STUDIA PRAWNO-EKONOMICZNE, t. LXXXV, 2012
PL ISSN 0081-6841 s. 113–140

Joanna KULESZA*

CENZURA TREŚCI ELEKTRONICZNYCH A MIĘDZYNARODOWA ODPOWIEDZIALNOŚĆ PAŃSTWA ZA NARUSZENIE PRAW CZŁOWIEKA

1. Wolność dostępu do informacji

Wolność wypowiedzi zajmuje uznane miejsce w katalogu praw człowieka. Jego treść określona została w podobny sposób w szeregu dokumentów prawa międzynarodowego – powielany jest schemat z art. 19 niewiążącej Powszechnej Deklaracji Praw Człowieka. W myśl postanowień tego przepisu, na prawo wolności wyrażania opinii składają się trzy wolności cząstkowe: prawo do swobody posiadania niezależnej opinii, prawo do otrzymywania informacji i poglądów wyrażanych przez innych (kluczowe dla czynionych rozważań) oraz prawo do rozpowszechniania informacji i poglądów. Wolność słowa we wszystkich tych aspektach może być realizowana – według cytowanego dokumentu – „wszelkimi środkami, bez względu na granice". W analogiczny sposób zakres wolności wypowiedzi określają dokumenty twardego prawa międzynarodowego, przykładowo: art. 19 MPPOP[1]. Tu także zapisano prawo każdego człowieka do posiadania „bez przeszkód" własnych poglądów (ust. 1) oraz dzielenia się nimi, to znaczy wyrażania opinii (ust. 2). Jako elementy tego prawa wskazano „swobodę poszukiwania, otrzymywania i rozpowszechniania wszelkich informacji i poglądów, bez względu na granice państwowe, ustnie, pismem lub drukiem, w postaci dzieła sztuki bądź w jakikolwiek inny sposób według własnego wyboru" (ust. 2). Mimo iż wykładnię tego artykułu można

* Dr, Katedra Prawa Międzynarodowego i Stosunków Międzynarodowych, Uniwersytet Łódzki.

[1] Międzynarodowy Pakt Praw Obywatelskich i Politycznych, Dz.U. z 1977 r., Nr 38, poz. 167 [dalej: **MPPOP**].

oprzeć na treści Rezolucji Rady Praw Człowieka ONZ 12/16 o wolności opinii i słowa[2], to i tak jego praktyczna aplikacja budzi wiele kontrowersji[3]. Niezależnie jednak od wątpliwości pozostaje bezsporne, że uniemożliwianie dostępu do treści elektronicznych godzi bezpośrednio w co najmniej jeden z trzech elementów składowych wolności słowa – w prawo do otrzymywania informacji. Ograniczanie wolności słowa czy prawa otrzymywania informacji nie oznacza jednak automatycznie bezprawności takiej ingerencji. Wolność słowa nie jest bowiem prawem bezwzględnym. Jej ograniczenia przewidziane zostały zarówno w Powszechnej Deklaracji Praw Człowieka (art. 29 ust. 2)[4], jak i w Międzynarodowym Pakcie Praw Obywatelskich i Politycznych (art. 19 ust. 3)[5]. Wolność słowa (a więc także wolność otrzymywania informacji) może być ograniczana tylko w szczególnych sytuacjach, to jest m.in. w imię bezpieczeństwa publicznego czy ochrony moralności. Generalne ograniczenie czy wyłączenie możliwości realizacji tego prawa może być uznane za sprzeczne z wymogami art. 19 ust. 3 MPPOP[6]. Wniosek taki nie jest jedynym możliwym:

---

[2] Resolution adopted by the Human Rights Council, Freedom of opinion and expression (A/HRC/RES/12/16), 2.10.2009 r.

[3] Por. ogólnie np.: **W. Sadurski**, *Freedom of Speech and Its Limits*, Kluwer Academic Publishers, Dordrecht 2002.

[4] Który stanowi, że „w korzystaniu ze swych praw i wolności każdy człowiek podlega jedynie takim ograniczeniom, które są ustalone przez prawo wyłącznie w celu zapewnienia odpowiedniego uznania i poszanowania praw i wolności innych i w celu uczynienia zadość słusznym wymogom moralności, porządku publicznego i powszechnego dobrobytu demokratycznego społeczeństwa".

[5] Realizacja praw przewidzianych w pkt 2 niniejszego artykułu pociąga za sobą specjalne obowiązki i specjalną odpowiedzialność. Może ona w konsekwencji podlegać pewnym ograniczeniom, które powinny być jednak wyraźnie przewidziane przez ustawę i które są niezbędne w celu: (a) poszanowania praw i dobrego imienia innych; (b) ochrony bezpieczeństwa państwowego lub porządku publicznego albo zdrowia lub moralności publicznej.

[6] W reżimie Europejskiej Konwencji Praw Człowieka (tj.: Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności z 1950 r., Dz.U. z 1993 r., Nr 61, poz. 284 [dalej: **EKPC**], prawo swobody wypowiedzi konstytuuje jej art. 10. Towarzyszące mu orzecznictwo ETPC implikuje pozytywny obowiązek państw do zapobiegania ingerencji w prawo jednostki do swobodnego komunikowania się, także jeśli ingerencja ta wynikałaby z relacji prywatnoprawnych. Por. np. wyrok ETPC z dnia 16 grudnia 2008 r. w sprawie *Khurshid Mustafa and Tarzibachi v. Szwecja*, nr skargi 23883/06, gdzie Trybunał uznał się za właściwy do oceny wyroków sądowych zapadłych w indywidualnych sprawach prywatnych, gdy krajowa praktyka sądowa nie gwarantuje korzystania z praw przepisanych Konwencją. Zob. też wyrok ETPC z 28 czerwca 2001 r. w sprawie *VgT Verein Gegen Tierfabriken v. Szwajcaria*, nr skargi 24699/94, gdzie ETPC ustalił, że „może istnieć immanentny (ang. *inherent*) pozy-

o ile np. w reżimie Europejskiej Konwencji Praw Człowieka dopuszczalne jest „uchylenie stosowania zobowiązań" wynikających z Konwencji w przypadku „wojny lub innego niebezpieczeństwa publicznego zagrażającego życiu narodu"[7], o tyle prawo wolności wypowiedzi nigdy nie może być wyłączone względem „działalności politycznej cudzoziemców"[8], a więc także ich prawa do przekazywania informacji na terytorium państwa zmagającego się z niebezpieczeństwem publicznym.

OpenNetInitiative – organizacja zajmująca się monitorowaniem krajowych ograniczeń dostępu do treści Internetu[9] – wskazuje na cztery grupy deklarowanych przez państwa uzasadnień blokowania dostępu do elektronicznych treści[10]. O ile następcze blokowanie treści z tzw. względów społecznych (oparte na normach etycznych właściwych krajowej wspólnocie, wyrażanych przepisami prawa) budzi względnie mało kontrowersji, o tyle filtrowanie ze względów politycznych czy bezpieczeństwa, jak i blokowanie dostępu do określonych narzędzi informatycznych, potencjalnie pozwalających na naruszenie krajowego prawa, niesie krytykę międzynarodowych organizacji chroniących praw człowieka[11]. Blokowanie dostępu do treści elektronicznych rzadko odbywa się bezpośrednio z inicjatywy władz ustawodawczych czy wykonawczych; czynią to dostawcy usług na podstawie przepisów prawa krajowego[12], choć wyjątkowo może ono nastąpić także w drodze decyzji sądu[13].

tywny obowiązek" państw zagwarantowania praw konwencyjnych poprzez wprowadzenie implementujących je regulacji krajowych.

7 Art. 15 EKPC.

8 Art. 16 EKPC.

9 Inicjatywa OpenNet to współpraca oparta na partnerstwie trzech instytucji akademickich: Citizen Lab z Munk Centem for International Studies z Uniwersytetu w Toronto, Bergman Center for Internet & Society w Harvard Law School oraz Advanced Network Research Group w ramach Cambridge Security Programme na Uniwersytecie Cambridge.

10 **R. Faris**, **N. Villeneuve**, *Measuring Global Internet Filtering*, [w:] **R.J. Deibert**, **J.G. Palfrey**, **R. Rohozinski**, **J. Zittrain** (eds), *Access Denied: The Practice and Policy of Global Internet Filtering*, MIT Press, Massachussetts 2008, s. 9.

11 Por. np.: **H. Noman**, **J.C. York**, *West Censoring East: The Use of Western Technologies by Middle East Censors*, OpenNetwork Inititive 2011, http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011 dostęp: 1.02.2012 r.

12 Por.: **J. Zittrain**, **J.G. Palfrey**, *Internet Filtering: The Politics and Mechanisms of Control*, [w:] **R.J. Deibert**, **J.G. Palfrey**, **R. Rohozinski**, **J. Zittrain** (eds), *Access Denied…*, s. 32 i n.

13 Np. decyzja sądu włoskiego o blokowaniu witryny PirateBay w związku z możliwością naruszenia praw autorskich przez jej użytkowników, np.: *Italy cracks down on Pirate Bay*,

2. Cenzura treści elektronicznych – technologia i legislacja

„Filtrowanie Internetu" to termin określający szeroki wachlarz zachowań[14]. Pierwotnie dotyczył on przede wszystkim praktyk państw niedemokratycznych, takich jak Chiny, Iran czy Egipt, gdzie na dostawców usług internetowych (*Internet Service Providers* – ISPs) ustawodawca nakładał, mocą prawa, obowiązek uniemożliwiania dostępu do określonych kategorii treści (pornograficznych, zagrażających bezpieczeństwu publicznemu czy moralności)[15]. Ten obowiązek oznacza, że podmioty oferujące dostęp do globalnej sieci muszą, pod groźbą sankcji, weryfikować treści osiągalne dla ich użytkowników. Usługodawcy czynią zadość tym wymaganiom na wiele sposobów, najczęściej wykorzystując programy filtrujące[16], działające w oparciu o słowa kluczowe[17], „czarne listy" zakazanych adresów internetowych lub „białe listy" adresów

New York Times 14.08.2008 r., http://www.nytimes.com/2008/08/14/technology/14iht–webpirate.15301147.html dostęp: 2.02.2012 r.

[14] Kontrolowanie dostępu do określonych kategorii elektronicznych treści obejmuje, obok stosowania środków informatycznych, także użycie instrumentów prawnych (dla uzupełnienia lub legitymizowania ingerencji technicznej), jak i działania pozaprawne i niejawne, w tym wykorzystanie usług podmiotów prywatnych. Obecnie filtrowanie Internetu to także hacking i wirusowanie komputerów zawierających szkodliwe treści czy ataki DDoS na serwery je hostujące (często stosowane względem witryn w języku rosyjskim). Por.: **R. Deibert**, **J.G. Palfrey**, **R. Rohozinski**, **J. Zittrain** (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, MIT Press, Massachussetts 2010, s. 6–7.

[15] W Chinach zakaz obejmuje treści, które mogłyby zagrozić „narodowej jedności", zaś Birma, Egipt i Malezja zakazują treści krytykujących partię rządzącą. Liberia żąda blokowania witryn, które zawierają „materiały antyliberyjskie", podczas gdy Zimbabwe filtruje strony administrowane poza granicami państwa, publikujące jakiekolwiek treści, które „mogłyby wzbudzić niepokój lub smutek". Por.: Privacy International and the GreenNet Educational Trust, *Silenced, An international Report on Censorship and Control of the Internet*, Stanford 2003, s. 20.

[16] Najczęściej będące produktami firm ze Stanów Zjednoczonych. Cisco Systems (CISCO) stanowiło jeden z filarów rozwoju Internetu w Chinach. Firma opracowała nie tylko oprogramowanie dla chińskich *root*-serwerów, ale także specjalnie na potrzeby rządu programy „wspomagające" krajową sieć edukacyjną. CISCO opracowuje także „Next-Generation Network", tzw. ChinaNet Next Carrying Network, CN2. Za informacją producenta dostępną na jego stronie domowej: *Cisco Announces IP Next-Generation Network Advancements for Service Providers*, San Jose, 5.12.2004, http://newsroom.cisco.com/dlls/2004/prod_120604.html dostęp: 5.11.2012 r.

[17] Jeśli w treści nazwy domenowej lub witryny pojawiają się określone słowa kluczowe (np. *seks* w przypadku treści pornograficznych czy *Falun Gong* – w przypadku cenzury politycznej), to dostęp do takiej witryny był automatycznie blokowany. Użytkownikom prezentowany

dozwolonych[18]. Niektórzy posiłkują się wsparciem licznych administratorów (pracowników i ochotników) śledzących i weryfikujących na bieżąco udostępnianą zawartość Internetu[19].

Filtrowanie Internetu było od samego początku oceniane negatywnie[20]. Wskazywano, że taka praktyka nie tylko narusza wolność wypowiedzi, ale także jest sprzeczna z celem powstania sieci globalnej[21]. Ideą twórców Internetu było utworzenie platformy służącej swobodnej, nieograniczonej wymianie myśli. Zobligowanie dostawców usług do antycypowania, które z udostępnianych przez nich treści mogą zostać uznane przez sądy i urzędy państwowe za sprzeczne z dyspozycją (często bardzo rozbudowanych) przepisów prawa krajowego, spowodowało, że prewencyjna cezura usługodawców z reguły obejmowała pokaźny zasób elektronicznych treści, niwecząc w ten sposób pierwotny zamysł „Ojców Internetu". W imię wolności słowa, zakaz wprowadzania prewencyjnej cenzury treści elektronicznych, dokonywanej przez dostawców usług elektronicznych, uznano za immanentną część swobód demokratycznego państwa[22]. Ani w Europie, ani w Ameryce Północnej dostawcy usług elektronicznych nie są prawnie zobligowani do tego, by uprzednio[23] weryfikować, jakie treści udostępniają swoim użytkownikom. Prywatna cenzura

był komunikat o tymczasowej lub trwałej niedostępności witryny z powodów technicznych. Por.: **R. Deibert**, **J.G. Palfrey**, **R. Rohozinski**, **J. Zittrain** (eds), *Access Controlled*..., s. 4–5.

[18] Por.: *ibidem*, s. 529–530.

[19] *Ibidem*, s. 552.

[20] Por. np. OpenNet Initiative, *A Starting Point: Legal Implications of Internet Filtering*, Toronto, Cambridge, Harvard 2004, s. 8–9.

[21] *Ibidem*.

[22] Por. np. Deklaracja Komitetu Ministrów Rady Europy dotycząca ochrony wolności wypowiedzi i informacji oraz wolności zgromadzeń w związku z nazwami domenowymi, przyjęta 21.09.2011 r., pkt 4 i 5: „Działania państwa, które ogranicza lub zakazuje dostępu do określonych treści internetowych stanowi ingerencję w prawo wolności wypowiedzi i prawo otrzymywania i przekazywania informacji. [...] W szczególności [...] państwa nie powinny, poprzez ogólne blokowanie i filtrowanie treści, wykonywać uprzedniej kontroli treści udostępnianych w Internecie, chyba że działania te podejmowane są na podstawie wstępnej lub ostatecznej decyzji w sprawie niezgodności z prawem takich treści, podjętej przez właściwe władze krajowe i w pełnym poszanowaniu ściśle określonych warunków z Art. 10 ust. 2 Europejskiej Konwencji Praw Człowieka. Środki te powinny dotyczyć jasno określonych treści i powinny być proporcjonalne".

[23] Por. np.: procedura *notice-and-take down*, opisana np. w polskiej ustawie o świadczeniu usług drogą elektroniczną (Dz.U. z 2002, Nr 144, poz. 1204), art. 12–15, która obliguje usługodawcę do uniemożliwienia dostępu do treści naruszających przepisy prawa niezwłocznie po nabyciu wiedzy o ich bezprawnym charakterze.

prewencyjna wciąż jest tu piętnowana jako nielegitymizowane ograniczenie wolności słowa[24].

Jednak czas zatarł tę wyraźna granicę między podejściem legislatorów ze Wschodu i Zachodu do cenzury sieci. Czy to powołując się na walkę z międzynarodowym terroryzmem, czy też na ochronę interesów dysponentów praw autorskich, porządki prawne coraz większej liczby państw[25] przewidują możliwość ograniczenia dostępu do kategorii treści elektronicznych określonych przez ustawodawcę w przepisach prawa lub wskazanych przez usługodawców w regulaminach świadczenia usług[26]. Wciąż funkcjonującą regułą jest brak zobowiązania dostawców do prewencyjnej kontroli dostępnych treści, co w praktyce oznacza, że powinni oni uniemożliwiać dostęp wyłącznie do tych materiałów, o których wiedzą, że mają bezprawny charakter[27]. Jednocześnie, ze wzmożoną siłą, na europejskich salach sądowych toczy się batalia o to, ile dostawcy wiedzieć powinni, a więc, w jakim zakresie mają kontrolować wymianę realizowaną przez swoich użytkowników[28].

Blokowanie dostępu do pewnych kategorii treści elektronicznych na określonym terytorium to temat aktualny i kontrowersyjny[29]. Argumenty

---

[24] Por.: **J. Zittrain**, **J.G. Palfrey**, *Reluctant Gatekeepers, Corporate Ethics on a Filtered Internet*, [w:] **R.J. Deibert**, **J.G. Palfrey**, **R. Rohozinski**, **J. Zittrain** (eds), *Access Denied*…, s. 120–123.

[25] Zob.: mapa filtrowania Internetu na świecie, http://map.opennet.net/, dostęp 1.02.2012 r.; OpenNetInitiative, zob. też: lista „wrogów Internetu", *Reporterzy bez Granic*, http://en.rsf.org/internet.html dostęp 1.02.2011 r.

[26] Por.: **J. Zittrain**, **J.G. Palfrey**, *Internet Filtering*..., s. 32 i n.

[27] Por. przyp. 10.

[28] Por. wyrok ETS z dnia 24 listopada 2011 r. w sprawie *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, sygn. C-70/10, gdzie ETS uznał nakaz sądowy dokonywania uprzedniej kontroli treści pobieranych i udostępnianych przez usługobiorców, nałożony na belgijskiego usługodawcę, za sprzeczny z prawem wspólnotowym.

[29] Także w Polsce toczy się wokół niego ożywiona debata. Zobacz np.: Stanowisko Fundacji „Dzieci Niczyje" w sprawie art. 21 dotyczącego blokowania pornografii dziecięcej w Internecie, zawartego w roboczej wersji Dyrektywy dotyczącej zwalczania nadużyć seksualnych, wykorzystywania seksualnego dzieci oraz dziecięcej pornografii, opublikowanej przez Komisję Europejską w marcu 2010 r., http://www.dzieckowsieci.pl/repository/newsy/blokowanie pornografii dziecięcej w Internecie – stanowisko FDN.pdf dostęp: 1.02.2012 r.; por. też: Petycja przeciwko projektowi Komisji Europejskiej blokowania treści w Internecie: *Usuwanie, nie blokowanie*, Fundacja Panoptykon 2011 r., http://www.panoptykon.org/content/petycja-przeciwko-projektowi-komisji-europejskiej-blokowania-tre-ci-w-internecie-usuwanie-ni dostęp: 1.02.2012 r..

przywoływane zarówno przez zwolenników, jak i przeciwników blokowania treści internetowych, opisane poniżej, są tak samo ważkie.

Przeciwnicy tej formy cenzury treści elektronicznych podnoszą, że blokowanie dostępu do określonych treści jest nieskuteczne, a jednocześnie generuje zbędne, wysokie koszty wynikające z konieczności tworzenia i stosowania zaawansowanego oprogramowania filtrującego. Co więcej – jak nie bez racji podnoszą zwolennicy całkowitej wolności słowa w sieci – blokowanie nie rozwiązuje prawdziwych problemów, które są jedynie odzwierciedlane w internetowych przekazach[30]. W dyskusji na temat cenzury elektronicznych treści pojawia się także argument ryzyka, jakie niesie ze sobą wszelka forma cenzury. Legitymizując jakikolwiek podmiot do ograniczania dostępu do informacji, tworzy się niebezpieczny wyjątek, który wykorzystany może zostać przez władze czy organizacje upoważnione do nadzorowania jego wykonywania w celu ograniczenia dostępu do treści innych niż wskazane w dyspozycji przepisu uzasadniającego stosowanie wyjątku. „Czarne listy" blokowanych treści są co do zasady tajne (tworzone przez policję wspólnie z organizacjami społecznymi, np. stowarzyszeniami czy fundacjami przeciwdziałającymi pedofilii), nie sposób więc zweryfikować, jakie adresy faktycznie zawierają i czy nie służą jako pretekst do ograniczenia dostępu do treści niezgodnych z polityką rządu lub zawierających jego krytykę. Jedynie nieograniczony dostęp do treści elektronicznych ochronić może przed takim ryzykiem.

Zwolennicy ograniczania dostępu do treści elektronicznych podnoszą, że choć stosowane technologie są niedoskonałe, to także w ten sposób – ograniczając dostęp do np. pornografii dziecięcej – należy walczyć z propagowaniem określonych treści, uznanych za szkodliwe. Walkę tę należy prowadzić *on-line* tak samo, jak dzieje się to w świecie pozawirtualnym[31]. Uniemożliwianie dostępu do elektronicznych treści naruszających krajowe prawo to jeden ze sposobów walki z przestępczością, zaś fakt ograniczonej skuteczności tej metody nie powinien decydować o rezygnacji z niej (podobnie, jak niska skuteczność w przeciwdziałaniu handlu substancjami niedozwolonymi nie determinuje rezygnacji z prewencji i ścigania narkotykowych gangów). Wśród propagatorów tych poglądów są nie tylko przedstawiciele rządów czy

[30] *Ibidem*.

[31] Por.: **J. Weckert**, *What is so Bad about Internet Content Regulation?*, Ethics and Information Technology 2000/2 (2), s. 105–111, który uzasadnia wprowadzenie cenzury treści elektronicznych w Australii.

organów ścigania, ale także firmy telekomunikacyjne, które w regulaminach oferowanych usług zawierają klauzule informujące o stosowaniu filtrów czy programów filtrujących, uniemożliwiających dostęp do określonych treści, uznanych za niezgodne z przepisami krajowego prawa.

3. Precedens egipski – powszechna blokada dostępu do Internetu

W lutym 2011 r. władze ogarniętego zamieszkami Egiptu zdecydowały o wprowadzeniu całkowitej blokady dostępu do Internetu dla odciętych już od innych mediów mieszkańców terytorium państwa. Cel ten został w pełni osiągnięty, co było możliwe dzięki zastosowaniu niepraktykowanego nigdzie indziej i nigdy wcześniej sposobu. Władze bezpośrednio nakazały dostawcom usług internetowych zaprzestania działalności[32]. Żadne państwo, jak dotąd, nie „wyłączyło" Internetu swoim mieszkańcom; autokracje takie, jak Kuba czy Korea Płn., konsekwentnie ograniczają do niego fizyczny dostęp, kontrolując ilość komputerów *on-line* czy dostęp do nich obywateli. Reakcja międzynarodowa na egipski precedens była również wyjątkowa. W kilka dni po wprowadzeniu blokady amerykańska firma Google[33] stworzyła swoim użytkownikom znajdującym się w Egipcie techniczną możliwość obejścia blokady dostępu do Internetu, nałożonej przez władze[34]. Zastosowane rozwiązanie było nieskomplikowane[35], jednak niespodziewanie szybko przyniosło zamierzony

[32] Jak podała firma Renesys specjalizująca się w badaniach nad szpiegostwem w sieci, rząd Egipski prawdopodobnie nakazał dostawcom usług internetowych odłączenie wszystkich międzynarodowych połączeń internetowych. Wykonanie tej decyzji nie wpłynęło jednak na międzynarodowy ruch danych elektronicznych. **J. Cowie**, *Egypt Leaves the Internet*, Rensys 27.01.2011, http://www.renesys.com/blog/2011/01/egypt–leaves–the–internet.shtml dostęp: 1.02.2012 r.

[33] Wykorzystując technologię zakupionej niedawno firmy zalążkowej (*start-up*) SayNow, we współpracy z serwisem Twitter (własnością innej amerykańskiej firmy Obvious).

[34] ps, PAP, *Google pomaga Egipcjanom – umożliwia komunikowanie przez Twitter*, G.W., 1.02.2011, http://wiadomosci.gazeta.pl/Wiadomosci/1,80277,9034000, Google_pomaga_Egipcjanom__umożliwia dostęp: 1.02.2011 r.

[35] System oparty jest na wykorzystaniu dwóch konkretnych międzynarodowych numerów telefonicznych – informacja pod nie przekazana zostaje automatycznie, niezwłocznie zamieszczona na serwisie Twitter, ze słowem kluczowym: #egipt. Jak poinformował przedstawiciel Google, przekazywanie w ten sposób informacji nie wymaga połączenia z Internetem. Informacje te dostępne są także w wersji audio – można ich wysłuchać, dzwoniąc na te same numery

cel: po niecałych 24 godzinach dostęp do Internetu i innych mediów w całym Egipcie, decyzją władz państwowych, został przywrócony.

Ten incydent w pełni obrazuje meritum prawnego problemu z filtrowaniem Internetu. Nie budzi bowiem wątpliwości, że praktyka władz Egiptu stanowiła poważną ingerencję w prawo dostępu do informacji jego mieszkańców. Jednocześnie reakcja amerykańskiej firmy może być uznana za pierwszy przykład realizacji zapowiedzianej na początku 2010 r. „doktryny Clinton" – polityki Stanów Zjednoczonych skierowanej przeciwko cenzurze Internetu i państwom ją praktykującym[36]. Opisany stan faktyczny zmusza do zapytania o przewidziany w prawie międzynarodowym zakres ochrony prawa dostępu do informacji jako elementu wolności słowa oraz ewentualnej odpowiedzialności państwa za inicjowanie cenzury elektronicznych treści. Czy państwo może zostać pociągnięte do odpowiedzialności międzynarodowej za ograniczenie prawa dostępu do informacji osobom w jego jurysdykcji, czy raczej uprawnienie to mieści się w jego kompetencjach władczych (*acta de iure imperii*) i jako takie nie podlega ocenie innych państw? Odpowiedź na to pytanie niesie analiza zakresu ochrony swobody wypowiedzi, przewidziana w prawie międzynarodowym.

4. Immunitet państwa a blokada treści elektronicznych

Należy ustalić, czy ograniczenie dostępu do sieci globalnej, zastosowane przez władze Egiptu, mieści się w ramach czynności chronionych immunitetem państwa, a więc, czy pozostaje w wyłącznej kompetencji państwa. Współcześnie konstrukcja immunitetu państwa zakłada, że władze państwowe mogą albo wykonywać wyłączne uprawnienia przysługujące państwom w świetle prawa międzynarodowego (*acta de iure imperii*)[37], albo też działać na arenie międzynarodowej – tak, jak podmioty prawa prywatnego, korzystając z kompetencji niezastrzeżonych dla państw (*acta de iure gestionis*)[38]. Nie ulega wątpliwości, że urzędowy nakaz zaprzestania działalności dostawców

telefoniczne lub wchodząc na stronę internetową: twitter.com/speak2tweet. ps, PAP, *Google pomaga Egipcjanom…*

[36] **J. Kulesza**, *Amerykańsko-chiński spór o cenzurę w Internecie*, PiP 2010/6, s. 29.

[37] Takich, jak przede wszystkim sprawowanie władzy ustawodawczej, wykonawczej i sądowniczej czy korzystanie ze zdolności kontraktowej czy prawa legacji.

[38] Podejmując np. działalność gospodarczą. Por. np.: **A. Wyrozumska**, **W. Czapliński**, *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Warszawa 1999, s. 231.

usług internetowych, ustanowiony przez władze Egiptu 27 stycznia 2011 r., jest działaniem władczym – jest przejawem sprawowania władzy państwowej. Jako taka, decyzja o całkowitej blokadzie treści elektronicznych w Egipcie nie może być przedmiotem oceny władz innego państwa. Co więcej, ograniczenie dostępu do treści elektronicznych, wykonywane na własnym terytorium przez podmioty pozostające w terytorialnej jurysdykcji suwerena, nie budzi wątpliwości. Władze Egiptu[39] wykonywały więc swoją suwerenną władzę, wprowadzając blokadę.

Odmienną kwestią pozostaje ocena jej zakresu (proporcjonalności) oraz zgodności z międzynarodowymi standardami ochrony praw człowieka (np. ewentualnego naruszenia prawa wolności słowa i dostępu do informacji mieszkańców Egiptu). Jak już wspomniano, prawo dostępu do informacji może być ograniczane w szczególnych przypadkach oraz w indywidualnych sprawach. Generalna odmowa dostępu do mediów (w tym Internetu) uznana powinna zostać za naruszenie międzynarodowego zobowiązania Egiptu. Jednocześnie warto już w tym miejscu wskazać, że transgraniczność globalnej sieci elektronicznej determinuje w znaczący sposób pojmowanie granic suwerennej władzy państwowej, wymuszając kolejną redefinicję kluczowego dla prawa międzynarodowego pojęcia suwerenności. Analiza konsekwencji, jakie specyfika struktury sieci globalnej niesie dla pojęcia suwerenności państwa została przeprowadzona na końcu niniejszego wywodu[40].

Analizując dalej *casus* Egiptu, należy wskazać, że nawet jeśli jego władze dopuściły się naruszenia międzynarodowego zobowiązania do poszanowania prawa dostępu do informacji mieszkańców państwa, to i tak w praktyce taka kwalifikacja działania Prezydenta Mubaraka jest mało prawdopodobna. Pomimo iż Egipt pozostaje stroną Międzynarodowego Paktu Praw Obywatelskich i Politycznych (MPPOP) i ciąży na nim bezpośrednie zobowiązanie do poszanowania prawa wolności wypowiedzi (wywodzone z art. 19 MPPOP), to istniejące międzynarodowe procedury ochrony praw człowieka i praktyka ich stosowania dają małe nadzieje na uznanie ekstensywnej egipskiej cenzury Internetu (ograniczenia prawa do komunikacji), także w połączeniu z innymi metodami ograniczania dostępu do informacji, stosowanymi przez władze tego

[39] Nie ma wątpliwości, że władza nie została formalnie odebrana prezydentowi Mubarakowi i podległym mu urzędnikom w dniu wprowadzenia blokady, a fakt skutecznego „odłączenia" Egiptu od Internetu może świadczyć o efektywności sprawowanej władzy.

[40] Por. pkt 7.

państwa za pogwałcenie prawa międzynarodowego. Dzieje się tak, mimo iż wspomniana Rezolucja Rady Praw Człowieka ONZ 12/16 o wolności opinii i słowa[41] zakazuje państwom-stronom nakładania ograniczeń na prawo do pokojowego gromadzenia się oraz na dostęp i wykorzystywanie technologii informacyjnych[42].

Zarówno procedura skargi międzynarodowej, jak i procedury specjalne stworzone w ramach ONZ dla ochrony praw człowieka, inicjowane są co do zasady[43] przez Radę Praw Człowieka, która obecnie zdominowana jest przez państwa afrykańskie i muzułmańskie - praktykujące surowe ograniczenia wolności słowa, wspierane przez Rosję i Chiny[44]. W tym kontekście szansa na uzyskanie międzynarodowej autoryzacji działań sankcjonujących ekstensywne praktyki cenzorskie Egiptu wydają się nikłe. Bez takiej autoryzacji wszelkie działania zmierzające do ograniczenia swobody działania władz egipskich pozostają niezgodne z prawem międzynarodowym. Nawet kontrowersyjna konstrukcja „interwencji humanitarnej", która bez autoryzacji Rady Bezpieczeństwa ONZ dopuszcza użycie siły przez jedno lub kilka państw w obronie praw niektórych człowieka, nie może tu znaleźć zastosowania, bowiem prawo do wolności słowa, swobodnej komunikacji czy wolność zgromadzeń (w odróżnieniu np. od zakazu ludobójstwa) nie posiadają charakteru norm peremptoryjnych[45].

Zważywszy poczynione uwagi, należy uznać, że nawet jeśli wdrożona w Egipcie blokada dostępu do Internetu (także w kontekście blokady innych mediów) zostałaby uznana za pogwałcenie prawa międzynarodowego, to brakuje skutecznych środków sankcjonujących to pogwałcenie. Jak więc należy ocenić zachowanie Google, zwłaszcza w kontekście wspomnianych deklaracji Sekretarz Stanu?

---

[41] Resolution adopted by the Human Rights Council, Freedom of opinion and expression (A/HRC/RES/12/16), 2.10.2009 r.

[42] Pkt (p) (iii).

[43] Z uwzględnieniem postanowień Protokołów Dodatkowych.

[44] Por.: **R. Evans**, *U.N. chief tells rights body drop rhetoric, blocs*, Reuters, 12.12.2008 r., http://www.reuters.com/article/2008/12/12/us–un–rights–idUSTRE4BB67820081212 dostęp: 1.02.2012 r.

[45] Por. **J. Kranz**, *Nowe perspektywy stosowania siły w stosunkach międzynarodowych*, [w:] **J. Menkes** (red.), *Prawo międzynarodowe – problemy i wyzwania. Księga pamiątkowa Profesor Renaty Sonnenfeld-Tomporek*, Warszawa 2006, s. 349–350. Interwencja taka mogłaby zostać uznana za dopuszczalną, gdyby miały miejsce akty ludobójstwa czy zbrodni wojennych.

5. Doktryna Clinton

Dnia 21 stycznia 2010 r. Sekretarz Stanu USA Hilary Clinton wypowiedziała wojnę cenzorom Internetu. Jej wystąpienie w nieprzypadkowo wybranym muzeum wolności słowa (Newseum) okrzyknięto proklamacją „doktryny Clinton". Określenie to nawiązuje do „doktryny Clintona" z 1999 r. zakładającej amerykańskie wsparcie dla Kosowa w obronie praw etnicznych mniejszości. Także obecna Sekretarz Stanu zamierza działać w obronie praw człowieka; tym razem przedmiotem ochrony będą: wolność słowa, prawo dostępu do informacji, prawo wolności zgromadzeń i wolność religii uzewnętrzniane za pośrednictwem Internetu[46]. W treści swojego wystąpienia Sekretarz Stanu potępiła Chiny, Koreę Północną, Egipt, Wietnam, Tunezję, Uzbekistan i Arabię Saudyjską za ograniczanie na ich terytoriach wolnego przepływu informacji. Uznała taką praktykę za naruszającą prawo mieszkańców wymienionych państw do dostępu do informacji. W ramach działań mających zapobiegać dalszemu łamaniu tych praw zapowiedziała rządowe wsparcie dla tworzenia i rozpowszechniania prywatnych technologii, pozwalających obejść elektroniczne zabezpieczenia dostępu nakładane przez cenzorów. Do czasu wystąpienia Sekretarz Clinton władze żadnego z państw nie wypowiadały się odnośnie do tej kwestii, przyjmując milcząco, że decyzja o dostępności określonych treści na terytorium suwerena pozostaje w jego wyłącznej gestii. I choć deklaracja Clinton z początku 2010 r. wywołana została przez zdarzenia z 2009 r. wymierzone bezpośrednio w interesy amerykańskich firm i bezpieczeństwo Stanów Zjednoczonych (wtedy to cyfrowe zasoby m.in. amerykańskiej firmy Google stały się przedmiotem elektronicznego włamania dokonanego z terytorium Chin), to jej praktyczne skutki nastąpiły dopiero w 2011 r. – w reakcji na blokadę Internetu w Egipcie. W ślad za przemówieniem w Newseum i wkrótce po działaniach Google w Egipcie, Clinton przedstawiła w lutym 2011 r. program „Wolność Internetu" (ang. *Internet Freedom*), który zawierał szczegółowy opis metod walki o prawo dostępu do elektronicznych treści[47].

---

[46] Por. **H.R. Clinton**, *Remarks on Internet Freedom*, wystąpienie z dnia 21.01.2010 r., http://www.state.gov/secretary/rm/2010/01/135519.htm dostęp: 1.02.2012 r.

[47] **H.R. Clinton**, *Internet Rights and Wrongs: Choices & Challenges in a Networked World, Remarks*, 15.02.2011 r., http://www.state.gov/secretary/rm/2011/02/156619.htm dostęp: 26.12.2012 r.

Zapowiedziana przez Hilary Clinton polityka, jeszcze zanim znalazła swoje materialne odzwierciedlenie w Egipcie, budziła wątpliwości z punktu widzenia prawa międzynarodowego. Będąc bowiem przedstawicielem władz mocarstwa, oficjalnie oświadczyła, że zamierza ona wspierać podmioty pozostające w jego jurysdykcji w prowadzeniu aktywności ułatwiającej naruszenia prawa tworzonego przez inne państwo.

Pierwsze pytanie, jakie sprowokowała deklaracja Clinton, znane jest prawu międzynarodowemu od dawna; to pytanie o wzajemną relację ochrony praw człowieka i immunitetu państwa (w tym wypadku państwa regulującego zachowania realizowane za pośrednictwem sieci globalnej). Internet uszczegóławia to pytanie, dodając jeszcze jeden element: poszerza je o zagadnienie granic władzy państwowej wykonywanej względem elementów cyberprzestrzeni (stron internetowych czy elementów infrastruktury sieci, takich jak *root*-serwery). W jakim zakresie państwo może ingerować w treści elektroniczne dostępne na jego terytorium? Jak stosować podstawową dla międzynarodowego porządku prawnego zasadę jurysdykcji terytorialnej w odniesieniu do cyberprzestrzeni?[48]

Jest pewne, że każde działanie państwa, które wywołuje skutki względem elektronicznych treści (zablokowanie do nich dostępu lub ich usunięcie) lub zasobów (usuwanie danych lub uszkodzenia infrastruktury, np. poprzez atak DDoS)[49], ma skutek transgraniczny. Wiadomość *e-mail* niedostarczona odbiorcy (np. mieszkańcowi Stanów Zjednoczonych) znajdującemu się poza jurysdykcją państwa nadawcy (np. Egiptu) ogranicza prawo tego pierwszego do otrzymania informacji. Analogicznie, usunięcie wiadomości o aktualnych wydarzeniach w Egipcie, opracowanych w języku arabskim, udostępnianych z komputerów firmy z siedzibą w Egipcie, ogranicza prawo dostępu do tej informacji jej potencjalnym odbiorcom zlokalizowanym poza Egiptem, np. w Stanach Zjednoczonych. W oparciu o koncepcję „nakierowania treści" (ang. *targeting*) można podnosić, że wiadomość dotycząca Egiptu, udostępniona w języku angielskim, była przeznaczona dla takich właśnie egipskich

[48] Odnośnie do stosowania zasady jurysdykcji terytorialnej w cyberprzestrzeni por. **J. Kulesza**, *Międzynarodowe prawo Internetu*, Poznań 2010, s. 37.

[49] Ang. *Distributed Denial of Service attacks* – ataki polegające na wysyłaniu jednocześnie bardzo dużej ilości zapytań o dany adres internetowy stanowiący cel ataku. W konsekwencji, witryna zlokalizowana pod owym adresem przestaje działać – duża ilość zapytań nie może zostać obsłużona przez serwery, na których się znajduje.

emigrantów[50]. Choć prawo wolności słowa nie jest prawem bezwzględnym, to ocena zasadności stosowanych ograniczeń – jak pokazuje praktyka stanowiąca przedmiot niniejszych rozważań – może znacząco się różnić. W tym przykładowym stanie faktycznym USA przysługiwałoby prawo (czy wręcz spoczywałby na nich obowiązek)[51] ochrony praw swoich mieszkańców w oparciu o zasadę jurysdykcji ochronnej. Stany Zjednoczone miałyby więc legitymację do działania w celu zapewnienia prawa dostępu do informacji swoim mieszkańcom, gdyby to prawo – wskutek transgranicznych skutków obcej legislacji – było zagrożone[52]. Praktyczne konsekwencje takiej interpretacji reguł jurysdykcyjnych mogą przynieść nieobliczalne skutki, bowiem każde ograniczenie dostępności treści elektronicznych cechuje jednoczesny, globalny skutek. Zasada jurysdykcji skutkowej i zasada jurysdykcji ochronnej muszą być stosowane w transgranicznej cyberprzestrzeni z ogromną ostrożnością, bowiem wszelkie działania realizowane przy wykorzystaniu sieci globalnej niosą ze sobą konieczne transgraniczne konsekwencje. Treści publikowane *on-line* dostępne są jednocześnie wszędzie tam, gdzie dostępny jest Internet, zaś ich usunięcie pozbawi możliwości zapoznania się z nimi wszystkich potencjalnych czytelników na świecie.

Za przykład zagrożenia praw jednostki wynikających ze stosowania zasady jurysdykcji skutkowej do oceny treści publikowanych w Internecie służyć może wyrok sądu w Bangkoku z października 2011 r. nakładający karę dwóch i pół roku pozbawienia wolności na Joe Gordona – obywatela Stanów Zjednoczonych, który opublikował w Internecie fragmenty autorskiego, angielskiego tłumaczenia nieautoryzowanej biografii króla Tajlandii, co w myśl przepisów prawa tego kraju stanowi przestępstwo znieważenia głowy państwa. Przywołując zasadę jurysdykcji skutkowej, sąd w Tajlandii skazał autora publikacji na karę dwóch i pół roku pozbawienia wolności, którą ten odbywa obecnie w tajlandzkim więzieniu (został zatrzymany bezpośrednio po wylądowaniu

---

[50] Por. np. **M. Świerczyński**, *Jurysdykcja krajowa a prawo właściwe w Internecie*, [w:] **P. Podrecki** (red.), *Prawo Internetu*, Warszawa 2004, s. 144; **T. Pajor**, *O potrzebie zmiany prawa prywatnego międzynarodowego w zakresie zobowiązań niewynikających z czynności prawnych*, KPP 2000/3, s. 685; **idem**, *Nowe tendencje w części ogólnej prawa prywatnego międzynarodowego państw europejskich*, Prob. Pr. HZ 1995/18, s. 65–66.

[51] Por. cytowane powyżej orzeczenie ETPC w sprawie *Khurshid Mustafa and Tarzibachi v. Szwecja*.

[52] Por. nakaz w sprawie *Microsoft Corporation v. John Does 1–27*, sygn. powództwa 1_10CV156 (LMBIJFA) oraz przyp. następny.

na lotnisku w Bangkoku, gdzie zamierzał spędzić wakacje)[53]. Co ciekawe, Stany Zjednoczone nie podjęły żadnych kroków zmierzających do udzielenia pomocy prawnej swojemu obywatelowi. Ta sprawa pokazuje, że stosowanie zasady jurysdykcji skutkowej do aktywności realizowanych on-line spowodowałoby całkowity brak pewności prawnej – krajowe gwarancje wolności słowa okazałyby się całkowicie nieskuteczne, ponieważ wszyscy autorzy treści elektronicznych musieliby liczyć się z prawnymi konsekwencjami publikowanych w Internecie tekstów, przewidzianymi w porządkach krajowych wszystkich państw, gdzie dostępny jest Internet. Nieznajomość lokalnego prawa nie chroni przed konsekwencjami jego naruszenia, zaś owo naruszenie powstać może z chwilą publikacji treści na terytorium państwa, a więc umieszczenia ich na powszechnie dostępnej stronie internetowej. Stosowanie zasady jurysdykcji skutkowej względem wypowiedzi dostępnych *on-line* jako zasady podstawowej niosłoby ze sobą niepożądany efekt mrożący. Wielu autorów zrezygnowałoby z publikowania treści elektronicznych, nie godząc się na całkowitą niepewność prawną, towarzyszącą takiej aktywności (musieliby znać gwarancje prawne wolności słowa we wszystkich państwach, w których dostępny jest Internet). Dlatego też zasada jurysdykcji skutkowej powinna być stosowana z ogromną ostrożnością względem aktywności realizowanych *on-line*.

Podobne niepożądane i daleko idące skutki nieść będzie stosowanie zasady jurysdykcji ochronnej względem aktywności podejmowanych z wykorzystaniem sieci globalnej. Zgodnie z zapisem art. 110 § 1 polskiego kodeksu karnego, werbalizującego tę właśnie zasadę, polską ustawę karną „stosuje się do cudzoziemca, który popełnił za granicą czyn zabroniony skierowany przeciwko interesom Rzeczypospolitej Polskiej [...]". Przywołując zasadę jurysdykcji ochronnej, od 2005 r. Stany Zjednoczone ubiegają się o wydanie przez Wielką Brytanię jej obywatela, Gary'ego McKinnona, który – zdaniem prokuratury stanu Wirginia – na przełomie lat 2002/03 dopuścił się serii włamań do komputerów amerykańskich urzędów centralnych. W 2009 r. Brytyjska Izba Lordów wyraziła zgodę na wydanie McKinnona Stanom Zjednoczonym, gdzie grozi mu kara znacznie surowsza od przewidzianej za podobne przestępstwo w prawie brytyjskim, jednak sprzeciw opinii społecznej spowodował, że

[53] Informacje o sprawie Joe Gordona: http://www.freejoegordon.com/updates dostęp: 15.05.2012 r.

decyzja ekstradycyjna wciąż nie została wykonana[54]. Ten przykład także pokazuje, że stosowanie zasady jurysdykcji ochronnej niesie ze sobą zaprzeczenie podstawowej zasadzie państwa prawa – zasadzie pewności prawa, która stanowi fundament demokratycznego społeczeństwa.

Jeśli więc zasady jurysdykcji skutkowej i ochronnej przywoływane są dla ochrony interesów państwowych przed zagrożeniami tworzonymi przez jednostki zamieszkujące poza granicami zagrożonego państwa, to logicznie poprawne i teoretycznie możliwe byłoby także przywołanie ich dla wykonywania przez państwa swoich pozytywnych obowiązków ochrony praw ich mieszkańców, w tym prawa dostępu do informacji. W kontekście powyższej praktyki stosowania zasad jurysdykcji skutkowej tak właśnie odczytywać można deklarację Sekretarz Clinton, mówiącą o rozpoczęciu walki z cenzurą Internetu. Oznaczać ona może gotowość Stanów Zjednoczonych do aktywnej ochrony prawa dostępu do informacji ich mieszkańców przed ograniczeniami wynikającymi z cenzorskich praktyk innych państw.

Warto jednocześnie podkreślić, że specyfika Internetu nadała starej debacie o relacji pomiędzy prawami człowieka a suwerennością państw nowy wymiar i sprowokowała drugie, ważniejsze pytanie. Jeśli bowiem Stany Zjednoczone uznają, że w danej sytuacji pierwszeństwo ma ochrona prawa człowieka, przed obowiązkiem respektowania suwerennych decyzji innego państwa (Egiptu), to – jako jedyne państwo na świecie[55] – mogą samodzielnie zdecydować o przełożeniu tego przekonania na praktykę (w opisywanej sytuacji: przy pomocy firmy Google, ale w kontekście wcześniejszych decyzji sądów stanowych USA – także poprzez ingerencję w System Nazw Domenowych)[56].

---

[54] Aktualne informacje o sprawie Gary'ego McKinnona: http://freegary.org.uk/ dostęp: 13.05.2012 r.

[55] Zważywszy, że kluczowe dla działania sieci globalnej zasoby zlokalizowane są w stanie Wirginia, w tym *root-zone-file* A (pierwowzór danych kopiowanych na pozostałych 12 *root*--serwerach) czy firma VeriSign, administrująca rejestrami najpopularniejszych domen: .com i .org. Pozostałych 21 spośród 25 administratorów domen rodzajowych najwyższego stopnia (generic Top Level Domains, gTLDs) także ma swoje siedziby w Stanach Zjednoczonych (por. dane dostępne na stronie Internet Assigned Numbers Authority, http://www.iana.org/domains/root/db/ dostęp: 15.05.2012 r.)

[56] Domain Name System (DNS), por.: **Ernesto**, *U.S. Resume Controversial File–Sharing Domain Seizures*, TorrentFreak 1.02.2011, http://torrentfreak.com/us–resume–file–sharing–domain–seizures–110201/ dostęp: 1.02.2012 r., gdzie autor zwraca uwagę na wykonany (1.02.2011) nakaz sądu okręgowego (District Court) zobowiązujący VeriSign (por. przyp. powyżej) do usunięcia hiszpańskojęzycznej, nieposiadającej żadnych związków z rynkiem

Jeśli więc władze Stanów Zjednoczonych uznają, że nałożone przez obcego suwerena ograniczenia wolności wypowiedzi wymagają od nich podjęcia działań w celu ochrony wolności słowa własnych mieszkańców (zwłaszcza ich prawa do otrzymywania i przesyłania informacji), to mają techniczne i prawne możliwości samodzielnego przełożenia tej oceny na działanie kładące kres naruszeniu. Mogą zobowiązać podmioty prawa USA mocą nakazu sądowego do zaprzestania praktyki filtrującej (czyniła to firma Google w Chinach do 2010 r., nim m.in. za namową Sekretarz Clinton wycofała swoje wpływy z chińskiego rynku usług internetowych). Inicjatywa wykazana przez Google w Egipcie nie wynikała z nakazu sądowego w USA, choć spotkała się z milczącym przyzwoleniem władz, co może zostać uznane za zaniechanie sprzeczne z peremptoryjną normą zakazującą ingerencji w sprawy wewnętrzne obcego państwa. Ocena taka wymaga analizy aktywności Stanów Zjednoczonych i działającej za ich przyzwoleniem firmy Gogle, z punktu widzenia prawa międzynarodowego, którą to analizę przedstawiono poniżej.

6. Program „Wolność Internetu" a odpowiedzialność państwa

Nie ulega wątpliwości, że co do formy obie deklaracje Sekretarz Clinton (ze stycznia 2010 r. i z lutego 2011 r.) są materialnymi źródłami prawa międzynarodowego – aktami jednostronnymi państwa. Nie ulega także wątpliwości, że akty te nie skutkują bezpośrednio w krajowym (amerykańskim) porządku prawnym – nie rodzą obowiązku podmiotów prawa USA, aby te udostępniły swoje zasoby celem zapobiegania cenzurze sieci (dla wywołania takiego skutku deklaracje musiałyby przybrać formę aktu prawa krajowego). Trudno byłoby także wykazać, iż opisane na wstępie zachowanie Google wynika bezpośrednio z upoważnienia przekazanego firmie przez rząd USA w treści wystąpień Sekretarz Clinton dotyczących tej konkretnej sytuacji, choćby dlatego, że jej deklaracja nie rodzi skutków w prawie wewnętrznym. Stany Zjednoczone nie ponoszą więc bezpośredniej odpowiedzialności za działanie Google pozwalające udaremnić egipską blokadę, bowiem ta nie

amerykańskim, witryny rojadirecta.org, uznanej przez dwie hiszpańskie instancje sądowe za działającą legalnie. Por. zablokowana przez Biuro Bezpieczeństwa Narodowego USA strona: http://www.rojadirecta.org/ dostęp: 13.05.2012 r., oraz jej działająca wersja w domenie krajowej najwyższego stopnia Czarnogóry: http://www.rojadirecta.org/ dostęp: 13.05.2012 r.

działała z upoważnienia czy na zlecenie władz krajowych. Nie oznacza to, że USA nie ponosi odpowiedzialności za zaniechanie sprzeczne z treścią jego międzynarodowego zobowiązania.

Decyzja władz Egiptu powinna zostać uszanowana przez inne podmioty prawa międzynarodowego, zgodnie ze znaną prawu międzynarodowemu zasadą nieingerencji w sprawy wewnętrzne innego państwa, wywodzoną z art. 2 ust. 4 KNZ, potwierdzoną treścią ust. 7 tego samego artykułu Karty. Jak słusznie wskazuje R. Vark, w ramach obowiązku poszanowania suwerenności innych państw władze kraju, z którego terytorium inicjowane są szkodliwe działania, zobowiązane są do współpracy z państwem poszkodowanym w sposób konieczny dla eliminacji owego szkodliwego działania[57]. Oznacza to, że jeśli samo państwo nie jest w stanie ochronić interesów innego suwerena i zlikwidować istniejących dla niego zagrożeń, nie może ono biernie pozwalać prywatnym grupom korzystać z ochrony wynikającej z nienaruszalności jego terytorium i suwerenności. W orzecznictwie zasada ta znalazła swoje najwyraźniejsze odbicie w orzeczeniu MTS w sprawie zakładników amerykańskich w Teheranie[58], w której sąd uznał, że zamach, pomimo iż nie może być przypisany państwu Iran, „nie oznacza, że Iran jest wolny od wszelkiej odpowiedzialności za niego; jako że jego postępowanie pozostawało w sprzeczności ze zobowiązaniami międzynarodowymi spoczywającymi na państwie, które zobligowane było zapewnić ochronę amerykańskich: ambasady i konsulatu. [...] Ten brak działania (*inaction*) ze strony rządu Iranu stanowi wyraźne pogwałcenie zobowiązania Iranu wobec Stanów Zjednoczonych i Konwencji wiedeńskiej o stosunkach dyplomatycznych"[59]. Jak słusznie zauważają R.M. Bratspies i R.A. Miller, sąd utożsamia ustalenie wystąpienia obowiązku dołożenia należytej staranności przez państwo z możliwością przypisania państwu odpowiedzialności za działania osób fizycznych[60]. Udostępnianie swojego terytorium podmiotom działającym na szkodę innego suwerena i niezapobieganie skutkom takich szkodliwych działań może nosić znamiona aktu międzynarodowo bezprawnego i rodzić odpowiedzial-

[57] **R. Vark**, *State Responsibility for Private Armed Groups in the Context of Terrorism*, Juridica International 2006/XI, s. 192.

[58] ICJ Rep. 1980, s. 3.

[59] *Ibidem*, s. 29, przyp. 42. .

[60] **R.M. Bratspies**, **R.A. Miller**, *Transboundary harm in international law: lessons from the Trail Smelter arbitration*, Cambridge University Press 2006, s. 233.

ność państwa za zaniechanie[61]. W ten sposób interpretowany jest par. 3 art. 14 Projektu artykułów Komisji Prawa Międzynarodowego (KPM) dotyczących odpowiedzialności państwa za czyny niezgodne z prawem międzynarodowym z 1992 r.[62] Jak podaje J. Crawford w uzasadnieniu projektu KPM[63], przepis ten dotyczy zobowiązania państwa do zapobieżenia powstaniu danego szkodliwego zdarzenia (*the breach of obligation to prevent a given event*). Zobowiązania do zapobieżenia danemu skutkowi najczęściej formułowane są jako zobowiązania do dołożenia najlepszych starań (*best efforts obligations*), obligujące państwo do podjęcia wszelkich rozsądnych (*reasonable*) lub niezbędnych (*neccesary*) środków w celu zapobieżenia powstania danego zdarzenia, jednak bez gwarancji, że zdarzenie to nie nastąpi. Standard powinnego zachowania wyznacza tu test należytej staranności, ustalany kazuistycznie dla każdej konkretnej sprawy[64].

Niedołożenie należytej staranności stwierdzone może zostać wtedy, gdy „państwo celowo albo niedbale spowodowało zdarzenie, któremu należało zapobiec"[65]. Taką samą ocenę prawną wywoła celowe lub niedbałe niezapobieżenie takiemu działaniu, realizowanemu przez inne podmioty na terytorium państwa, czy też powstrzymanie się przed ich ograniczeniem (ang. *abating*)[66]. Państwo może więc zostać uznane za odpowiedzialne wskutek niewprowadzenia stosownej legislacji, niewykonywania obowiązujących aktów prawnych

---

[61] Projekt artykułów o odpowiedzialności państwa za czyny niezgodne z prawem międzynarodowym, Komisja Prawa Międzynarodowego 1992, doc. A/CN.4/L.472, art. 14 ust. 3, Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, A/56/10, Yearbook of the International Law Commission 2001/2 (2), s. 62.

[62] Projekt artykułów KPM dotyczących odpowiedzialności państwa za czyny niezgodne z prawem międzynarodowym z 1992 r. (*Draft Articles on State Responsibility: Titles and texts of articles adopted by the Drafting Committee*, doc. A/CN.4/L.472).

[63] **J. Crawford**, *The International Law Commission's articles on state responsibility: introduction, text, and commentaries*, Cambridge University Press 2002, s. 140.

[64] A. Wyrozumska i W. Czapliński podają jako przykład niedochowania wymogu należytej staranności zaniedbanie podjęcia kroków mających uchronić określone osoby lub przedmioty przed atakami oraz odmowę ukarania takich ataków, jak i wyraźne poparcie przez państwo aktów dokonywanych przez jednostki na szkodę państw trzecich lub ich obywateli (**A. Wyrozumska**, **W. Czapliński**, *Prawo...*, s. 436). Także **I. Brownlie** (*System of the Law of Nations*, Part I: *State responsibility*, Oxford University Press 1983, s. 45) wskazuje jako kryterium stosowane przez sądy, element skutkowości łączący zaniechanie państwa i naruszenie prawa międzynarodowego.

[65] Second report on international liability for injurious consequences arising out of acts not prohibited by international law by Mr. P.S. Rao, Special Rapporteur, A/CN.4/501, s. 8, pkt 24.

[66] *Ibidem*, przyp. 37.

czy też niezapobiegania lub niepowstrzymania bezprawnej działalności, jak i za nieukaranie osób za nią odpowiedzialnych[67]. Naruszenie zobowiązania do dokładania należytej staranności stwierdzone może zostać także wtedy, gdy państwo wiedziało albo powinno było wiedzieć, że dane działanie może wywołać znaczącą szkodę u innych państw[68].

Gabinet Prezydenta Obamy wiedział, że Google realizuje działania skutecznie[69] zmierzające do udaremnienia egzekucji nakazu wydanego przez władze Egiptu, i nie podjął żadnych kroków, aby takim działaniom zapobiec. Wykazując należytą staranność, Stany Zjednoczone powinny uniemożliwić firmie z Redmond świadczenie omawianej powyżej usługi, jako skutkującej uniemożliwieniem wykonywania władzy państwowej w Egipcie.

7. Specyfika cyberprzestrzeni a pojęcie suwerenności

O ile ekstensywne praktyki filtrujące stosowane przez takie państwa, jak Egipt czy Chiny, zasługują na potępienie ze względów etycznych, o tyle prawo międzynarodowe nie oferuje skutecznych narzędzi do walki z nimi. Co więcej, istniejący zbiór norm peremptoryjnych obliguje państwa do szanowania decyzji innych suwerenów i powstrzymania się od samodzielnej, nieautoryzowanej przez Radę Bezpieczeństwa ONZ ingerencji w ich sprawy wewnętrzne[70], nawet gdy taka ingerencja jest technicznie i logistycznie możliwa. Taki stan rzeczy wydaje się niepożądany z przedstawionych już powodów: wszelka działalność państwa względem treści elektronicznych wywołuje skutki nie tylko lokalne, ale jednocześnie we wszystkich państwach, gdzie dostępny jest Internet. Wobec braku międzynarodowych mechanizmów rozwiązania problemów, jakie niesie ze sobą ten stan rzeczy, każde z państw może we własnym imieniu wystąpić przeciwko naruszycielowi prawa dostępu do informacji swoich rezydentów, powołując się na zasadę jurysdykcji skutkowej czy ochronnej.

---

[67] *Ibidem*, przyp. 38.

[68] *Ibidem*, przyp. 39, gdzie mowa o odpowiedzialności za szkodliwe wykorzystanie międzynarodowych ciągów wodnych.

[69] Za dowód skuteczności usług Google niech posłuży fakt, że kolejnego dnia po jej zaoferowaniu blokada mediów w Egipcie została zniesiona.

[70] Koncepcja interwencji humanitarnej wciąż nie może być zaliczona do katalogu uznanych instytucji prawa międzynarodowego, z uwagi na brak towarzyszącej jej *opinio iuris*.

Dlatego też na arenie międzynarodowej coraz śmielej formułowane jest zobowiązanie państw do powstrzymania się od ingerencji w elektroniczne treści[71]. Wyznaczanie granic wolności słowa, jako warunkowane względami kulturowymi, należało od początków ewolucji praw człowieka do wyłącznych kompetencji państwa (chyba że te decydowały się nimi dzielić w ramach organizacji międzynarodowych, takich jak Rada Europy). Jednak wobec globalnego charakteru komunikacji elektronicznej wydaje się, że nadszedł czas, aby ustalić na poziomie międzynarodowym minimalny standard także dla wolności słowa, realizowanej *on-line*. Określenia takie, jak *public service value of the Internet*[72], oraz postulat prawa dostępu do Internetu jako prawa obywatelskiego (mocowanego w krajowym porządku prawnym) nie tylko pojawiają się coraz częściej w wypowiedziach przedstawicieli organizacji pozarządowych i przedstawicieli doktryny, ale znajdują swoje odbicie także w krajowych porządkach prawnych (prawo dostępu do Internetu jest elementem wolności obywatelskich uznanych w prawie Finlandii czy Litwy). Jednocześnie sugestie dotyczące ewentualnego międzynarodowego obowiązku państw, opiewającego na zapewnienie dostępu do treści elektronicznych, formułowane są wąsko – jedynie odnośnie do zagwarantowania swobodnej wymiany międzynarodowej (a nie dostępu w granicach państwa)[73].

Wobec intensyfikacji procesów globalizacyjnych i popularyzacji Internetu (jedynej platformy jednoczesnej, międzynarodowej, zapewniającej bezpo-

[71] Por. np. liczne deklaracje Komitetu Ministrów Rady Europy (Declaration of the Committee of Ministers on freedom of communication on the Internet of 28 May 2003; Deklaracja Komitetu Ministrów Rady Europy dotycząca ochrony wolności wypowiedzi i informacji oraz wolności zgromadzeń w związku z nazwami domenowymi, przyjęta 21.09.2011 r.)

[72] Por. np. Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet (Adopted by the Committee of Ministers on 7 November 2007 at the 1010th meeting of the Ministers' Deputies).

[73] Mowa tu o sytuacji, w której zablokowanie swobodnego przepływu treści elektronicznych w jednym państwie spowoduje znaczące ograniczenie dostępu do nich w państwach ościennych, korzystających z infrastruktury filtrującego suwerena. Przykładem służyć tu może sytuacja z 2008 r., gdy podczas konfliktu gruzińsko-rosyjskiego infrastruktura elektroniczna Gruzji została zablokowana, w wyniku czego Armenia straciła połączenie z Internetem (korzysta z linii transazjatycko-europejskiej, przebiegającej przez terytorium Gruzji). Por.: *Internet governance and critical internet resources, report prepared by the Council of Europe Secretariat Media and Information Society Division, Directorate General of Human Rights and Legal Affairs*, Rada Europy, Strasbourg 2009, s. 22.

średnią wymianę informacji blisko $^1/_3$ mieszkańców globu[74]) niezbędne jest równoległe zintensyfikowanie debaty nad podstawowymi wartościami, jakie powinny być w cyberprzestrzeni chronione, oraz o sposobach ich ochrony[75]. W treści tej debaty należy uwzględnić samą specyfikę tego wyjątkowego medium. Zważywszy na powyższe oraz architekturę i specyfikę Internetu, wydaje się, że nastał czas, by zmodyfikować tradycyjne pojęcie suwerenności państw ze względu na rosnącą potrzebę ochrony praw człowieka[76].

W tym właśnie kontekście R.H. Weber proponuje zastąpienie obecnego znaczenia suwerenności, zakorzenionego w porządku westfalskim, koncepcją „suwerenności współdzielonej" (*cooperative sovereignty*)[77], nawiązującej do znanej już idei „suwerenności dzielonej" (*shared sovereignty*), pojawiającej się najczęściej w kontekście międzypaństwowych ustaleń traktatowych[78]. Autor ten uwzględnia w swojej propozycji zasadę zarządzania wielopodmiotowego (*multistakeholder governance*)[79] – jedną z podstawowych reguł międzynarodowego prawa Internetu[80]. Zasada ta oznacza, że na kształt funkcjonowania Internetu wpływ mają w równej mierze (choć „w swoich właściwych rolach")[81] państwa i podmioty prawa prywatnego (przedsiębiorcy i użytkownicy działający samodzielnie lub za pośrednictwem zrzeszających ich

---

[74] Według firmy Miniwatts Marketing Group, zajmującej się statystyką dostępu do sieci, 28,3% populacji świata ma dostęp do Internetu, http://www.internetworldstats.com/stats.htm dostęp: 2.02.2011 r.

[75] Por. np. Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet; Declaration by the Committee of Ministers on Internet governance principles.

[76] Por. np.: **R. Kwiecień**, *Pokój czy sprawiedliwość? O aksjologicznej podstawie współczesnego prawa międzynarodowego*, [w:] **J. Menkes** (red.), *Prawo międzynarodowe…*, s. 380, gdzie autor wskazuje na pochodną wobec stanu prawa międzynarodowego treść pojęcia suwerenności.

[77] **R.H. Weber**, *New Sovereignty Concepts in the Age of Internet*, Journal of Internet Law, August 2010, s. 19.

[78] Por. **S.D. Krasner**, *The Hole in the Whole: Sovereignty, Shared Sovereignty, and International Law*, Michigan Journal of International Law 2004/25 (4), s. 19 i n.

[79] **R.H. Weber**, *New Sovereignty…*, s. 14.

[80] **R. Uerpman-Wittzack**, *Principles of International Internet Law*, German Law Journal 2010/11 (1), s. 1248.

[81] Por.: *Report of the Working Group on Internet Governance*, Tunis 2005, s. 4, pkt 10, www.wgig.org/docs/WGIGREPORT.pdf dostęp: 2.02.2012 r.

organizacji)[82]. Decyzje o dostępności elektronicznych treści podejmowane być więc powinny w porozumieniu z innymi aktorami elektronicznej wymiany – nie tylko przedstawicielami innych państw, ale także przedsiębiorcami (ISPs) czy organizacjami społecznymi reprezentującymi samych użytkowników.

Ta odważna teza wymaga wielu uzupełnień. Jeśli miałaby być przełożona na język prawa międzynarodowego, to wymagałaby inkorporacji w traktacie[83] (otwartym do podpisu także dla podmiotów prawa prywatnego) lub jednolitej praktyki zwyczajowej popartej *opinio iuris*. Oba rozwiązania wykazują znaczące mankamenty: przede wszystkim wymagają czasu i nie gwarantują dostatecznej elastyczności powstałych rozwiązań, niezbędnej wobec specyfiki regulowanej materii. Wady te każą odwołać się, przynajmniej tymczasowo, do rozwiązań miękkiego prawa międzynarodowego[84]. Niemniej jednak omówiony powyżej postulat Webera wart jest zapamiętania. Jak już wspomniano, transgraniczna specyfika cyberprzestrzeni, przekładająca się bezpośrednio na konieczność zagwarantowania pewności prawa na poziomie międzynarodowym, wymaga ponownego przeanalizowania koncepcji suwerenności. Zaproponowana przez R.H. Webera koncepcja suwerenności współdzielonej oparta jest na założeniu możliwości identyfikacji wartości leżących u podstaw różnych interpretacji pojęcia suwerenności, która może następnie prowadzić do identyfikacji powszechnie akceptowanych, podstawowych praw. Suwerenność współdzielona mogłaby więc zarówno nadawać kształt, jak i stymulować dalsze dyskusje nad właściwym podziałem władzy pomiędzy państwami[85]. Podział ów musiałby łączyć prerogatywy wynikające z suwerenności z obowiązkami prawa międzynarodowego, zwłaszcza w zakresie praw człowieka. Cytowany autor sugeruje, że państwa dzielą wspólny, międzynarodowy obowiązek tworzenia i implementowania polityk skoncentrowanych na ochronie praw człowieka[86]. W tym właśnie kontekście odczytywana być powinna, czyniona

---

[82] Por.: **W. Kleinwächter**, *Multistakeholderism and the IGF: Laboratory, Clearinghouse, Watchdog*, [w:] **W.J. Drake** (ed.), *Reforming Internet governance: perspectives from the Working Group on Internet Governance (WGIG)*, New York 2005, s. 79.

[83] Por.: **J. Kulesza**, *Ramowa konwencja Internetu*, PiP 2009/10, s. 5–17.

[84] Np.: *International and multi-stakeholder co-operation on cross-border Internet, Interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services incorporating analysis of proposals for international*, Rada Europy, H/Inf 2010/10, http://www.coe.int/t/dghl/standardsetting/media/mc–s–ci/default_EN.asp dostęp: 2.02.2012 r.

[85] **R.H. Weber**, *New Sovereignty*..., s. 14.

[86] *Ibidem*, s. 16.

w treści niniejszego opracowania, sugestia konieczności i możliwości zidentyfikowania i implementowania międzynarodowego standardu wolności słowa, obowiązującego w transgranicznej cyberprzestrzeni.

Państwa z pewnością zdecydują się na dalsze ograniczanie własnej suwerenności w związku z popularyzacją Internetu; jeśli nie ze względu na ochronę praw człowieka, to chociażby dla zagwarantowania międzynarodowego cyberbezpieczeństwa. Jeżeli standard należytej staranności i reguły proporcjonalności w sytuacjach dotyczących wolności słowa nie zostaną szybko wypracowane, to – co jest widoczne już teraz – rosnąca obawa przed „cyberterroryzmem" zmusi państwa do wyznaczania międzynarodowych standardów cyberobronności[87]. Jednocześnie należy pamiętać, że granice międzynarodowego bezpieczeństwa przebiegają tam, gdzie rozpoczyna się ochrona praw jednostki – względy obronności nie mogą przeważyć nad koniecznością zagwarantowania jednostkom prywatności czy wolności wypowiedzi. Zaś ci, którzy gotowi są poświęcić wolność za bezpieczeństwo, nie zasługują ani na wolność, ani na bezpieczeństwo.

Bibliografia

Brownlie I., *System of the Law of Nations*, Part I: *State responsibility*, Oxford University Press 1983.

Deibert R.J., **Palfrey J.G.**, **Rohozinski R.**, **Zittrain J.** (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, MIT Press, Massachussetts 2010.

Deibert R.J., **Palfrey J.G.**, **Rohozinski R.**, **Zittrain J.** (eds), *Access Denied: The Practice and Policy of Global Internet filtering*, MIT Press, Massachussetts 2008.

Drake W. J., *Reforming Internet governance: perspectives from the Working Group on Internet Governance (WGIG)*, New York 2005.

Krasner S.D., *The Hole in the Whole: Sovereignty, Shared Sovereignty, and International Law*, Michigan Journal of International Law 2004/25 (4).

Kulesza J., *Amerykańsko-chiński spór o cenzurę w Internecie*, PiP 2010/6.

Kulesza J., *Międzynarodowe prawo Internetu*, Poznań 2010.

Kulesza J., *Ramowa konwencja Internetu*, PiP 2009/10.

Machała W., **Sarbiński R.**, *Wymiana plików muzycznych za pośrednictwem Internetu a prawo autorskie*, PiP 2002/9.

[87] Por. choćby prace Centrum doskonałości NATO ds. współpracy w zakresie cyberobronności (NATO Cooperative Cyber Defence Centre of Excellence; NATO CCD COE) z siedzibą w Estonii.

Menkes J. (red.). *Prawo międzynarodowe – problemy i wyzwania. Księga pamiątkowa Profesor Renaty Sonnenfeld-Tomporek*, Warszawa 2006.

OpenNet Initiative, *A Starting Point: Legal Implications of Internet Filtering*, Toronto/Cambridge/Harvard 2004.

Pajor T., *Nowe tendencje w części ogólnej prawa prywatnego międzynarodowego państw europejskich*, Prob. Pr. HZ 1995/18.

Pajor T., *O potrzebie zmiany prawa prywatnego międzynarodowego w zakresie zobowiązań niewynikających z czynności prawnych*, KPP 2000/3.

Podrecki P. (red.), *Prawo Internetu*, Warszawa 2004.

Privacy International and the GreenNet Educational Trust, *Silenced, An international Report on Censorship and Control of the Internet*, Stanford 2003.

Sadurski W., *Freedom of Speech and Its Limits*, Kluwer Academic Publishers, Dordrecht 2002.

Uerpman–Wittzack R., *Principles of International Internet Law*, German Law Journal 2010/11 (1).

Weber R.H., *New Sovereignty Concepts in the Age of Internet*, Journal of Internet Law, August 2010.

Weckert J., *What is so Bad about Internet Content Regulation?*, Ethics and Information Technology 2000/2 (2).

Wyrozumska A., **Czapliński W.**, *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Warszawa 1999.

Akty prawne

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z 1950 r., Dz.U. z 1993 r., Nr 61, poz. 284.

Międzynarodowy Pakt Praw Obywatelskich i Politycznych, Dz.U. z 1977 r., Nr 38, poz. 167.

Ustawa o świadczeniu usług drogą elektroniczną, Dz.U. z 2002 r., Nr 144, poz. 1204.

Akty miękkiego prawa międzynarodowego:

Declaration of the Committee of Ministers on freedom of communication on the Internet of 28 May 2003. Deklaracja Komitetu Ministrów Rady Europy dotycząca ochrony wolności wypowiedzi i informacji oraz wolności zgromadzeń w związku z nazwami domenowymi, przyjęta 21.09.2011 r.

Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, A/56/10, Yearbook of the International Law Commission 2001/2(2).

International and multi-stakeholder co-operation on cross-border Internet, Interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services incorporating analysis of proposals for international, Rada Europy, H/Inf 2010/10, http://www.coe.int/t/dghl/standardsetting/media/mc–s–ci/default_EN.asp dostęp: 2.02.2012 r.

Internet governance and critical internet resources, report prepared by the Council of Europe Secretariat Media and Information Society Division, Directorate General of Human Rights and Legal Affairs, Rada Europy, Strasbourg 2009, s. 22.
Recommendation CM/Rec (2007) 16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet.
Recommendation CM/Rec (2011) 8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet; Declaration by the Committee of Ministers on Internet governance principles.
Report of the Working Group on Internet Governance, Tunis 2005, *www.wgig.org/docs/WGIGREPORT.pdf* dostęp 2.02.2012 r.
Resolution adopted by the Human Rights Council, Freedom of opinion and expression (A/ RC/ RES/12/16), 2.10.2009 r.

Orzeczenia sądowe:

Nakaz w sprawie *Microsoft Corporation v. John Does 1–27*, sygn. powództwa 1_10CV156 (LMBIJFA).
Wyrok ETPC z 28 czerwca 2001 r. w sprawie *VgT Verein Gegen Tierfabriken v. Szwajcaria*, nr skargi 24699/94.
Wyrok ETPC z dnia 16 grudnia 2008 r. w sprawie *Khurshid Mustafa And Tarzibachi v. Szwecja*, nr skargi 23883/06.
Wyrok ETS z dnia 24 listopada 2011 r. w sprawie *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, sygn. C-70/10.

Strony internetowe

Cisco Announces IP Next-Generation Network Advancements for Service Providers, San Jose, 5.12.2004 dostęp: 5.11.2012: http://newsroom.cisco.com/dlls/2004/prod_120604.html.
Cowie J., *Egypt Leaves the Internet*, Rensys 27.01.2011, http://www.renesys.com/blog/2011/01/egypt–leaves–the-internet.shtml dostęp: 1.02.2012 r.
Clinton H.R., *Internet Rights and Wrongs: Choices & Challenges in a Networked World, Remarks*, 15.02.2011 r., http://www.state.gov/secretary/rm/2011/02/156619.htm dostęp: 26.12.2012 r.
Clinton H.R., *Remarks on Internet Freedom*, 21.01.2010 r., http://www.state.gov/secretary/rm/2010/01/135519.htm dostęp: 1.02.2012 r.
Ernesto, *U.S. Resume Controversial File–Sharing Domain Seizures*, TorrentFreak 1.02.2011, http://torrentfreak.com/us–resume–file–sharing–domain–seizures–110201/ dostęp: 1.02.2012 r.,
Evans R., *U.N. chief tells rights body drop rhetoric, blocs*, Reuters, 12.12.2008 r., http://www.reuters.com/article/2008/12/12/us–un–rights–idUSTRE4BB67820081212 dostęp: 1.02.2012 r.
Italy cracks down on Pirate Bay, New York Times 14.08.2008 r., http://www.nytimes.com/2008/08/14/technology/14iht–webpirate.15301147.html dostęp: 2.02.2012 r.

Noman H., **York J.C.**, *West Censoring East: The Use of Western Technologies by Middle East Censors*, OpenNetwork Inititive 2011, http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011 dostęp: 1.02.2012 r.

ps, PAP, *Google pomaga Egipcjanom – umożliwia komunikowanie przez Twitter*, G.W. 1.02.2011, http://wiadomosci.gazeta.pl/Wiadomosci/1,80277,9034000,Google_pomaga_Egipcjanom___umozliwia_komunikowanie.html dostęp: 1.02.2011 r.

Stanowisko Fundacji „Dzieci Niczyje" w sprawie art. 21 dotyczącego blokowania pornografii dziecięcej w Internecie, zawartego w roboczej wersji Dyrektywy dotyczącej zwalczania nadużyć seksualnych, wykorzystywania seksualnego dzieci oraz dziecięcej pornografii, opublikowanej przez Komisję Europejską w marcu 2010 r., http://www.dzieckowsieci.pl/repository/newsy/blokowanie_pornografii_dzieciecej_w_Internecie_–_stanowisko_FDN.pdf dostęp: 1.02.2012 r.;

Usuwanie, nie blokowanie, Fundacja Panoptykon 2011 r., http://www.panoptykon.org/content/petycja-przeciwko-projektowi-komisji-europejskiej-blokowania-tre-ci-w-internecie-usuwanie-ni dostęp: 1.02.2012 r.

Joanna KULESZA

ON-LINE CENSORSHIP AND STATE RESPONSIBILITY FOR HUMAN RIGHTS VIOLATIONS

(S u m m a r y)

In the article the author examines state filtering of electronic content in terms of its compliance with international law, especially with provisions guaranteeing the freedom of expression and access to information. The White House implemented program "Internet Freedom", whose aim is to introduce software enabling the circumvention of local content control in "filtering countries", is subject to thorough analysis. The analysis covers recent (2011) events in Egypt, where the world's first successful attempt at shutting down the Internet within state borders was completed. Although enforced through legitimate state actions this Internet shut-down was circumvented with the use of Google-introduced technology. The technology and its use seemed to meet the ideas behind the "Internet Freedom" program, introduced by the White House a few month prior to the Egypt events.

In the course of argument the author discusses international responsibility for the possible breach of their international obligations by both: Egypt and the U.S. She provides for the assessment of the legality of the actions of Egyptian authorities' introducing an Internate filter that constitutes an infringement of freedom of expression, as well as the responsibility of United States for their failure to halt a U.S. legal entity enabling users to circumvent the legitimate Egyptian technology. The author argues that the character of the global network requires a redefinition of state sovereignty, especially in the context of human rights protection on-line. An idea introduced by R.H. Weber of "shared sovereignty" is mentioned, as it reflects the basic principle of international Internet law: the principle of multistakeholder governance.