat do promocji i ochrony prawa do wolności opinii i wypowiedzi[2]. W szczególności rezolucja żąda od Specjalnego Sprawozdawcy, aby „dostarczał swoich opinii na temat korzyści i wyzwań nowych technologii informacyjnych i komunikacyjnych, w tym Internetu oraz technologii mobilnych, do egzekwowania prawa do wolności opinii i wypowiedzi, w tym prawa do poszukiwania, otrzymywania i przekazywania informacji oraz znaczenia szerokiej różnorodności źródeł, jak również dostępu do społeczeństwa informacyjnego dla wszystkich”[3].

Według raportu Specjalnego Sprawozdawcy z 16 maja 2011 roku Internet poprzez umożliwianie indywidualnym jednostkom natychmiastowej i niedrogiej wymiany informacji i idei ponad granicami krajów pozwala na dostęp do informacji i wiedzy, który wcześniej nie był możliwy. To z kolei przyczynia się do odkrywania prawdy i postępu społeczeństwa jako całości[4]. Internet stał się podstawowym środkiem, za pomocą którego użytkownicy mogą korzystać ze swoich praw do wolności opinii i wypowiedzi zagwarantowanej w artykule 19 Powszechnej Deklaracji Praw Człowieka oraz Międzynarodowego Paktu Praw Obywatelskich i Politycznych.

[1] P. Elmer-Dewitt: First Nation in Cyberspace, *TIME International* 1993, nr 49.
[2] http://ap.ohchr.org/documents/E/HRC/resolutions/A_HRC_RES_7_36.pdf (dostęp: 16.09.2013).
[3] Tamże.
[4] F. La Rue: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27, 16 maja 2011, s. 7.

W raporcie uznano również, że dzięki temu, iż Internet dla jednostek indywidualnych działa jako katalizator spełniania swoich praw do wolności opinii i wypowiedzi, jednocześnie ułatwia realizację wielu innych praw człowieka.

Artykuł 19 ust. 3 w Międzynarodowym Pakcie Praw Obywatelskich i Politycznych określa rodzaje ograniczeń, które są sprzeczne z zobowiązaniami państw w celu zagwarantowania prawa do wolności słowa. Zgodnie z wymienionym paktem istnieją pewne wyłączenia dotyczące typów wypowiedzi, które mogą być legalnie zabronione, zwłaszcza w celu ochrony praw innych osób. Ograniczenie prawa do wolności wypowiedzi musi przejść trzyczęściowy skumulowany test[5]: a) musi być zapewnione przez prawo, które jest zrozumiałe i dostępne dla każdego (zasada przewidywalności i przejrzystości); b) musi realizować jeden z celów określonych w artykule 19, ustęp 3, a mianowicie w celu ochrony praw lub reputacji innych osób, czy też w celu ochrony bezpieczeństwa narodowego lub porządku publicznego, bądź zdrowia albo moralności społecznej; oraz c) musi być udowodnione jako niezbędne i będące najmniej restrykcyjnymi środkami koniecznymi do osiągnięcia rzekomego celu (zasada konieczności i proporcjonalności). Ponadto wszelkie przepisy ograniczające prawo do swobody wypowiedzi muszą być stosowane przez organ, który jest niezależny od wszelkich politycznych, handlowych lub innych nieuzasadnionych wpływów.

Uzasadnione rodzaje informacji, które mogą być ograniczane, to: dziecięca pornografia, mowa nienawiści, zniesławienie, bezpośrednie lub publiczne podżeganie do popełnienia ludobójstwa, a także popieranie nienawiści narodowej, rasowej lub religijnej, stanowiące podżeganie do dyskryminacji, wrogości lub przemocy.

Wiele krajów jednak ogranicza, kontroluje, manipuluje lub cenzuruje treści rozpowszechniane za pośrednictwem Internetu bez żadnej podstawy prawnej. Specjalny Sprawozdawca jest zdania, że arbitralne wykorzystanie prawa karnego do sankcji prawnie uzasadnionych wypowiedzi stanowi jedną z najcięższych form ograniczeń prawa do wolności słowa, ponieważ nie tylko tworzy poczucie braku bezpieczeństwa wśród użytkowników, ale też prowadzi do innych naruszeń praw człowieka, takich jak zatrzymania i tortury oraz inne formy okrutnego, nieludzkiego lub poniżającego traktowania albo karania. Poniżej opisuję kilka wymienionych przez Specjalnego Sprawozdawcę sposobów ograniczania wolności w Internecie:

- Arbitralne blokowanie lub filtrowanie treści – jednym z najczęściej występujących na świecie sposobów ograniczania prawa do wolności opinii i wypowiedzi jest blokowanie i filtrowanie treści w Internecie. W lutym 2008 roku rząd Pakistanu nieumyślnie zablokował całemu światu dostęp do serwisu umożliwiającego bezpłatne umieszczanie i oglądanie filmów – YouTube. Przez dwie godziny użytkownicy na całym świecie nie mogli skorzystać z serwisu, ponieważ rząd Pakistanu, próbując zablokować swo-

[5] Tamże, s. 8.

im obywatelom dostęp do filmu wideo szydzącego z proroka Mahometa, spowodował poważną usterkę techniczną[6].

- Sankcjonowanie karne legalnej wypowiedzi – fizyczne wyciszanie krytyki lub niezgody poprzez arbitralne aresztowania i zatrzymania, porwania, nękanie i zastraszanie to zjawisko stare, lecz również odnoszące się do użytkowników Internetu. Rządy niektórych państw starają się zapobiec nie tylko temu, aby informacja dotarła do użytkownika, ale także biorą na cel bezpośrednio tych, którzy szukają, otrzymują lub przekazują politycznie wrażliwą informację poprzez sieć internetową.
- Nałożenie odpowiedzialności na pośrednika (usługodawcę) – niektóre państwa wprowadziły ustawy nakładające odpowiedzialność na dostawców usług internetowych (ale też wyszukiwarki internetowe i serwisy społecznościowe), jeżeli nie będą filtrować, usuwać lub blokować generowanych przez użytkowników treści, które są uznane za nielegalne. Na przykład ustawa 5651 w Turcji nakłada nowe zobowiązania na dostawców treści oraz usług internetowych, jak również upoważnia blokowanie stron zawierających bezprawne treści, w tym „obrażanie" założyciela Republiki Turcji, Mustafy Kemala Atatürka.
- Odłączanie użytkowników od dostępu do Internetu, w tym na podstawie naruszenia prawa własności intelektualnej – firma telekomunikacyjna Renesys przeprowadziła badania, w których próbowała oszacować, jak trudno byłoby odłączyć cały świat od Internetu. Ryzyko określano na podstawie liczby dostawców usług sieciowych w każdym kraju. Najwyższe ryzyko zagrożenia odcięciem jest w krajach z jednym lub dwoma dostawcami – takich krajów jest 61, a wśród nich Syria, Tunezja, Turkmenistan, Libia, Etiopia, Uzbekistan, Birma i Jemen. Znaczące ryzyko jest w kolejnych 72 krajach, takich jak Oman, Benin, Botswana, Rwanda, Pakistan, Kirgistan, Uganda, Armenia i Iran[7]. To oznacza, że w 133 krajach kontrola nad siecią jest na tyle scentralizowana, że można praktycznie odłączyć Internet po jednym telefonie.
- Cyberataki – w trakcie konfliktu zbrojnego w Syrii zwiększyły swoją aktywność grupy hakerskie opowiadające się za opozycją (Free Syrian Army) albo za Baszszarem al-Asadem (Syrian Electronic Army). Grupa lojalna wobec prezydenta Syrii dokonała kilku ataków na strony główne mediów, w tym pod koniec sierpnia na domenę strony *The New York Times*, całkowicie blokując do niej dostęp. Wcześniej SEA włamała się na konta Twittera takich mediów jak Associated Press czy *The Washington Post* oraz atakowała stronę CNN.com[8].
- Niewystarczająca ochrona prawa do prywatności i ochrony danych – Internet udostępnia nowe narzędzia i mechanizmy, za pomocą których państwa

[6] Zob. https://opennet.net/youtube-censored-a-recent-history (dostęp: 16.09.2013).

[7] Zob. http://www.renesys.com/2012/11/could-it-happen-in-your-countr/ (dostęp: 16.09.2013).

[8] Zob. http://edition.cnn.com/2013/08/27/tech/web/new-york-times-website-attack/index.html?hpt=hp_t4 (dostęp: 16.09.2013).

oraz prywatne korporacje mogą monitorować i zbierać informacje na temat użytkowników i ich poczynań w sieci. Władze państw najczęściej uzasadniają tego typu działania dbaniem o bezpieczeństwo narodowe lub walką z terroryzmem. Znane są przypadki wykorzystywania popularnych serwisów społecznościowych typu Facebook do identyfikowania i śledzenia aktywności obrońców praw człowieka lub opozycji. Natomiast w niektórych państwach promuje się system identyfikacji oparty na używaniu prawdziwych imion. W Chinach w 2012 roku Ministerstwo Bezpieczeństwa Publicznego ustanowiło, że taki system powstanie i każdy większy portal będzie musiał go wdrożyć do czerwca 2014 roku[9]. Tym samym wyeliminuje się anonimowość w kraju, w którym prawa człowieka są często łamane.

Dostęp do Internetu na świecie

Nie można zapomnieć, że korzystanie z Internetu jest uzależnione od jego dostępności w danym miejscu. Zgodnie z informacjami zaprezentowanymi w raporcie Urzędu Komunikacji Elektronicznej pod koniec 2013 roku 8% osób w Polsce nie ma w ogóle dostępu do Internetu. Najgorzej jest w powiatach jędrzejowskim i starachowickim, w których na 40% terenu nie ma zasięgu[10]. Dane ze świata prezentuje raport Narodów Zjednoczonych pod nazwą Milenijne Cele Rozwoju. Według tych badań pod koniec 2013 roku dostęp do Internetu ma mieć 2,7 miliarda ludzi[11], czyli niecała jedna trzecia populacji na świecie.

Różnice w dostępie są przyczyną powstawania tzw. cyfrowego podziału (*digital divide*), który najczęściej oznacza, że tylko pewna część społeczeństwa może korzystać z dobrodziejstw sieci, tym samym tworząc sztuczną elitę. Według danych za rok 2013, pochodzących z raportu ITU (International Telecommunication Union), występują znaczne różnice w dostępie do Internetu między państwami rozwiniętymi a wciąż rozwijającymi się. W przypadku tych pierwszych można znaleźć 76,8 internautów na 100 obywateli, natomiast w przypadku krajów rozwijających się jest to zaledwie 30,7 internautów[12].

21 sierpnia 2013 roku powstał Internet.org, inicjatywa globalnej współpracy między gigantami technologicznymi, takimi jak Facebook, Ericsson, MediaTek, Nokia, Opera, Qualcomm oraz Samsung. Głównym celem przedsięwzięcia jest powiększenie dostępności Internetu dla pozostałych 5 miliardów osób. Aby osiągnąć ten cel, Internet.org skupi się w krajach rozwijających się na trzech wy-

[9] Zob. http://advocacy.globalvoicesonline.org/2013/06/10/the-business-behind-chinas-internet-real-name-registration-system/ (dostęp: 16.09.2013).

[10] Zob. http://wyborcza.biz/biznes/1,106928,14500769,Bardzo_dziurawe_sieci__8_proc__kraju_nie_ma_w_ogole.html (dostęp: 16.09.2013).

[11] Zob. http://www.un.org/millenniumgoals/pdf/report-2013/mdg-report-2013-english.pdf (dostęp: 16.09.2013).

[12] Zob. http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU_Key_2005-2013_ICT_data.xls (dostęp: 16.09.2013).

zwaniach: (a) sprawienie, aby dostęp do Internetu był możliwy w przystępnej cenie; (b) inwestycja w narzędzia zwiększające efektywność przesyłanych danych; (c) wypracowanie nowych modeli biznesowych, które umożliwiają dostęp do Internetu[13]. Plany projektu są zakrojone na około 5–10 lat.

Istnieje już kilka inicjatyw na świecie, których głównym celem jest zwiększenie liczby użytkowników albo ułatwienie dostępu do Internetu. Wspomniany już Facebook uruchomił usługę Facebook Zero, specjalnie przygotowaną wersję tekstową swojego serwisu, którą bez problemu da się uruchomić nawet na starszych modelach telefonów, a co najważniejsze – bezpłatną[14]. Portal społecznościowy współpracuje z operatorami komórkowymi w Afryce, dzięki czemu korzystanie z serwisu Facebook Zero nie wymaga żadnych opłat. W ten sposób Facebook poszerza swoją liczbę użytkowników.

W podobny sposób działa Google na Filipinach, gdzie po porozumieniu się z operatorem Globe Telecom wszystkie najważniejsze usługi, jak wyszukiwarka Google, poczta elektroniczna Gmail oraz portal społecznościowy Google+, są dostępne bez konieczności uiszczania opłaty za przesyłanie danych[15]. Jednocześnie właściciel najpopularniejszej wyszukiwarki na świecie rozwija projekt „Loon for all", który polega na budowie sieci balonów zawieszonych około 18 kilometrów nad ziemią. Balony miałyby dostarczać Internet w miejscach pozbawionych dostępu do sieci, tym samym redukując ich liczbę i pozwalając na korzystanie z Internetu nawet w rejonach dotkniętych kataklizmami[16].

Według orzeczenia niemieckiego Trybunału Federalnego w Karlsruhe z 2013 roku Internet jest artykułem pierwszej potrzeby i „utrata możliwości korzystania z Internetu jest porównywalna do utraty możliwości korzystania z samochodu"[17]. Podobnie jest od 2009 roku w Finlandii, gdzie dostęp do łącza o prędkości przynajmniej 1 Mbps jest uważany za podstawowe prawo obywatelskie – każdy obywatel musi mieć techniczną możliwość uzyskania dostępu do sieci[18]. Organizacja międzynarodowa Internet Society przeprowadziła w 2012 roku globalny sondaż wśród użytkowników Internetu, w którym zapytano, czy Internet powinien być gwarantowanym podstawowym prawem człowieka – 83% przepytanych osób odpowiedziało pozytywnie[19].

[13] Zob. https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851575_492821944140017_1070145609_n.pdf (dostęp: 16.09.2013).

[14] Zob. http://technologie.gazeta.pl/internet/1,104530,12625795,Mark_Zuckerberg_szuka_przyjaciol_w_krajach_rozwijajacych.html (dostęp: 16.09.2013).

[15] Zob. http://surf.globe.com.ph/plan/freezone (dostęp: 16.09.2013).

[16] Zob. http://www.google.com/loon/ (dostęp: 16.09.2013).

[17] Zob. http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&pm_nummer=0014/13 (dostęp: 28.04.2013).

[18] Zob. http://www.komputerswiat.pl/nowosci/internet/2013/04/internet-niezbedny-do-zycia-w-jakim-kraju.aspx (dostęp: 28.04.2013).

[19] Zob. https://www.internetsociety.org/sites/default/files/GIUS2012-GlobalData-Table-20121120_0.pdf (dostęp: 16.09.2013).

Anti-Counterfeiting Trade Agreement (ACTA)

Umowa międzynarodowa, która powstawała już od 2006 roku z inicjatywy przedstawicieli Stanów Zjednoczonych i Japonii, miała na celu zwalczanie obrotu towarami podrabianymi i ustalenie standardów w walce z naruszeniami własności intelektualnej. W regulacji podjęto kwestie obrotu podrabianymi dobrami, zasady handlu lekami generycznymi oraz, co wywołało największe kontrowersje, problemu rozpowszechniania poprzez Internet dzieł prawnie chronionych.

Od początku prac nad umową ustalono, że jej szczegóły miały pozostać tajne. Oficjalne negocjacje rozpoczęto w czerwcu 2008 i już w tym samym roku, po opublikowaniu pierwszej roboczej wersji dokumentu przez serwis WikiLeaks, wzbudził on niepokój wśród zainteresowanych. 20 kwietnia 2010 roku udostępniono publicznie dokument projektu w wersji oficjalnej[20]. Na odpowiedź nie trzeba było długo czekać – 75 praktykujących prawników i profesorów prawa wydało wspólne oświadczenie, w którym podkreślali, że bieżąca wersja ACTA zagraża licznym aspektom interesu publicznego. Również Parlament Europejski skrytykował prace nad porozumieniem za brak przejrzystości w sposobie prowadzenia rozmów oraz utrudniony dostęp do materiałów negocjacyjnych.

Mimo krytyki 1 października 2011 roku umowę podpisały Kanada, USA, Australia, Japonia, Maroko, Nowa Zelandia, Singapur i Korea Południowa. Rada Unii Europejskiej przyjęła ostateczne porozumienie 16 grudnia 2011 roku, a informacje o nim zamieszczono na ostatniej stronie komunikatu prasowego na temat rolnictwa i rybołówstwa. 26 stycznia 2012 roku Unia Europejska i 22 państwa członkowskie (bez Cypru, Estonii, Niemiec, Holandii i Słowacji) podpisały umowę ACTA. Nic dziwnego, że tego typu sposób uchwalenia umowy międzynarodowej wywoływał wielkie kontrowersje i ogólny sprzeciw w różnych krajach. Wynikiem tych protestów było odrzucenie porozumienia przez Parlament Europejski 4 lipca 2012 roku[21].

Najwięcej zarzutów wobec porozumienia ACTA dotyczyło sposobu prowadzenia negocjacji, a dokładniej braku publicznego dostępu do materiałów. Przez cały okres prac raz po raz pojawiały się apele o jawność. „W dniu 24 listopada, w imieniu Stowarzyszenia Internet Society Poland, zostały złożone do Kancelarii Prezesa Rady Ministrów, do Ministerstwa Gospodarki i do Ministerstwa Kultury i Dziedzictwa Narodowego wnioski o udostępnienie informacji publicznej na temat posiadanych przez te urzędy dokumentów i innych informacji związanych z negocjacjami umowy międzynarodowej, której robocza nazwa brzmi Anti-Counterfeiting Trade Agreement (ACTA)”[22]. Grupa organizacji i stowarzyszeń z całego świata (w tym Electronic Frontier Foundation – amerykańska organizacja

PŁASZCZYZNY

[20] Zob. http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146029.pdf (dostęp: 16.09.2013).

[21] Zob. http://fakty.interia.pl/raport-internauci-przeciwko-acta/aktualnosci/news-parlament-europejski-odrzucil-acta,nId,918949 (dostęp: 16.09.2013).

[22] Zob. http://www.isoc.org.pl/200911/acta (dostęp: 16.09.2013).

non profit zajmująca się walką o prawo do anonimowości, prywatności i wolności słowa w elektronicznym świecie) wystosowały wspólny list otwarty w tej sprawie – jednak podejścia nie zmieniono. Jednocześnie wraz z kolejnymi przeciekami na temat porozumienia pojawiało się coraz więcej zarzutów o wbudowywanie mechanizmów cenzorskich w techniczne specyfikacje usług dostępu do Internetu. Wszystko w imię walki z przejawami naruszania cudzej własności intelektualnej.

Kontrowersje wzbudzały między innymi zapiski w rozdziale II: Ramy prawne dla dochodzenia i egzekwowania praw własności intelektualnej, sekcji 5: Dochodzenie i egzekwowanie praw własności intelektualnej w środowisku cyfrowym. W 2009 roku kilka międzynarodowych organizacji, w tym Electronic Frontier Foundation, Free Software Foundation oraz Free Knowledge Institute, opublikowało list otwarty, w którym wyraziło opinie, że regulacje te naruszają fundamentalne prawa i demokrację w ogóle. Według nich ACTA ograniczałaby konstytucyjne prawa i wolności obywateli, a w szczególności wolność słowa i prawo do prywatności w komunikacji[23].

Według organizacji pozarządowych ACTA mogło prowadzić do blokowania legalnych i wartościowych treści dostępnych w Internecie, ponieważ w przepisie tym przewidziano sposób stosowania środków zabezpieczających w postaci odcinania użytkowników od dostępu do sieci.

Fundacja Panoptykon pokusiła się o opracowanie wskazujące zapisy budzące największy sprzeciw[24]. Zgodnie z tym dokumentem artykuł 8 (Nakazy) dopuszczał prywatną egzekucję praw autorskich oraz zapobieganie ich domniemanym naruszeniom bez kontroli sądu i gwarancji uczciwego procesu, jak również zakładał zastosowanie procedury karnej także w przypadkach wystąpienia naruszeń zupełnie błahych, pod warunkiem że naruszenie było umyślne.

Artykuł 27 (Dochodzenie i egzekwowanie w środowisku cyfrowym) dopuszczał monitorowanie i rejestrowanie działań podejmowanych w sieci przez miliony użytkowników, mimo braku uzasadnionych podejrzeń co do niezgodności ich zachowań z prawem (co narusza przyjęte w prawie europejskim zasady ochrony danych osobowych). Jednocześnie „zapisy ochronne z art. 27, zasadniczo bez znaczenia, są dodatkowo osłabione informacją zawartą w przypisach. Wyjaśniają one, że ochrona operatorów sieci przed odpowiedzialnością karną (będąca najistotniejszym elementem wolnego Internetu i kluczem do jego sukcesu) jest dopuszczalna, ale jako drugorzędna wobec interesów właścicieli praw autorskich. Sytuacja, w której interes wąskiej grupy właścicieli praw autorskich ma tę samą rangę co interes dostawców Internetu i całego społeczeństwa, stoi w bezpośredniej sprzeczności z treścią orzeczeń Europejskiego Trybunału Sprawiedliwości w sprawie Telefonica przeciwko Promusicae (C275/06), a zwłaszcza w sprawie Scarlet przeciwko Sabam (C70/10). Uzasadnienie tego ostatniego wyraźnie mówi,

[23] Zob. http://freeknowledge.eu/acta-a-global-threat-to-freedoms-open-letter (dostęp: 16.09.2013).

[24] Zob. http://www.tvn24.pl/ktore-zapisy-acta-budza-najwiekszy-sprzeciw,198269,s.html (dostęp: 16.09.2013).

że jedna grupa praw nie może mieć większej rangi niż inna, lecz «należy dbać o zachowanie równowagi pomiędzy prawem własności intelektualnej a swobodą prowadzenia działalności gospodarczej, prawem do ochrony danych osobowych oraz swobodą wymiany informacji». Tymczasem przypis 16 porozumienia ACTA stawia interesy właścicieli praw autorskich w pozycji nadrzędnej, przez co stoi w niezgodzie z prawodawstwem europejskim"[25].

ACTA zgodnie z art. 23 (Przestępstwa) przewidywało również nowe zasady ustalania wysokości odszkodowań z tytułu stwierdzonych naruszeń prawa autorskiego. Jednym z punktów odniesienia dla sądu miała być „sugerowana cena detaliczna" produktu, a nie rzeczywiście utracone korzyści. Tego typu zapis mógł hamować innowacyjność, bo przedsiębiorcy, aby nie ryzykować wysokich odszkodowań, powstrzymywaliby się od wdrażania nowych pomysłów, które w jakikolwiek sposób mogłyby się inspirować projektami stworzonymi wcześniej przez inne firmy.

Wśród artykułów można było też znaleźć „zapisy ochronne", jednak w wielu przypadkach były one spisane nieprecyzyjnie albo nie wprowadzały niczego nowego, a jedynie odnosiły się do wcześniejszych przepisów. Takim przykładem był art. 4 ust. 1, dotyczący ujawniania informacji czy przetwarzania danych osobowych w celu wspólnego egzekwowania praw własności intelektualnej w sektorze prywatnym, albo art. 27 ust. 2–4, który odwołuje się do konieczności zachowania „zasad podstawowych, takich jak: wolność wypowiedzi, prawo do uczciwego procesu czy prawo do prywatności". Ten ostatni był nieegzekwowalny, ponieważ określenie „zasad podstawowych" nie precyzowało, o jakie prawa chodzi – czy o Konwencję ONZ o Prawach Politycznych i Obywatelskich, czy też o Europejską Konwencję Praw Człowieka[26].

Co dla użytkownika Internetu mogło oznaczać wprowadzenie w życie ACTA? Każdy mógł nagle stać się „piratem", bo umowa ta przewidywała kary dla osób dopuszczających się piractwa na skalę handlową. Podczas przeglądania danej witryny przeglądarka internetowa zapisuje na komputerze jej lokalną kopię, czyli grafiki oraz treść artykułów. Brak zdefiniowania „skali handlowej" oraz zbyt ogólna definicja „pirata" są w powyższym przypadku kluczowe. Użytkownicy nie mogliby również obejść zabezpieczeń przed wyświetlaniem materiałów w danym kraju – dzisiaj wiele materiałów filmowych znajdujących się na serwisach amerykańskich jest niedostępnych dla użytkowników próbujących je obejrzeć z komputerów w Polsce. Również wielu właścicieli stron mogłoby zrezygnować z prowadzenia serwisów z obawy przed odpowiadaniem za treści zamieszczone przez ich użytkowników. Polska Izba Informatyki i Telekomunikacji stwierdziła: „Gdyby wprowadzić odpowiedzialność po stronie przedsiębiorców internetowych za treści umieszczane przez użytkowników oraz obowiązek monitorowania

[25] Tamże.

[26] Zob. http://www.tvn24.pl/ktore-zapisy-acta-budza-najwiekszy-sprzeciw,198269,s.html (dostęp: 16.09.2013).

tych treści, to nie tylko doprowadziłoby to do cenzury w Internecie, ale przede wszystkim sens biznesowy platform internetowych przestałby istnieć, co z kolei skutkowałoby załamaniem gospodarki internetowej”[27].

„Dostawca internetu będzie Cię śledził” – brzmiało jedno z ostrzeżeń na temat ACTA opublikowanych na portalu Onet. ACTA wymagało od dostawców usług internetowych monitorowania swoich użytkowników i na żądanie właściciela praw autorskich podania danych osoby, którą tylko podejrzewa się o posiadanie treści naruszających prawa autorskie. Jednocześnie oskarżający mógł żądać informacji o wskazanych osobach w jakikolwiek sposób powiązanych z podejrzanym, czyli dane osób, które pobierały pliki od podejrzanego, też musiałyby być ujawnione. Oznaczałoby to też olbrzymie wydatki małych dostawców internetowych na infrastrukturę monitorującą każdą akcję internauty.

Polacy vs ACTA

W związku ze wszystkimi powyższymi zarzutami wobec porozumienia ACTA zaniepokojenie przebiegiem prac wyrażały wielokrotnie różne organizacje pozarządowe, m.in. Internet Society Polska, Fundacja Nowoczesna Polska oraz Fundacja Panoptykon. Media zainteresowały się tematem pod koniec 2011 roku, gdy Piotr Waglowski – znany bloger zajmujący się tematyką prawnych aspektów społeczeństwa informacyjnego, mocno zaangażowany społecznie w rozwój polskiego Internetu – opisał, w jaki sposób zapadła rządowa decyzja o podpisaniu w imieniu Polski umowy ACTA. Otóż uchwała przygotowana przez Ministerstwo Kultury i Dziedzictwa Narodowego, którą Donald Tusk podpisał mimo wcześniejszych zapewnień o tym, że jej nie podpisze, dopóki nie zostaną wyjaśnione wątpliwości zgłaszane przez „stronę społeczną”, w tytule nie miała nawet skótu „ACTA”. Jej nazwa to: „Uchwała w sprawie udzielenia zgody na podpisanie Umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi między Unią Europejską i jej państwami członkowskimi, Australią, Kanadą, Japonią, Republiką Korei, Meksykańskimi Stanami Zjednoczonymi, Królestwem Marokańskim, Nową Zelandią, Republiką Singapuru, Konfederacją Szwajcarską i Stanami Zjednoczonymi Ameryki”. Na swoim blogu prawo.vagla.pl Waglowski relacjonował: „16 listopada, na dwa dni przed... powołaniem przez Prezydenta RP rządu (co nastąpiło 18 listopada – dokładnie w tym dniu pismo MKiDN wpłynęło do Departamentu Rady Ministrów w Kancelarii Prezesa Rady Ministrów). W efekcie «obiegowego» procedowania podjęto więc uchwałę (nie było uwag, pewnie nikt tego pisma nawet nie przeczytał) z dniem 25 listopada”[28].

W obawie przed zbyt pochopnym podejściem do ACTA i na prośbę wielu organizacji pozarządowych 19 stycznia 2012 roku minister administracji i cyfryza-

[27] Zob. http://www.piit.org.pl/_gAllery/11/83/11839/Memo_PIIT_ACTA_finalx.pdf (dostęp: 16.09.2013).

[28] Zob. http://prawo.vagla.pl/node/9631 (dostęp: 16.09.2013).

cji Michał Boni poprosił premiera o ponowną dyskusję nad tą sprawą. Internauci zaczęli się organizować – powstawały strony pod hasłem „Nie dla ACTA" na portalu Facebook, które w szybkim tempie zdobywały członków, jak również przygotowano wzór listu w sprawie ACTA i zachęcano do wysyłania go do posłów ze swoich okręgów. Głos zabrał także Generalny Inspektor Ochrony Danych Osobowych, który stwierdził: „GIODO uznaje podpisanie i ratyfikację konwencji ACTA za niebezpieczne dla praw i wolności określonych w Konstytucji Rzeczypospolitej Polskiej". W swojej opinii GIODO przewiduje, że „na osoby fizyczne, osoby prawne i inne jednostki organizacyjne nakładane będą nieznane dziś prawu polskiemu obowiązki ujawnienia danych osobowych osób fizycznych podejrzewanych o naruszenie norm konwencyjnych"[29].

W nocy 21 stycznia 2012 roku grupa Anonymous („globalna i zdecentralizowana grupa aktywistów internetowych sprzeciwiająca się ograniczaniu wolności obywatelskich, korupcji, konsumpcjonizmowi, cenzurze, *fair use*, (…) czy łamaniu praw zwierząt"[30]) zaatakowała polskie serwisy rządowe, m.in. Sejmu, Agencji Bezpieczeństwa Wewnętrznego, Ministerstwa Obrony Narodowej, Polskiego Stronnictwa Ludowego i innych. Atak zaczął się od strony sejm.gov.pl, na skutek czego serwis ten był niedostępny dla użytkowników. Przez cały dzień 22 stycznia trwały ataki na inne strony rządowe, m.in. Kancelarii Premiera oraz Kancelarii Prezydenta, ale ofiarą stały się również serwisy CERT (Computer Emergency Response Team, odpowiedzialny za reagowanie na wydarzenia, które mogą naruszyć bezpieczeństwo w Internecie) oraz ZAiKS-u (Związku Autorów i Kompozytorów Scenicznych). Jednocześnie grupa Anonymous zagroziła, że jeżeli Polska zgodzi się na uchwalenie ACTA, grupa ujawni „pliki i dokumenty dotyczące wielu polskich osób publicznych". Na koniec w nocy polska grupa Anonymous opublikowała wpis na portalu Twitter o treści: „Przepraszamy wszystkich POSŁÓW i INSTYTUCJE, które czują się urażone atakami. Nie chcemy was wykończyć – chcemy zwrócić waszą uwagę"[31]. Równocześnie 22 stycznia grupa hakerów określająca się mianem „Polish Underground" włamała się na stronę Kancelarii Premiera i zamieściła na nich komunikat: „Internetu nam cenzurować nie będziecie. Praw człowieka nie odbierzecie! Chyba że chcecie, abyśmy naprawdę pokazali swoją prawdziwą siłę ;-)". Grupa przy okazji ujawniła, że login i hasło administratora witryny to „admin" i „admin1". Następnego dnia włamano się do prywatnego laptopa wiceministra administracji i cyfryzacji Igora Ostrowskiego i wykradziono dane[32].

Aby zasygnalizować rządowi swój sprzeciw wobec ACTA, kilkadziesiąt serwisów w Polsce wzięło udział w akcji protestacyjnej. Akcję można było podzielić

[29] Zob. http://www.tvn24.pl/wiadomosci-z-kraju,3/giodo-acta-niebezpieczne-dla-konstytucyjnych-praw-i-wolnosci,198213.html (dostęp: 16.09.2013).

[30] Zob. http://pl.wikipedia.org/wiki/Anonymous_(aktywi%C5%9Bci_internetowi) (dostęp: 16.09.2013).

[31] Zob. http://technologie.gazeta.pl/internet/1,104530,11010982,Tango_Down__trwa_akcja_hakerow _wymierzona_w_strony.html (dostęp: 16.09.2013).

[32] Zob. http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2012/04/jak-wlamano-sie-na-strone-premiera.aspx (dostęp: 16.09.2013).

na trzy rodzaje: banner informacyjny, częściowe zaciemnienie serwisu (odwiedzającym wyświetlała się zaczerniona strona informująca o proteście i zagrożeniach związanych z ACTA, którą można było wyłączyć i przejść do serwisu) lub całkowite wyłączenie serwerów (zasoby serwisów były wówczas niedostępne). W proteście 24 stycznia wzięło udział ponad 2000 stron[33], z czego najpopularniejsze to Allegro, Demotywatory, Wykop, JoeMonster, Antyweb i Kwejk. Protest ten był inspirowany podobną akcją w Stanach Zjednoczonych, przeprowadzoną w styczniu 2012 roku najpierw przez portal Wikipedia, a potem przez portal Reddit, które protestowały przeciwko wprowadzeniu ustaw SOPA (Stop Online Piracy Act) i PIPA (Protect IP Act). Są to dwa kontrowersyjne projekty antypirackich ustaw w Stanach Zjednoczonych, którym – tak samo jak w przypadku ACTA – przeciwnicy zarzucają chęć cenzury Internetu i zagrożenie wolności słowa.

Zamieszanie i krytyka działań polskiego rządu związanych z ACTA doprowadziły do masowych protestów w całej Polsce. Niezadowolenie wyrażane w Internecie wylało się na ulice polskich miast – demonstracje odbyły się w Bydgoszczy, Krakowie, Łodzi, Kielcach, Katowicach, Szczecinie, Trójmieście, Warszawie i we Wrocławiu. Najwięcej, bo aż 15 tysięcy osób protestowało w Krakowie. W Kielcach natomiast pokojowa demonstracja przerodziła się w zamieszki, po których zatrzymano 20 osób.

Ostatecznie do wprowadzenia w życie zapisów ACTA nie doszło. Sprzeciw dużej części społeczeństwa nie pozwolił na gładkie zaakceptowanie ograniczeń w świecie Internetu. Pytanie tylko brzmi, czy w walce z ograniczeniami Internetu trzeba samemu łamać prawo do wolności słowa. Cyberataki, włamania do serwisów to właśnie działania tego typu. Jedno zagrożenie w postaci umowy międzynarodowej minęło, jednak na horyzoncie majaczyła już kolejna próba „usidlenia" sieci.

ITR – powtórka z rozrywki?

Polska została członkiem Międzynarodowego Związku Telekomunikacyjnego (ITU – agenda ONZ) w 1921 roku. Poza członkami-państwami w ITU są również członkowie sektorowi, czyli przedsiębiorstwa, głównie telekomunikacyjne – jest to około 500 firm z różnych krajów. W grudniu 2012 roku Międzynarodowy Związek Komunikacyjny zorganizował konferencję w Dubaju – World Conference on International Telecommunications.

W trakcie konferencji miał być zmieniony traktat międzynarodowy przyjęty podczas World Administrative Telegraphy and Telephone Conference w Melbourne w 1988 roku, który nosi nazwę International Telecommunication Regulations (ITR). Tak jak w przypadku ACTA wielu miało zastrzeżenia co do czytelności i przejrzystości trybu procedowania nad tymi zmianami.

[33] Zob. https://docs.google.com/spreadsheet/pub?hl=en_US&key=0AmbqTnGR_U0JdDNmcWQzcUlyTlBlOTZVYnpBOGFTMHc&hl=en_US&gid=0 (dostęp: 16.09.2013).

Celem zmiany traktatu miało być ustanowienie międzynarodowego zarządzania Internetem, czyli stworzenie nowych regulacji w dotychczas wolnej od tego sieci. W ten sposób ITU rozciągnęłoby swój mandat na regulację sfery praw i wolności użytkowników sieci. Propozycje dotyczyły: ustanowienia nadzoru ITU nad organizacjami obecnie zarządzającymi Internetem; poddania cyberbezpieczeństwa i ochrony danych kontroli międzynarodowej; pozwolenia zagranicznym telekomom na naliczanie opłat za „międzynarodowy" ruch internetowy, co miałoby służyć przychodom państwowych telekomów; uregulowania kwestii wymiany ruchu pomiędzy dostawcami usług internetowych w zakresie stawek i warunków[34]. Ścierają się tutaj dwa podejścia: proregulacyjne proponowane przez rządy i korporacje oraz liberalne reprezentowane przez organizacje pozarządowe, ale też osoby zarządzające takimi firmami jak Google. Eric Schmidt ostro skrytykował plany ustanowienia nowej kontroli nad Internetem: „To byłaby katastrofa... Dla niektórych otwartość oraz interoperacyjność to jedno z największych osiągnięć ludzkości w czasie jej istnienia. (...) jeśli obecny model zarządzania działa dobrze – a tak myślę – nie zmieniałbym [kontroli nad Internetem], a gdybym to robił, byłbym bardzo, bardzo ostrożny" – mówił przedstawiciel Google, podkreślając też, że kosztem regulacji nierzadko jest innowacja[35].

Fundacja Panoptykon jako największy zarzut wobec proponowanego rozwiązania przedstawiała jego nietransparentność i brak dopuszczenia uczestnictwa organizacji społeczeństwa obywatelskiego oraz obywateli bezpośrednio do rozmów. Dostęp do wewnętrznych dokumentów ITU jest sprzedawany „zrzeszonym" członkom korporacyjnym za ogromne sumy pieniędzy, co nie pozwala na swobodny udział w procesie negocjacyjnym. W związku z tym fundacja wystosowała list otwarty do ITU, aby zniesiono bariery w dostępie do informacji i dokumentów negocjacyjnych. Prośba została wysłuchana, ponieważ kilka miesięcy później ITU ujawnił część materiałów, a Ministerstwo Administracji i Cyfryzacji ogłosiło konsultacje społeczne polskiego stanowiska wobec zmian.

Podczas grudniowego szczytu ITU w Dubaju takie kraje jak Rosja, Zjednoczone Emiraty Arabskie, Chiny, Algieria, Arabia Saudyjska i Sudan zgłosiły propozycję definicji nowego terminu: „krajowy segment Internetu" lub dowolnej innej sieci telekomunikacyjnej na terytorium danego państwa. Pozwoliłoby to państwom na pełną regulację Internetu w swoich granicach, od filtrowania treści po wprowadzenie opłat za ruch przychodzący z zagranicy. Rosja, Chiny, kraje arabskie i afrykańskie forsowały zapiski zakazujące anonimowości w Internecie, umożliwiające odcięcie obywatelom dostępu do sieci w razie zagrożenia i cenzurę wypowiedzi. Dodatkowo, gdy uzgodniono, że do traktatu zostaną wpisane prawa człowieka, między innymi Iran i Algieria zaczęły zabiegać, by te zapisy przeredagować. Wzbudziło to zdecydowany sprzeciw USA, Unii Europejskiej, a w tym Polski.

PŁASZCZYZNY

[34] Zob. http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html (dostęp: 16.09.2013).

[35] Zob. http://di.com.pl/news/43934,0,Schmidt_Traktat_ONZ_zagraza_wolnosci_sieci.html (dostęp: 16.09.2013).

Kraje optujące za kontrolą ruchu w sieci już to robią w różnym wymiarze w swoich państwach, w Dubaju chodziło jednak o mandat międzynarodowy. Na przykład w Rosji wprowadzono czarną listę domen, które dostawcy Internetu muszą blokować. Wspominany już przykład z Pakistanu, gdy zablokowano dostęp do YouTube za treści obraźliwe dla islamu, również wpisuje się w ten trend. Co ciekawe, na początku konferencji przyjęto standard Y.2770, który opisuje „wymagania dla głębokiej inspekcji pakietów w sieciach nowej generacji" (inaczej DPI – Deep Packet Inspection). Korzystając z DPI, można nie tylko przeczytać, kto nadał list i do kogo, ale też zapoznać się z jego treścią. Głęboka inspekcja pakietów może być przydatna do mierzenia ruchu lub blokowania konkretnych usług (np. VoIP, gier), lecz także do identyfikowania użytkowników BitTorrenta, którzy publikują materiały w sieci P2P, albo do wykrywania przesyłania konkretnego pliku między użytkownikami. ITU przyjęło zatem standard ewidentnie zagrażający prywatności internautów.

Negocjacje i wprowadzanie zmian do traktatu trwało do samego końca sesji plenarnych. Wiele wskazywało na to, że dojdzie do kompromisu. Mimo że z wielu radykalnych propozycji się wycofano, USA, Wielka Brytania, Kanada, Szwecja oraz Polska zapowiedziały, iż traktatu nie podpiszą. W głosowaniu 77 krajów opowiedziało się za, 33 przeciw, osiem się wstrzymało.

W debacie część z państw intensywnie zabiegała o to, by rozmydlić zapis o prawach człowieka, poszerzając go o zapisy dotyczące prawa państw do dostępu do sieci, część natomiast nadal proponowała zapisy, które mogłyby być zinterpretowane jako odnoszące się do Internetu[36].

Obrady unaoczniły głębokie podziały między państwami dotyczące koncepcji globalnego zarządzania Internetem. Ujawniły one również słabość samego ITU, który ze swoimi procedurami tkwi najwyraźniej w latach siedemdziesiątych ubiegłego wieku. Smaczku dodawały publikacje prasowe towarzyszące wydarzeniu, które zwracały uwagę na to, że sekretarz generalny ITU Hamadoun Touré studiował w ZSRR. Jednocześnie rosyjski prezydent podkreślał, że Rosja była jednym z członków-założycieli ITU, tym samym starając się nadać większe znaczenie swojemu krajowi w negocjacjach. Rosyjskie media przypominały zaś, że USA zbyt często w przeszłości wpływały na ICANN, instytucję zarządzającą dziś systemem domen i adresów internetowych. Minister Michał Boni podsumował: „Zebrały się państwa ITU, czyli agendy ONZ, instytucji, której historia zasadza się na Powszechnej Deklaracji Praw Człowieka, i nagle problemem staje się wpisanie do traktatu poszanowania praw człowieka. Zaczyna się gra o to, jakich sformułowań w tym kontekście użyć. Widać, że są państwa, które mają zasadniczy problem ze zrozumieniem nowej fali demokratycznej i tego, że pokusę upaństwawiania Internetu trzeba odrzucić. Wcześniej Internet był w rękach biznesu, państwa oraz ośrodków naukowych. Dziś trzeba dopisać tu nowego partnera:

[36] Zob. http://wyborcza.biz/biznes/1,101558,13048664,Szczyt_w_Dubaju__Polska_nie_podpisze_traktatu_ITR.html (dostęp: 16.09.2013).

obywateli”[37]. Gdyby zachodnia koalicja przystała na te zapisy, *de facto* dałaby niektórym reżimom międzynarodowy mandat do stosowania cenzury.

Podsumowanie

Dwudziestowieczna idea swobodnego przepływu informacji jest wciąż aktualna, choć dzisiaj dotyczy głównie wolności słowa w Internecie. Internet z jednej strony umożliwia rozwój technik ułatwiających przepływ informacji coraz większym grupom społecznym, ale z drugiej pozwala na sprawowanie nadzoru elektronicznego nad zawartością tych informacji poprzez programy inwigilacji elektronicznej. Przykładowo system XKeyscore ułatwia służbom specjalnym penetrowanie treści wszystkich materiałów dostępnych w Internecie, kontrolowanie poczty, jak i zachowania typowego użytkownika komputera podłączonego do sieci. Staliśmy się zatem beneficjentami postępu naukowo-technicznego umożliwiającego nam swobodny dostęp do całej zawartości Internetu, a jednocześnie sami udostępniamy służbom specjalnym wszystko to, co gromadzimy, tworzymy czy dystrybuujemy ze swojego komputera. W sieci swobodnego przepływu informacji jesteśmy obserwowani jako jej użytkownicy: wszyscy mogą mieć do nas dostęp i nie możemy już bronić swojego prawa do prywatności – chyba że zbuntujemy się i odłączymy komputery.

Ronald Deibert, który kieruje m.in. Citizen Lab i bada problemy związane z cyfrową inwigilacją na University of Toronto, jest autorem książki „Black Code. Inside the Battle for Cyberspace”. Tłumaczy w niej, na czym polega problem po 11 września 2001 roku. Amerykanie przerażeni skalą zamachu dokonali transakcji „wolność i prywatność za bezpieczeństwo”. Uwierzyli, że zwiększenie prerogatyw służb specjalnych wzmoże ich skuteczność w „wojnie z terrorem”[38]. Wynikiem tego może być na przykład program inwigilacji cyfrowej prowadzony przez amerykańską agencję bezpieczeństwa NSA – ujawniony w czerwcu 2013 roku przez byłego pracownika Edwarda Snowdena program PRISM.

Ciekawe, czy twórcy idei swobodnego przepływu informacji wyobrażali sobie, że kiedyś będą mogli mieć tak nieograniczony dostęp do informacji, jaki ma NSA. Jak się okazało, NSA jest w stanie dotrzeć do około 75% całej aktywności internetowej w USA. Agencja przechowuje zawartość niektórych przechwyconych e-maili przesyłanych między sobą przez Amerykanów i wyłapuje krajowe rozmowy wykonywane za pośrednictwem Internetu. Posiada również dostęp do korespondencji użytkowników serwisów internetowych Yahoo, Gmail, Hotmail, AOL, Facebook, YouTube i Skype.

Do tej pory użytkownicy wymieniali się informacjami, opiniami, zawierali nowe i utrzymywali stare znajomości, prowadzili biznes i konsumowali kulturę w przeświadczeniu, że ich działania nie są monitorowane, a każdy, kto chce

[37] T. Grynkiewicz: Klęska w Dubaju, *Gazeta Wyborcza* 2012, nr 293, s. 10.

[38] Zob. http://www.polityka.pl/swiat/komentarze/1545337,1,amerykanska-afera-podsluchowa.read (dostęp: 16.09.2013).

zachować anonimowość i prywatność, jest w stanie czuć się bezpiecznie. Pod otoczką bezpieczeństwa narodowego i walki z terroryzmem stworzono program, który wcale nie różni się od tego, co robią rządy Chin, Iranu czy innych reżimów. Stanowi to *de facto* legitymizację działania dzisiejszych dyktatorów, nawet technologie są te same.

Większości świadomych internautów nie zdziwiła informacja o inwigilacji. Można się było spodziewać, że jeżeli istnieje technologia udostępniająca milionom użytkowników dzielenie się (zwykle darmową) informacją, to treści te muszą przechodzić przez czyjeś serwery i ktoś do tych serwerów może mieć dostęp. Dlatego też Amerykanie nie przejęli się zbytnio rewelacjami Snowdena. Ponad połowa z nich poświęca swoje prawo do prywatności i zgadza się, by rząd ich szpiegował, jeśli ma to zapobiec zamachom terrorystycznym[39].

NSA kontrolująca naszą prywatną korespondencję nie musi być problematyczna. Prawdę mówiąc, nasze dane jej w ogóle nie interesują. Ma do nich pełny dostęp i wykorzystywanie tego przeciwko nam generowałoby koszty większe od zysków. Zresztą jeśli nie mamy złych zamiarów, nie musimy się niczego obawiać. Większym problemem jest informacja, że NSA ma najpewniej dostęp również do zaszyfrowanych danych w Internecie. Z ujawnionych dokumentów wynika, że NSA płaciło firmom IT za zostawianie tzw. *backdoorów* (świadomie pozostawione luki w bezpieczeństwie oprogramowania, którymi można się dostać do naszych danych). Taka informacja może być wykorzystana także przez przestępców – teraz mogą skupiać się na odnajdywaniu celowo umieszczonych luk w programach do szyfrowania treści.

Czy programy typu PRISM oznaczają, że dostępna na całym świecie sieć internetowa jest tak naprawdę pod kontrolą rządu USA? Jeżeli tak, tworzyłoby to ogromną dysproporcję w dostępie do informacji wśród rządów i agencji wywiadowczych poszczególnych krajów. Oznaczałoby to również, że kraje, które do tej pory wykorzystywały oprogramowania i sprzęt produkowane w USA, mogą się czuć zagrożone, a bezpieczne korzystanie z nich zostało zupełnie skompromitowane. 11 czerwca nowa koalicja aktywistów, organizacji i firm internetowych Stop Watching US, w skład której weszły m.in. Mozilla, Reddit, Greenpeace USA, National Coalition Against Censorship czy Electronic Frontier Foundation, opublikowała list do Kongresu Stanów Zjednoczonych. Postuluje w nim zaprzestanie inwigilacji, powołanie specjalnej komisji do zbadania jej zakresu i pociągnięcie do odpowiedzialności urzędników, którzy zdaniem koalicji łamali amerykańską konstytucję. Jaki wpływ na ideę swobodnego przepływu informacji i wolność słowa w Internecie będą miały w przyszłości PRISM oraz kolejne projekty międzynarodowej legislacji typu ACTA i ITR? Czas pokaże. A NSA i tak już pewnie zna na to pytanie odpowiedź.

[39] Zob. http://swiat.newsweek.pl/wujek-sam-patrzy-przez-prism,105385,1,1.html (dostęp: 16.09.2013).

Bibliografia

Castells M.: Społeczeństwo sieci, Wydawnictwo Naukowe PWN, Warszawa 2011.
Cohen J., Schmidt E.: The New Digital Age: Reshaping the Future of People, Nations and Business, Alfred A. Knopf, New York 2013.
de Sola Pool I.: Technologies of Freedom, Belknap Press of Harvard University Press, Cambridge–Londyn 1983.
Elmer-Dawitt P.: First Nation in Cyberspace, *TIME Internation* 1993, nr 49.
Grynkiewicz T.: Klęska w Dubaju, *Gazeta Wyborcza* 2012, nr 293, s. 10.
La Rue F.: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27, 16 maja 2011.
Lax S.: Access denied in the information age, Palgrave, New York 2001.
Levinson P.: Nowe nowe media, Wydawnictwo WAM, Kraków 2010.
McLuhan M.: Zrozumieć media. Przedłużenia człowieka, Wydawnictwo Naukowo-Techniczne, Warszawa 2004.
Nordenstreng K., Varis T.: The nonhomogenity of the national state and the international flow of communication, [w:] G. Gerbner, L.P. Gross, W.K. Melody (red.): Communications Technology and Social Policy. Understanding the New "Cultural Revolution", Wiley, New York 1973.
Olędzki J.: Komunikowanie w świecie, Wydawnictwo ASPRA-JR, Warszawa 2001.
Schiller H.J.: Communication and Cultural Domination, International Arts and Sciences Press, New York 1976.
Segev E.: Google and the Digital Divide: The Biases of Online Knowledge, Woodhead Publishing, Cambridge 2010.
UNESCO, World Communication and Information Report, Paryż, 1999–2000.