Wyciek planu arbitralnego cenzurowania sieci

22 września 2012

Projekt „Czysty Internet” ma służyć zwalczaniu terroryzmu dzięki tzw. dobrowolnym środkom kontrolowania tego, co robią użytkownicy sieci. Wewnętrzny dokument, który właśnie wyciekł, ujawnia szczegóły tego niebezpiecznego przedsięwzięcia i zaprzecza wielu wcześniejszym zapewnieniom. Projekt jest finansowany przez Komisję Europejską i, nie bez powodu, cieszy się dużym zainteresowaniem firm oferujących technologie filtrowania treści. Równocześnie wiele rządów zdecydowało się zwiększyć dofinansowanie dla projektów, które mają na celu rozwój takich technologii.

Zanim doszło do wycieku, organizacje drążące sens i cele projektu „Czysty Internet” otrzymywały od jego koordynatorów zapewnienia, że projekt „będzie się skupiał się diagnozie problemów, a w dalszym toku prac zostaną zaproponowane konkretne rozwiązania legislacyjne”. Słyszeliśmy również, że nie jest jego celem ograniczanie takich działań użytkowników, które nie są zabronione przez prawo. Ujawniony właśnie dokument nie pozostawia jednak wątpliwości, że głównym celem całego przedsięwzięcia jest wprowadzenie praktycznych (pozaprawnych!) rozwiązań, które umożliwią blokowanie treści kontrowersyjnych, ale nie zakazanych przez prawo. Koncepcja „Czystego Internetu” opiera się właśnie na założeniu, że firmy prywatne powinny zapewnić dodatkową ”warstwę” bezpieczeństwa, chroniącą społeczeństwo przed „niechcianymi” treściami, których nie można wyeliminować przy wykorzystaniu istniejących prawnych procedur.

„Czysty Internet”, którego celem jest walka z terroryzmem, powiela wiele rozwiązań promowanych przez koalicję szefów firm telekomunikacyjnych i technologicznych (CEO Coalition), która działa na rzecz ochrony dzieci w Internecie i również jest

finansowana ze środków Komisji Europejskiej. Oba projekty, niezależnie i nie koordynując swoich prac, rozwijają takie technologie, jak „przyciski” do zgłaszania lub oznaczania (oflagowywania) treści w sieci, tym samym powielając badania nad dobrowolnymi metodami powiadamiania oraz usuwania potencjalnie nielegalnych treści z Internetu.

Projekt „Czysty Internet” zakłada, że dostawcy usług internetowych „dobrowolnie” zobowiążą się do aktywnego nadzorowania swoich klientów, blokowania i filtrowania treści. Na tej bazie ma powstać sieć składająca się z zaufanych informatorów online. Wbrew wcześniejszym zapewnieniom, twórcy projektu rekomendują również zaostrzenie prawa w poszczególnych państwach członkowskich. Wreszcie, wykraczając daleko poza obowiązujące ramy prawne, „Czysty Internet” promuje wykorzystywanie ogólnych warunków umów do usuwania „w pełni legalnych” treści, pozostawiając decyzję co do priorytetów “etyce biznesu”, jaką wyznaje dana firma. Projekt zmierza tym samym do stworzenia prywatnych mechanizmów cenzury, które będą egzekwowane w oparciu o ogólne warunki umów i nie będą poddane żadnej kontroli sadowej.

Oto najważniejsze z proponowanych rozwiązań:

– Prawo zezwalające policji na kontrolowanie przepływu informacji w sieci, łącznie z (teoretycznie anonimowymi) dyskusjami online.

– Usunięcie wszelkiego ustawodawstwa, które zabrania filtrowania treści lub kontrolowania tego, co pracownicy w swoich godzinach pracy przeglądają w sieci.

– Organy egzekwujące prawo powinny być w stanie usunąć daną treść “bez potrzeby stosowania skomplikowanych i sformalizowanych procedur”, zgodnie z zasada “zaobserwuj i zareaguj”.

– “Świadome” udostępnianie linków do “treści związanych z działalnością terrorystyczną” (co istotne, projekt nie odnosi

się do treści uznanych za nielegalne przez sąd ale do niezdefiniowanych, ogólnie rozumianych "treści związanych z działalnością terrorystyczną") powinno stanowić przestępstwo na takiej samej zasadzie, jak owa działalność terrorystyczna.

– Stworzenie podstaw prawnych dla obowiązkowego systemu identyfikacji on-line (tzw. prawo "potwierdzonej tożsamości") aby zapobiec anonimowemu korzystaniu z usług internetowych.

– Dostawcy usług internetowych powinni być pociągani do odpowiedzialności za niewykorzystywanie w "rozsądny" sposób możliwości sprawowania nadzoru elektronicznego w celu identyfikowania (bliżej niezdefiniowanej) działalności terrorystycznej w Internecie.

– Firmy udostępniające technologie filtrujące oraz ich klienci powinni być pociągani do odpowiedzialności w przypadku niezgłoszenia "nielegalnych" treści rozpoznanych przez programy filtrujące.

– Użytkownicy powinni być również pociągani do odpowiedzialności za "świadome" zgłaszanie treści, które nie są nielegalne.

– Rządy powinny brać pod uwagę stopień zaangażowania dostawców usług internetowych w filtrowanie (nadzorowanie) treści w Internecie przy rozstrzyganiu publicznych przetargów na usługi internetowe.

– Systemy "ostrzegawcze" oraz blokujące treść powinny stać się integralną częścią serwisów społecznościowych.

– Anonimowość użytkowników zgłaszających (potencjalnie) nielegalną treść powinna zostać zachowana… jednak ich adresy IP powinny być rejestrowane, aby umożliwić ściganie w przypadku podejrzenia, że świadomie zgłaszają treści, które są legalne lub umożliwić szybsze analizowanie zgłoszeń od zaufanych informatorów.

– Firmy powinny wdrożyć systemy monitorujące treści udostępniane przez ich klientów on-line, tak aby treści raz usunięte, lub treści do nich podobne, nie były przesyłane i udostępniane ponownie.

– Należy przejść od systemu opartego na literze prawa, w którym to sąd decyduje o tym, czy dana treść narusza prawo, do systemu, w którym organy egzekwujące prawo (np. policja) są w stanie wydawać decyzje quasi-sądowe i żądać od dostawców usług internetowych usuwania treści z sieci.

Pełna treść dokumentu TUTAJ.

Źródło: Fundacja Panoptykon