Centrum Cyfrowe
ul. Andersa 29
00-159 Warszawa
centrumcyfrowe.pl
kontakt@centrumcyfrowe.pl

Warszawa, 10 maja 2016

Stanowisko Centrum Cyfrowego w sprawie blokowania stron internetowych

Dotyczy projektu ustawy o działaniach antyterrorystycznych z 5 maja 2016 w zakresie blokowania danych informatycznych mających związek ze zdarzeniem terrorystycznym

We współczesnym świecie bezpieczeństwo musi być ważone wraz z innymi wartościami: wolnością słowa, prawem do prywatności, domniemaniem niewinności. Przepisy kreujące infrastrukturę bezpieczeństwa muszą być precyzyjne, proporcjonalne, a przede wszystkim skuteczne. Skoro tworzą ograniczenia dla swobody ruchu czy wypowiedzi, jako społeczeństwo nie możemy pozwolić sobie na wdrażanie regulacji, które nie przynoszą dobrych rezultatów przy tego rodzaju ograniczeniach. Możliwość zablokowania dostępu do danych ponieważ mogą one mieć związek ze zdarzeniem terrorystycznym nie spełnia żadnego z warunków, które powinny być brane pod uwagę przy tworzeniu polityk bezpieczeństwa. Blokowanie jest łatwe do obejścia, nieskuteczne dla realizacji tak zdefiniowanego celu oraz otwiera możliwości nadużycia infrastruktury blokującej dla celów wykraczających poza oryginalny zamysł ustawodawcy.

Projekt ustawy antyterrorystycznej w zakresie blokowania danych informatycznych mających związek ze zdarzeniem terrorystycznym budzi następujące zastrzeżenia:

1. Nieefektywność

Blokowanie treści w internecie nie usuwa ich trwale z sieci, a jedynie blokuje ich dostępność.
W stosunku do treści o niskiej szkodliwości czy braku znamion przestępstwa jest to rozwiązanie nieproporcjonalne, a w stosunku do treści które są nielegalne nie rozwiązuje ono problemu ich ogólnej dostępności po czasie trwania blokady. Rozwiązanie to jest zarazem nazbyt restrykcyjne dla ogółu przypadków i nieskuteczne dla tych, które wymagają rzeczywistej interwencji organów ścigania. Jako takie nie realizuje celu ustawy i dlatego też nie powinno być narzędziem w walce z zagrożeniem terrorystycznym.
Blokowanie stron nie dosięgnie też ewentualnych treści o charakterze terrorystycznym, gdyż nie są one dostępne w miejscach, gdzie blokowanie treści mogłoby skutecznie zajść. Zdaniem twórców

projektu proponowane rozwiązanie ma zapobiegać prowadzeniu działalności terrorystycznej przez organizacje terrorystyczne, szczególnie w kontekście instruktażu i kontaktowania się z członkami siatki terrorystycznej. Należy pamiętać, że treści udostępniane przez organizacje terrorystyczne rzadko dostępne są w tradycyjny sposób, o wiele częściej wykorzystywany jest tzw. darknet (inaczej deep net, poziom sieci niedostępny dla przeciętnego użytkownika, wymagający koszystania z określonych narzędzi i ustawień), który wymyka się krajowym regulacjom.

2. Niebezpieczny precedens

Mechanizm blokowania danych w internecie nie polega na usunięciu treści, a blokowaniu dostępu do nich poprzez filtrowanie zapytań o dostęp do danego adresu internetowego. Wprowadzenie takiego mechanizmu w przypadku jednego rodzaju danych, dodatkowo bez efektywnej kontroli sądowej, może skutkować chęcią blokowania różnych innych treści, np. pornograficznych czy hazardowych, ale także związanych z działalnością strażniczą czy aktywnością obywatelską polegającą na wyrażaniu sprzeciwu w debacie publicznej. Przepisy te tworzą podwaliny dla cenzury prewencyjnej i będą miały negatywny wpływ na rozwój społeczeństwa informacyjnego.

3. Brak precyzyjnych definicji

Korzystanie z internetu, a przede wszystkim publikowanie, jest formą korzystania z wolności słowa, gwarantowanej zarówno przez Konstytucję RP jak i Europejską Konwencję Praw Człowieka. Ewentualne ograniczenia tego konstytucyjnego prawa muszą spełniać zasady proporcjonalności, co nie ma miejsca w projekcie.
Po pierwsze, określenie “dane informatyczne” jest bardzo szerokie i może dotyczyć zarówno poszczególnych treści, jak i funkcjonowania całych portali internetowych, w tym również społecznościowych. W efekcie działanie Szefa ABW może doprowadzić do zablokowania protokołów, na których opierają się komunikatory (Facebook, Twitter) czy sieci anonimowej wymiany danych. Po drugie, żądanie Szefa ABW uzależnione jest tylko od związku danych z przestępstwem o charakterze terrorystycznym – definicja tego pojęcia jest również bardzo szeroka i niedookreślona. W proponowanym projekcie zarówno pojęcie “danych informatycznych” jak i “przestępstw o charakterze terrorystycznym” definiowane będzie przez Szefa ABW, przez co skutkować może szeroką kontrolą zarówno treści, jak i sposobu funkcjonowania internetu.

4. Brak adekwatnej kontroli sądowej

Jeśli ustawa wejdzie w życie, Szef ABW za zgodą prokuratora generalnego będzie mógł zablokować każdą treść dostepną w internecie, bez względu na jej charakter czy dostępność, biorąc pod uwagę jedynie dostrzeżone przez siebie powiązanie ze zdarzeniem o charakterze terrorystycznym.
W proponowanej regulacji następcza kontrolna sądowa jest przewidziana, jednak realnie będzie miała iluzoryczny charakter. Blokada dostępności danych informatycznych znoszona będzie w przypadku nieudzielenia przez sąd w terminie 5 dni zgody na zarządzenie zablokowania dostępności określonych danych informatycznych – biorąc pod uwagę dynamikę wymiany informacji

we współczesnym świecie 5 dni oczekiwania na następczą kontrolę sądową ograniczy wolność słowa i zakłóci funkcjonowanie różnych form aktywności w internecie.

5. Brak kontradyktoryjności postępowania

Postanowienia Sądu Okręgowego w Warszawie, dotyczące zarówno zatwierdzenia żądania Szefa ABW, jak i przedłużenia blokowania danych informatycznych, może być zaskarżone wyłącznie przez Szefa ABW. Brak jest jakiejkolwiek konstradyktojności postępowania – zażalenia nie może złożyć zarówno osoba, której dane będą blokowane, ani też żaden inny podmiot działający w interesie społecznym. Narusza to zasadę równego traktowania stron postępowania poprzez uprzywilejowanie Szefa ABW.

6. Brak transparentności blokowania danych

Ustawa nie przewiduje żadnych mechanizmów gwarantujących transparentność działań Szefa ABW. Osoba, której dane zostaną zablokowane, nie tylko nie zostanie poinformowana o podstawie prawnej czy ewentualnych zarzutach, ale nawet o samym fakcie zablokowania danych w internecie. Poza tym, poza następczą kontrolą sądową, nie przewidziano żadnych mechanizmów społecznej kontroli np. w postaci publikowania danych nt. blokowania na wniosek Szefa ABW.

7. Wprowadzenie niepewności prawnej dla przedsiębiorców działałających w internecine

Należy pamiętać, że internet to nie tylko środowisko komunikacji, ale również przestrzeń prowadzenia działalności biznesowej. Polska ma ambicje by być krajem wspierającym e-handel i e-usługi. Jednakże wprowadzenie rozwiązań przewidzianych w projekcie skutkować będzie brakiem pewności prawnej prowadzenia działałaności gospodarczej on-line – zablokowanie możlliwości prowadzenia biznesu nawet na 5 dni jest równoznaczne ze stratami, na które wiele firm nie może sobie pozwolić. Bez jasnych ram prawnych działalności w internecie, nowe firmy będą zakładanie za granicą, a nie w Polsce.