Warszawa, 14.03.2011 r.

Pani
prof. dr hab. Irena Lipowicz
Rzecznik Praw Obywatelskich

Szanowna Pani,

W nawiązaniu do debaty na temat tego, czy blokowanie stron internetowych to dobry środek w walce z rozpowszechnianiem tzw. pornografii dziecięcej w Internecie, którą była Pani uprzejma gościć 10 lutego 2011 r. oraz w związku z trwającymi pracami nad dyrektywą o zwalczaniu seksualnego wykorzystywania dzieci (nr ref. COD/2010/0064) – która jako jedną z metod walki z rozprzestrzenianiem obrazów seksualnego wykorzystywania dzieci przewiduje blokowanie stron internetowych – Fundacja Panoptykon pragnie zaprezentować swoje stanowisko oraz ustosunkować się do problemów i pytań postawionych przez Panią na zakończenie wspomnianej debaty.

Jednocześnie dziękujemy Pani za zainteresowanie tą niezwykle istotną problematyką i chęć do animowania debaty publicznej z udziałem ekspertów, decydentów politycznych, organizacji pozarządowych i przedstawicieli świata nauki. Wyrażamy nadzieję, że wspomniana debata z 10 lutego będzie jedynie wstępem do pogłębionej i merytorycznej rozmowy na temat skuteczności, sensowności oraz skutków społecznych blokowania stron internetowych, jako środka wymierzonego przeciwko jakiemukolwiek niepożądanemu zjawisku – nie tylko rozprzestrzenianiu obrazów seksualnego wykorzystywania dzieci. W imieniu Fundacji Panoptykon po raz kolejny pragnę zapewnić o naszej gotowości do udziału w dalszych odsłonach tej dyskusji.

W tym kontekście chciałabym krótko podsumować nasze stanowisko w sprawie wspomnianej dyrektywy:

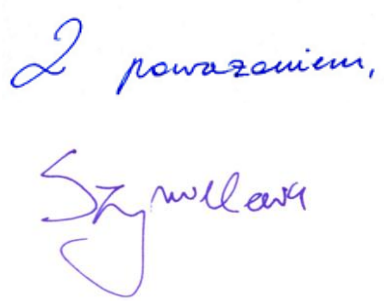
(1) Niezmiennie uważamy, że treści pedofilskie należy skutecznie usuwać, a nie prowizorycznie blokować. Blokowanie stron nie likwiduje dostępu do treści, które próbujemy wyeliminować. Dostęp do zablokowanych stron wciąż jest możliwy – wystarczy wybrać inną „drogę" w sieci. Blokowanie jest ponadto niebezpieczne dla wolności słowa, a nie jedynie dla „wolności rozpowszechniania pornografii dziecięcej", jak przekonują jego zwolennicy. Praktyka państw, które eksperymentowały z tym środkiem pokazuje, że nie jest możliwe ograniczenie blokowania jedynie do treści uznawanych za nielegalne. Usuwanie nielegalnych treści musi być traktowane jako

priorytet i wymaga stworzenia odpowiednich ram prawnych i podjęcia działań na arenie międzynarodowej.

(2) Państwa Unii Europejskiej powinny podjąć wszelkie kroki w celu wzmocnienia współpracy międzynarodowej, w tym z państwami trzecimi, w celu skutecznego i szybkiego usuwania nielegalnych treści z Internetu. Priorytetem musi być rozwiązanie systemowych problemów w komunikacji i współpracy z organami ścigania z państw trzecich, które powodują, że reakcja na zawiadomienie o istnieniu nielegalnych treści na serwerach za granicą jest niewystarczająco sprawna i szybka (współpraca ta mogłaby obejmować np. stworzenie punktów kontaktowych dla odpowiednich instytucji za granicą).

(3) Należy stworzyć europejski system corocznego raportowania o postępach w usuwaniu nielegalnych treści z Internetu. Konsekwentne stosowanie tego środka umożliwi instytucjom Unii Europejskiej ocenę sukcesów i porażek poszczególnych państw członkowskich na płaszczyźnie krajowej i międzynarodowej, co z kolei pomoże w promowaniu najlepszych praktyk i zagwarantowaniu, że podejmowane są maksymalne starania na polu wykrywania przestępstw, ścigania sprawców i identyfikowania ofiar.

W załączeniu przesyłam odpowiedź Fundacji Panoptykon na pytania postawione przez Panią na zakończenie debaty z 10 lutego, z zaproszeniem do jej opublikowania. W przygotowaniu tego stanowiska wykorzystaliśmy m.in. opinie ekspertów z dziedziny prawa, informatyki i telekomunikacji, które docierały do nas drogą mailową w odpowiedzi na wezwanie do wspólnego przygotowania odpowiedzi na postawione przez Panią pytania. Zapraszam również do zapoznania się z surowym materiałem – czyli oryginalnymi wypowiedziami wspomnianych ekspertów – który zgromadziliśmy na stronie: http://akcja-odpowiadamy-rpo.wikidot.com/



Katarzyna Szymielewicz

Dyrektorka Fundacji

ODPOWIEDZI FUNDACJI PANOPTYKON NA PYTANIA POSTAWIONE PRZEZ RZECZNIK PRAW OBYWATELSKICH ODNOŚNIE BLOKOWANIA TREŚCI W INTERNECIE

1. Dlaczego blokowanie jest nieskuteczne i łatwe do obejścia?

- Brak dowodów na to, że blokowanie stron WWW ogranicza dostęp do nielegalnych treści

Zablokowane strony nie znikają z sieci. Niedozwolona treść jest wciąż dostępna na serwerze. Blokowanie tylko nieznacznie utrudnia do niej dostęp. Nie ma żadnych wiarygodnych danych potwierdzających to, że osoby zainteresowane tego typu treściami nie są w stanie do nich dotrzeć (powszechnie znane metody dotarcia są przedstawione poniżej). Co więcej, takich danych nie da się zgromadzić, ponieważ komunikacja w szyfrowanych kanałach, poprzez serwery *proxy* czy sieci *peer-to-peer* jest niemożliwa lub niezwykle trudna do śledzenia i rejestrowania. Tym samym nie ma dowodów na to, że blokowanie ma jakąkolwiek skuteczność w ograniczaniu dostępu do nielegalnych materiałów w Internecie.

W debacie publicznej pojawia się zwykle tylko jeden argument na potwierdzenie skuteczności blokowania: liczba uniemożliwionych wejść na zablokowane strony internetowe (ostatnio pojawiająca liczba to 58 000 000 rocznie). Wartość tego argumentu w poważniej debacie jest bardzo ograniczona. Po pierwsze, nie bierze się w tych szacunkach pod uwagę, co rzeczywiście było przedmiotem blokowania: niszowa strona dedykowana pedofilskim treściom czy popularna strona pornograficzna albo wręcz portal, taki jak Wikipedia, na którym obok tysięcy legalnych zdjęć trafiło się jedno dyskusyjne (zdarza się, że ocena, czy na zdjęciu mamy do czynienia z dzieckiem, wymaga opinii trzech biegłych). Mając na uwadze średnią liczbę wejść na popularne strony – która w wypadku Wikipedii wynosi ok. 8 miliardów miesięcznie, a w wypadku największych serwisów pornograficznych szacuje się ją jeszcze wyżej – milionowy wynik w skali roku można uzyskać np. poprzez pomyłkowe zablokowanie kilku takich stron na okres jednego dnia. Po drugie – nawet przyjmując, że przedmiotem blokowania były tylko nielegalne treści pornograficzne - nikt nie bada, ile osób z owych 58 000 000 „zablokowanych" użytkowników w efekcie weszło na poszukiwane strony dzięki serwerom *proxy* czy sieci TOR (więcej na temat tych narzędzi poniżej).

- Brak spodziewanych rezultatów w krajach Unii Europejskiej, które wprowadziły blokowanie

W kilku krajach europejskich udało stworzyć mniej lub bardziej powszechne systemy blokujące, a zatem policje z tych krajów powinny mieć wiedzę na temat ich skuteczności. Mimo tego nie przeprowadzono – a jeśli przeprowadzono, to nie ujawniono – analizy jak blokowanie wpływa na dostępność pornografii dziecięcej i inne działania przestępcze związane z pedofilią. Skoro współpracując ze sobą europejskie policje nie publikują wyników takich analiz, należy założyć, że nie dysponują dowodami na to, że w państwach, w których stosuje się blokowanie, sytuacja uległa zmianie na lepsze.

Podobny zarzut dotyczy projektów finansowanych przez Komisję Europejską, które promują blokowanie jako formę walki z rozpowszechnianiem pornografii dziecięcej (np. CIRCAMP[1]). Komisja Europejska jak dotąd nie przedstawiła żadnych danych potwierdzających skuteczność tego mechanizmu w zmniejszaniu dostępności tego typu materiałów.

- Łatwość przenoszenia blokowanych stron na inne serwery

Ponadto, nikt nie kwestionuje faktu, że blokowane strony są natychmiast przenoszone na inne serwery. Ten fakt sam w sobie podważa skuteczność i sensowność blokowania, które generuje jedynie kosztowną „zabawę w kotka i myszkę". Np. kanadyjska gorąca linia ds. wykorzystywania dzieci zarejestrowała przenoszenie tylko jednej strony 121 razy w ciągu 48 godzin.

W związku ze świadomością tych tendencji, sama Komisja Europejska wielokrotnie powoływała się na argument nieskuteczności blokowania treści w Internecie, rezygnując z wprowadzenia tego instrumentu w ramach innych polityk. Np. w dokumencie z 2007 w sprawie oceny skuteczności sposobów walki z terroryzmem Komisja Europejska odradzała blokowanie stron ze względu na zbyt dużą techniczną łatwość ich przenoszenia z miejsca na miejsce[2]. W projekcie zielonej księgi w sprawie hazardu w Internecie, w odniesieniu do blokownia stron pojawia się stwierdzenie, że "jego skuteczność jest ograniczona"[3].

- Widoczna tendencja do umieszczania nielegalnych treści w legalnych serwisach

Kolejną tendencją, istotnie podważającą skuteczność i sensowność blokowania stron zawierających obrazy seksualnego wykorzystywania dzieci jest widoczna tendencja, polegająca na zanikaniu stron dedykowanych treściom pedofilskim oraz wykorzystywaniu w celach hostingowych legalnych stron i usług bądź twardych dysków komputerów przejętych bez wiedzy ich właścicieli. Blokowanie tego typu treści jest albo technicznie niemożliwe (w przypadku treści umieszczonych na bezprawnie przejętych twardych dyskach), albo jednoznaczne z ocenzurowaniem legalnych treści (w przypadku zablokowania np. popularnego serwisu do hostingu zdjęć).

Tę tendencję potwierdzają doniesienia podmiotów profesjonalnie zajmujących się blokowaniem treści pedofilskich. Na przykład sponsorowana przez Komisję Europejską gorąca linia ds. walki z pornografią dziecięcą w Wielkiej Brytanii donosi o znaczącym wzroście ilości stron, których *de facto* nie da się skutecznie zablokować. Jednocześnie nielegalne treści umieszczane w legalnych serwisach lub dzięki przejęciu kontroli nad cudzym sprzętem są bardzo łatwe do usunięcia i skutecznego wyeliminowania z Internetu: właściciele takich serwisów lub sprzętu są skłonni usuwać nielegalne treści natychmiast, jak tylko zostaną powiadomieni o ich istnieniu.

- Nieudane doświadczenia z zastosowaniem podobnej technologii do eliminowania innych niechcianych zjawisk (spam, wirusy komputerowe)

Za istotny dowód nieskuteczności blokowania treści w Internecie mogą również posłużyć nieudane doświadczenia z eliminowaniem innych niechcianych zjawisk, które (podobnie jak

[1] http://circamp.eu/index.php?option=com_content&view=article&id=11:circamp-overview&catid=1:project&I.
[2] Ocena skutków decyzji ramowej Rady w sprawie terroryzmu, opublikowana przez Komisję Europejską http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2007:1424:FIN:EN:PDF.
[3] http://www.statewatch.org/news/2011/jan/eu-com-draft-green-paper-on-internet-gambling.pdf.

blokowanie) zakładały potrzebę skontrolowania pakietów przesyłanych przez sieć. Najbardziej jaskrawym przykładem są wirusy komputerowe i spam. Od lat proceder rozpowszechniania niechcianych lub niebezpiecznych treści w Internecie jest tępiony, a mimo to skala tych zjawisk nie maleje. Ten przykład pokazuje, że na każde zabezpieczenie czy blokadę szybko znajdzie się technologiczna odpowiedź. Jedyną skuteczną metodą eliminowania cyberprzestępczości i spamu jest tropienie osób odpowiedzialnych za generowanie tych zjawisk i pociąganie ich do odpowiedzialności karnej. Tę samą logikę należy zastosować do rozpowszechniania tzw. pornografii dziecięcej.

- Łatwość omijania blokad w dostępie do treści i rozwój technologii anonimizujących

Wreszcie, warto zaznaczyć, że ominięcie infrastruktury blokującej jest niezwykle proste i każdy użytkownik Internetu może tę umiejętność opanować w kilka minut. Najbardziej popularne metody to: skorzystanie anonimowego serwera *proxy*[4], tunelowania (VPN), sieci TOR, możliwości przesyłania danych w sieci *peer-to-peer* czy alternatywnego systemu DNS[5]. Wraz z postępującym rozwojem i komercjalizacją technologii anonimizujących stanie się to jeszcze łatwiejsze, tym bardziej, że rząd USA po raz kolejny ogłosił, że przeznacza miliony dolarów na rozwój i wsparcie technologii omijania blokad internetowych[6]. Według USA rozwijanie tego typu narzędzi i zwiększanie świadomości użytkowników Internetu w zakresie tego, jak omijać narzucone im blokady, ma fundamentalne znaczenie dla zagwarantowania wolnego i otwartego Internetu w przyszłości, a tym samym zachowania ważnego instrumentu przemian demokratycznych[7].

- Opinie ekspertów z zakresu technologii komunikacyjnych

Z braku danych statystycznych i innych „twardych dowodów", najbardziej wiarygodnym źródłem wiedzy na temat skuteczności blokowania sieci, jakim dysponujemy, są opinie ekspertów. Warto w tym miejscu przytoczyć dwie, pochodzące z różnych środowisk i kontekstów politycznych[8].

(i) Opinia Polskiego Towarzystwa Informatycznego

Rok temu, w związku z propozycją stworzenia w Polsce Rejestru Stron i Usług Niedozwolonych, Polskie Towarzystwo Informatyczne przedstawiło zdecydowanie krytyczną opinię[9]. Eksperci PTI jednoznacznie stwierdzają, że ten instrument nie tylko nie może być skuteczny, ale także stanowi zagrożenie dla publikowania legalnych treści w Internecie. W opinii czytamy m.in.: „Właściciele stron, podlegających blokadzie, bez trudu będą mogli jej uniknąć przez odpowiednio częstą zmianę adresów IP z odpowiednio dużej puli (w przypadku zastosowania protokołu IPv6, co technicznie wydaje się być możliwe w niedalekiej przyszłości, pula ta w praktyce jest nieograniczona) albo systematyczną zmianę nazw domeny (np. przez dodawanie losowej kombinacji znaków) i kierowanie do aktualnego adresu przez inną stronę, która sama w sobie nie

[4] Np. www.proxyforall.com; www.zend2.com.
[5] http://en.wikipedia.org/wiki/Alternative_DNS_root.
[6] http://www.state.gov/secretary/rm/2010/01/135519.htm.
[7] http://wyborcza.pl/1,75477,9119720,USA_wyzwola_internet.html.
[8] Polskie Towarzystwo Informatyczne to polska organizacja zrzeszająca ekspertów z dziedziny informatyki, która stawia sobie cele naukowe, społeczne i edukacyjne – natomiast nie reprezentuje biznesu. EuroISPA to międzynarodowa organizacja branżowa, reprezentująca na forum Unii Europejskiej interesy podmiotów świadczących usługi internetowe.
[9] http://www.pti.org.pl/index.php/corporate/content/download/2448/24324/file/Opinia%20PTI%20nt%20Rejestru%20Stron%20i%20Us%C5%82ug%20Niedozwolonych.pdf.

będzie zawierała żadnych nielegalnych treści, a więc nie będzie podstaw do jej zablokowania. (…) Każda osoba, nawet bez żadnego przygotowania technicznego, może ominąć blokadę za pośrednictwem serwerów proxy, dostępnych przez zaszyfrowany protokół komunikacyjny. Nie jest możliwe określenie, z jakimi stronami kontaktuje się użytkownik takiego serwera, a sam serwer bez wątpienia nie zawiera żadnych nielegalnych stron i nie ma podstaw do jego zablokowania, nawet gdyby znajdował się w Polsce". PTI w swojej opinii konkluduje: „Z przyczyn technicznych w demokratycznym systemie prawnym nie da się zrealizować skutecznej blokady dostępu do stron, których treść narusza polskie prawo. Jedynym skutecznym środkiem pozostaje sprawne ściganie i karanie osób naruszających prawo. Należy dążyć do usprawnienia tych działań, np. przez powierzenie spraw dotyczących przestępstw internetowych wskazanym prokuraturom i sądom i skoncentrowanie tam osób dobrze znających tę tematykę".

(ii) Opinia Europejskiego Stowarzyszenia Dostawców Usług Internetowych

W odpowiedzi na aktualnie dyskutowany projekt dyrektywy w sprawie zwalczania seksualnego wykorzystywania dzieci, Europejskie Stowarzyszenie Dostawców Usług Internetowych (EuroISPA) wystosowało apel do Parlamentu Europejskiego o wdrożenie systemu usuwania internetowej pornografii dziecięcej ze stron źródłowych, jednocześnie krytykując projekt blokowania takich treści. Zdaniem przedstawicieli EuroISPA nakładanie na operatorów obowiązku filtrowania i blokowania treści jest złym rozwiązaniem, ponieważ stwarza jedynie pozory robienia czegoś użytecznego, podczas gdy bardzo łatwo można taką barierę obejść. Zdaniem EuroISPA, usunięcie treści źródłowych o charakterze pornograficznym jest jedynym skutecznym środkiem technicznym, którego wprowadzenie przyniesie oczekiwany efekt. Operatorzy zwracają uwagę na to, że poprzez samo blokowanie stron, treści pornograficzne nie znikają z sieci i są dostępne dla osób, które mogą stanowić realne zagrożenie dla dzieci. Malcolm Hutty, prezes EuroISPA, powiedział: "Jeśli chcemy by dyrektywa dotycząca wykorzystywania seksualnego dzieci była jak najbardziej restrykcyjna, należy położyć nacisk na stworzenie skutecznych procedur szybkiego lokalizowania i usuwania cyberpornografii. Blokowanie stron nie jest skuteczną bronią i powinno się go unikać. Należy zrewidować procedury w taki sposób, aby przepływ informacji między organami egzekwującymi prawo o zwalczaniu pornografii a operatorami sieci odbywał się szybko i bez zakłóceń."

2. Dlaczego blokowanie jednego typu treści może doprowadzić z czasem do blokowania innych rodzajów treści/usług?

Po pierwsze, takie sytuacje już mają miejsce. Wielka Brytania początkowo wprowadziła blokowanie stron na zasadach swoistej samoregulacji – jako środek dobrowolny dla dostawców Internetu i tylko w stosunku do tzw. pornografii dziecięcej. Jednak już w kwietniu ubiegłego roku wprowadzono prawo, które nakazuje blokowanie stron służących do nielegalnej wymiany plików. Podobna ewolucja prawa dokonała się w Danii, gdzie niedługo po wprowadzeniu blokowania stron z obrazami seksualnego wykorzystywania dzieci pojawił się projekt prawa nakładającego na dostawców Internetu obowiązek blokowania nielicencjonowanych serwisów hazardowych. Co więcej, w państwach, gdzie funkcjonują mniej lub bardziej powszechne systemy blokowania, także sądy zaczynają wykorzystywać ten instrument, jako użyteczny środek egzekwowania prawa w obszarach wykraczających poza jego pierwotne przeznaczenie. W

szczególności zdarzało się, że sądy orzekające w sprawach o naruszenie prawa autorskiego nakazywały blokowanie treści, które uznawały za nielegalnie dystrybuowane.

W tym miejscu warto zauważyć, że bez względu na ewolucję przepisów prawnych, zdarzają się – i są udokumentowane – przypadki blokowania legalnych treści, wynikające z tego, że wszelkie systemy filtrujące i blokujące są obarczone dużym ryzykiem błędów. Ostatnio bardzo głośny był przypadek zablokowania 84 000 przypadkowych stron w USA[10], właśnie w ramach strategii blokowania stron z pornografią dziecięcą.

Po drugie, plany zastosowania blokowania jako narzędzia „walki" z innymi niepożądanymi zjawiskami w Internecie wyraźnie widać w dokumentach strategicznych Komisji Europejskiej. Unia Europejska w ramach prac badawczych finansuje rozwijanie oprogramowania do kontroli Internetu. W przeszłości bez powodzenia usiłowano opracować techniczne środki zabezpieczające prawa autorskie (Digital Rights Management – DRM), które byłyby w zgodzie z obowiązującym prawem. Od kilku lat finansowane jest rozwijanie oprogramowania służącego do blokowania. Za tymi pracami badawczymi w zakresie zwiększania nadzoru nad Internetem idą poszukiwania pól dla praktycznego zastosowania ich wyników. Jedna z takich prób dotyczyła nielicencjonowanego hazardu. W projekcie zielonej księgi w sprawie hazardu pojawia się stwierdzenie, że „możliwość blokowania dostępu do treści operatorom nieposiadającym licencji ogólnokrajowych może być uzasadniona"[11]. Blokowanie również pojawia się w kontekście propozycji wzmocnienia narzędzi egzekwowania praw autorskich w Internecie. W opinii Komisji Europejskiej dotyczącej głośnej sprawy Scarlet v. Sabam, która toczy się właśnie przed Europejskim Trybunale Sprawiedliwości, czytamy, że „ani odpowiednie dyrektywy ani prawo do prywatności czy swobody wypowiedzi nie są przeszkodą dla wprowadzenia systemu filtrującego, którego celem byłoby rozpoznawanie i blokowanie plików, co do których uprawnione osoby zgłaszają swoje roszczenia z tytułu prawa autorskiego"[12].

Po trzecie, takie zagrożenie potwierdza ogólna tendencja, zaznaczająca się w przypadku różnych środków ograniczających wolności obywatelskie. Najnowsza historia prawa pokazuje, że zazwyczaj wprowadzeniu kontrowersyjnych środków ograniczenia wolności towarzyszy albo logika stanu wyjątkowego (np. potrzeba walki z terroryzmem w przypadku ograniczeń swobód obywatelskich wprowadzanych w Wielkiej Brytanii i USA) albo zapewnienia, że środki te będą stosowane jedynie w szczególnych, uzasadnionych okolicznościach (np. wprowadzanie monitoringu wizyjnego w Wielkiej Brytanii, które było pomyślane jako wyjątkowe zabezpieczenie). W każdym z przywołanych przypadków środek o charakterze wyjątkowym był następnie „oswajany" i zaczynał być stosowany w sposób rutynowy, w ramach prewencji kryminalnej czy ogólnej polityki bezpieczeństwa.

[10] https://www.cdt.org/speech/pennwebblock/index.php.
http://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216/
[11] http://www.statewatch.org/news/2011/jan/eu-com-draft-green-paper-on-internet-gambling.pdf.
[12] http://itm.mlex.com/Attachments/2011-01-13_1B8G0W13A97M04RY/C70_10%20FR %20Hearing.pdf.

3. Co wskazuje na to, że blokowanie nielegalnych treści najprawdopodobniej będzie używane jako środek zastępczy, a nie uzupełniający skuteczne ściganie sprawców i usuwanie treści?

Przede wszystkim doświadczenia z krajów już stosujących blokowanie pokazują, że nie jest ono używane jako część kompleksowej strategii walki z seksualnym wykorzystywaniem dzieci, ale jako łatwe panaceum zastępujące trudniejsze działania. Np. duńska policja podczas przesłuchania w Niemieckim Parlamencie potwierdziła, że zaprzestała nawet przekazywania informacji o nielegalnych stronach organom ścigania innych państw i ograniczyła się tylko do ich blokowania u siebie. Również sama Komisja Europejska wydaje się być przekonana, że skuteczne usuwanie treści oraz ściganie sprawców to cel nieosiągalny i warto się z nim mierzyć. W materiałach roboczych przedłożonych przez Komisję Europejską wraz ze wstępnym projektem dyrektywy stwierdza się, że usuwanie u źródła pornografii dziecięcej jest często niemożliwe lub trwa zbyt długo. Blokowanie przedstawiane jest w nich jako działanie skuteczne, w przeciwieństwie do mało skutecznego usuwania. Taka ocena sytuacji pochodzi od kręgów policyjnych, czy też kręgów politycznych nadzorujących policję – a zatem nie należy jej bynajmniej bagatelizować.

Te obawy, związane z negatywnymi konsekwencjami wdrożenia blokowania z punktu widzenia eliminowania nielegalnych treści i ścigania sprawców, potwierdzają praktyczne obserwacje Fundacji Kidprotect.pl, która na co dzień współpracuje z organami ścigania. W większości spraw dotyczących tworzenia lub rozpowszechniania pornografii dziecięcej eksperci fundacji napotykają niechęć po stronie prokuratur do podejmowania i prowadzenia tego typu spraw. Powodem tego jest ich czasochłonność, skomplikowanie i wysokie koszty procesowe. W tym kontekście wydaje się więcej niż prawdopodobne, że z momentem pojawienia się instrumentu bardzo prostego w zastosowaniu, szybkiego i nie generującego kosztów (bezpośrednio po stronie policji) – jakim byłoby blokowanie stron z nielegalnymi materiałami – organy ścigania znalazłyby się pod silną presją, żeby stosować to prowizoryczne i nieskuteczne rozwiązanie zamiast prowadzić rzetelne śledztwo.

Tę niebezpieczną tendencję udowodnił też eksperyment przeprowadzony przez niemiecką grupę AK Zenzur[13]. Aktywiści przeprowadzili analizę „czarnej listy" (listy zablokowanych stron internetowych z domniemanymi treściami o charakterze pornografii dziecięcej), która wyciekła w Danii i okazało się, że niektóre ze stron – umieszczone na serwerach w USA – są już na tej liście ponad dwa lata. Co ciekawe, po zawiadomieniu właścicieli serwerów (bezpośrednio przez osoby z AK Zenzur, a zatem osoby pozbawione szczególnego autorytetu, jakim cieszą się np. organy ścigania) strony te zniknęły z Internetu w ciągu 30 minut. Zarówno ten wyrywkowy eksperyment, jak i badania prowadzone w USA na szeroką skalę pokazują, że stron z tzw. pornografią dziecięcą nie trzeba blokować – można je skutecznie usuwać. Natomiast sam akt zablokowania strony zdecydowanie tę perspektywę skutecznego usunięcia treści z Internetu oddala.

4. Dlaczego nie należy dopuszczać blokowania nawet jako rozwiązania doraźnego (tymczasowego)?

[13] http://ak-zensur.de/2010/09/29/analysis-blacklists.pdf.

Z dwóch zasadniczych powodów. W przypadku wprowadzenia blokowania jako rozwiązania doraźnego (tymczasowego) pojawiają się dokładnie te same zagrożenia dla wolności oraz te same wątpliwe korzyści.

Po pierwsze, samo wprowadzenie infrastruktury cenzurującej – czyli stworzenie technicznych możliwości filtrowania i blokowania treści w Internecie na poziomie podmiotów, które tę treść[14] dostarczają zwykłym użytkownikom - stanowi istotne ograniczenie praw obywatelskich i generuje wszystkie zagrożenia, o których była już mowa (m.in. przypadkowe blokowanie legalnych treści, ryzyko objęcia tym mechanizmem innych typów treści). Ponadto, samo zagrożenie blokowaniem stron – bez względu na czas trwania – wywoła przewidywalny efekt w środowisku przestępczym. Jest bardzo prawdopodobne, że w odpowiedzi na wprowadzenie takiego instrumentu, przestępcy – którym zależy na uniknięciu wykrycia – zaczną rutynowo szyfrować swoje komunikaty i używać powszechnie dostępnych narzędzi anonimizujących. Eksperci współpracujący z organami ścigania twierdzą, że teraz udaje się przynajmniej łapać „leniwych" przestępców. Po wprowadzeniu mechanizmów filtrujących i blokujących na szeroką skalę być może część z przestępców zrezygnuje ze swojej działalności w obawie przed wykryciem, ale większość zapewne się „dokształci" – tym samym utrudniając pracę policji. Tych wszystkich negatywnych skutków i zagrożeń nie da się uniknąć przez sam fakt wprowadzenia czasowego ograniczenia blokowania.

Po drugie, nie wydaje się, aby blokowanie stosowane jako środek doraźny (tymczasowy) mogło przynieść jakiekolwiek wymierne korzyści. Przede wszystkim, nie można byłoby zastosować takiego środka w sytuacji, gdy zaalarmowanie domniemanego przestępcy mogłoby przynieść szkodę śledztwu. Ten warunek eliminuje zastosowanie takiego środka w większości przypadków, zakładając poważne podejście organów ścigania do eliminowania treści i namierzania sprawców. Zakładając jednak jego zastosowanie w niektórych przypadkach, blokowanie doraźne (tymczasowe) będzie wykazywało te same fundamentalne wady, jakie zostały omówione powyżej: nieskuteczność i łatwość ominięcia. Tym samym, wszystkie osoby rzeczywiście zainteresowane nielegalnymi treściami będą mogły tę barierę przełamać, a zatem nie wywrze ona realnego efektu na ograniczenie zjawiska wtórnej wiktymizacji ofiar przemocy. Jedyna wyobrażalna korzyść z zastosowania blokowania doraźnego (tymczasowego) to czasowe ograniczenie możliwości przypadkowego trafienia na nielegalny materiał w Internecie. Biorąc jednak pod uwagę bardzo niskie prawdopodobieństwo takich przypadkowych zetknięć z pornografią dziecięcą oraz opisane powyżej koszty społeczne, wydaje się, że ten środek nie powinien przejść testu proporcjonalności w demokratycznym państwie.

5. Czy blokowanie stron – ze względów technicznych – musi działać jako „system wczesnego ostrzegania przestępców"?

Tak, zawsze będzie to sygnał, że podjęte zostały działania zapobiegawcze. Każdy serwer rejestruje ilość zapytań (czyli próśb o dostarczenie treści poszczególnych stron WWW, które są na tym serwerze przechowywane) kierowanych do niego przez użytkowników Internetu. Jest to narzędzie neutralne i wręcz konieczne do sprawnego obsługiwania ruchu kierowanego na

[14] w sensie technologicznym są to pakiety informacji

serwer. Z zasady administratorzy poszczególnych stron mają stały i bezpośredni dostęp do tych danych, ponieważ także w ich przypadku wiedza na temat liczby zapytań o treść strony internetowej jest niezbędna do działania. Na podstawie tych standardowo dostępnych danych administratorzy mogą w czasie rzeczywistym rejestrować, czy ilość zapytań o treść prowadzonej przez nich strony rożnie lub maleje. Nagły spadek "odwiedzin" na stronie jest sygnałem alarmowym, który można łatwo zweryfikować poprzez próbę wejścia na zablokowaną stronę. Nie da się zatem wyeliminować ostrzegawczej funkcji blokowania stron internetowych.

6. **Czy problem pojawiania się w spamie odnośników do treści z tzw. pornografią dziecięcą jest poważny?**

   Nie jest. Liczba osób zachęconych w ten sposób do zainteresowania się pornografią dziecięca jest tak nikła, że trudno byłoby nawet przeprowadzić badanie, ile jest takich przypadków. Ze względów czysto ekonomicznych należy przypuszczać, że spamerzy mają o wiele większe korzyści z umieszczania w spamie odnośników do innego typu treści (ofert sprzedaży nielegalnych substancji, leków, środków i usług kosmetycznych, stron fishingowych itp.)

7. **Czy rozwiązaniem problemu mógłby być system "oddolnej samoregulacji" użytkowników Internetu lub ISPs; a jeśli tak, jaki?**

   Fundacja Panoptykon zadała to pytanie – na otwartym forum – osobom znanym z zaangażowania w rozwój polskiego Internetu i świadomym oddolnych tendencji w różnych środowiskach internetowych. Oto zestawienie najciekawszych odpowiedzi (zachowaliśmy oryginalną pisownię):

   - Co do tworzenia "ruchu obrońców", (…) to trochę tak jakby tworzyć ludową milicję bez żadnych uprawnień, równolegle do policji. Normalny internauta nie zajmuje się wyszukiwaniem treści pornograficznych, zresztą nawet nie powinien się tym zajmować. Zdecydowanie natomiast byłoby nieźle, gdyby w przypadku trafienia na takowe miał możliwość zgłoszenia podejrzenia popełnienia przestępstwa nie tylko do dyżurnetu, kidprotecta czy podobnych inicjatyw bądź co bądź pozapaństwowych ale bezpośrednio na policję (i żeby nie musiał w tym celu udawać się osobiście na najbliższą komendę, gdzie poczeka sobie aż będzie dostępny funkcjonariusz z uprawnieniami do wypełniania odpowiednich formularzy). Tyle, że opracowania na poziomie – powiedzmy – profilu zaufanego w e-PUAPie obsługi zgłoszenia przestępstwa to nie jest praca dla środowiska fascynatów, ale dla urzędników państwa (opłacanych z tychże fascynatów podatków). (Maciej Szmit)

   - Należałby zrównać IAPów [*Internet access providers*] z drukarzami, kamerzystami i radiowcami, którzy powinni mieć w takim razie obowiązek wyłączenia transmisji słuchowiska/wstrzymania druku prasy/zaprzestania transmisji widowiska telewizyjnego zawierających w ich mniemaniu informację zakazaną. Podobnie należałoby nałożyć odpowiednie nakazy prawne na firmy zajmujące się dystrybucją gazet i książek, na kioskarzy i właścicieli księgarń: po otrzymaniu wiarygodnego donosu kioskarz powinien zdejmować gazety z wystawy i dzwonić do innych kioskarzy w całym kraju, żeby zrobili to samo. Dlaczego sprzedawca książek ma mieć lepiej i móc być mniej biegłym w seksuologii od administratora routera dostępowego? (Maciej Szmit)

- Rejestr brytyjski, na który się powoływała np. Fundacja Dzieci Niczyje, to właśnie przykład samoregulacji. Operatorem jest organizacja non-profit powołana przez brytyjskich operatorów Internetu, a korzystanie z publikowanej listy jest dobrowolne (pokrycie chyba ok. 95%). Samoregulacja to także sprawne i ujednolicone procedury zgłaszania takich treści, a także usuwania i współpracy z organami ścigania. (Paweł Krawczyk)

- Procedury są – jest Porozumienie Na Rzecz Bezpieczeństwa Dzieci w Internecie, samoregulacja właśnie. Większość operatorów daje u siebie linki do jednego z hotline - naszego lub Dyżurnet. Myślę, że to udostępnianie to coś, co warto rozwijać. Na pewno brakuje platformy współpracy operatorów, dostawców treści, organizacji pozarządowych i organów ścigania. Choć i tu bym nie panikował - jest np. coroczna konferencja TAPT w Szczytnie, gdzie wszyscy prawie się spotykają i rozmawiają. (Jakub Śpiewak)

- Problem z samoregulacją polega na tym, ze de facto musiałaby to być samo-regulacja środowisk publikujących i korzystających z pornografii dziecięcej - co jest niemożliwe. w każdym innym wypadku te środowiska niemal na pewno ominą, za pomocą technicznych środków, mechanizmy samoregulacji. dlatego zgadzam się z głosami, że raczej trzeba tu liczyć na "twarde" ściganie przestępstw i przestępców. (Aleksander Tarkowski)

- Tam gdzie samoregulacja funkcjonuje (W. Brytania i Skandynawia) jest to samoregulacja organizacji zwalczających pornografię dziecięcą i operatorów telekomunikacyjnych, którzy współpracują z policją. Moim zdaniem to działa (choć głos oponentów w związku zakusami aby regulować Internet chyba przybiera na sile) ze względu na to, że w tych społeczeństwach państwo oferuje obywatelom także rzeczy które są im potrzebne do życia (np. jakiś standard służby zdrowia). Dzięki temu usługa jak filtrowanie Internetu jest odbierane jako część tej szerszej oferty. Poza tym państwo (w tym policja) jest na tyle praworządne i uczciwe, że jak obiecało że chodzi o filtrowanie pornografii dziecięcej to pod byle pretekstem nie przekracza takiej granicy.

Dla większości społeczeństw europejskich (a szczególnie w Polsce) państwo jest wrogiem obywatela, a co najmniej oszukuje go odnośnie tzw. usług powszechnych, które jeśli są to mają bardzo niska jakość. Na tym podglebiu mało kto uwierzy, że państwu pozwalającemu na samoregulację nie chodzi o wprowadzenie cenzury, a organizacje antypornograficzne i inni zwolennicy takich działań filtrujących mogą mieć uczciwe zamiary. (Józef Halbersztadt)

- Problem w tym, że w przypadku takim jak filtrowanie Internetu dochodzi do kolizji wartości i praw podstawowych. Społeczeństwo może uważać, że także w tej sprawie do państwa nie można mieć zaufania. Jednak w przeszłości, którą ocenia się za praworządną kiedy społeczeństwo uważało, że należy ograniczyć władze państwa czyniło to poprzez prawo. Np. dlatego wprowadzono trójpodział władzy. Wprowadzenie samoregulacji oznacza, że do ważenia racji w kolizji między moralnością i ochrona wrażliwości jednostek, a zagrożeniem dla wolności wprowadza się elementy pozaprawne. Władzę sądowniczą wyspecjalizowaną w prawnym wyważaniu racji zastępuje się milicją moralną i podmiotami komercyjnymi jakimi są operatorzy. Dla żadnej z tych stron wolność nie jest przedmiotem istotnego zainteresowania. To podważa samo stosowanie zasady samoregulacji w tego rodzaju sytuacjach. (Józef Halbersztadt)

- Samoregulacja dostawców usług internetowych miałaby tutaj jeden zasadniczy plus dla nich samych - pozwoliłaby im na zaimplementowanie w sposób możliwie najprostszy i najtańszy dla nich. Dla podatników zresztą też - przypomnijcie sobie 5 mln zł i hordy nowych etatów opisane w projekcie RSiUN. Gdyby polscy ISP wprowadzili samoregulację i obejmowałby ona choćby 60% największych ISP to administracja straciłaby główny argument propagandowy dla wprowadzania cenzury. Przy czym jako samoregulację rozumiem ujednolicenie procedur zgłaszania i kasowania treści pedofilskich, a nie system brytyjski z faktycznym blokowaniem stron. (Paweł Krawczyk)