10 powodów, dla których blokowanie Internetu to zły pomysł

30 czerwca 2017

Blokowanie Internetu w walce z terrorystami, nielegalnym hazardem – a ostatnio też nadużyciami finansowymi i Uberem – to trend, który na dobre rozgrzał wyobraźnię rządzących. I zmusza nas do tego, by co kilka miesięcy powtarzać te same, nietracące na aktualności argumenty, które zebraliśmy w 2009 r., gdy rząd Donalda Tuska chciał tworzyć Rejestr Stron i Usług Niedozwolonych. Poniżej znajdziecie 10 powodów, dla których blokowanie Internetu to zły pomysł. A na dokładkę nieco historii.

PRAGNIENIE BLOKOWANIA OD 2009 R.

Idea rozwiązywania problemów społecznych przez blokowanie stron internetowych wyszła od Donalda Tuska. W roku 2009 zaproponował on wprowadzenie Rejestru Stron i Usług Niedozwolonych. W ten sposób pod kontrolą miał znaleźć się nielegalny hazard, treści pedofilskie i promujące nienawiść w Internecie.

Pomysł wywołał istną burzę. Krytykowali go również politycy partii, która dziś jest u władzy. Ostatecznie Donald Tusk zmienił zdanie. Czy uległ presji społecznej, czy zrozumiał problem, dość że w roku 2011 twierdził, że „przestawiono mu optykę na prawa podstawowe w Internecie". Jednak od czasu do czasu pomysł blokowania pojawiał się jeszcze na ustach członków rządu Tuska (np. minister sprawiedliwości Marek Biernacki proponował blokowanie stron zawierających treści pornograficzne).

Kolejne podejście do cenzury zrobił rząd Ewy Kopacz, odkurzając pomysł stworzenia rejestru stron niedozwolonych do

blokowania e-hazardu. Wiceminister finansów Jacek Kapica mówił wtedy, że „liczy na rosnące społeczne przyzwolenie dla blokowania”. Czy miał rację i rzeczywiście stajemy się społeczeństwem mniej wyczulonym na takie próby? Za czasów Ewy Kopacz powrócił też pomysł blokowania pornografii. Ostatecznie upadł w sejmie z przyczyn formalnych.

Po dojściu do władzy politycy PiS zapomnieli o tym, jak gorąco krytykowali blokowanie za poprzedników. Rząd Beaty Szydło w ustawie antyterrorystycznej wprowadził możliwość wyłączania systemów teleinformatycznych, a krótko potem blokowanie elektronicznych bukmacherów i kasyn w ustawie antyhazardowej.

Trzeba było przypomnieć argumenty, które padały w roku 2009: raz uruchomiona machina cenzury będzie się rozwijać; dziś zablokujemy nielegalny hazard, a jutro strony niewygodne politycznie. Niestety ten scenariusz już się realizuje. W kolejce po uprawnienia do blokowania stoi KNF i Ministerstwo Infrastruktury i Budownictwa, które chcą zaprząc ten mechanizm do własnych celów. Co będzie następne?

1. ILUZJA PROSTEGO ROZWIĄZANIA

To problem o podłożu czysto psychologicznym. Zwolennicy różnych form blokowania sądzą, że znaleźli genialnie proste rozwiązanie złożonego problemu. W praktyce jednak blokowanie ani nie jest proste, ani nie stanowi rozwiązania problemu. Wyjaśnijmy to na przykładzie prostej analogii: wszystkie przypadki jazdy po pijanemu zależą od dostępu do alkoholu. Pozornie proste rozwiązanie, by uporać się z pijanymi kierowcami, to totalny zakaz sprzedaży alkoholu.

Ale żaden rząd nie wprowadzi w Polsce takiego zakazu. Z wielu przyczyn: alkohol można nie tylko kupić, ale też zrobić, a wpływy z akcyzy trudno zignorować. Kontrolowanie zakazu kosztuje. Wniosek? Prohibicja nie byłaby ani prosta do wprowadzenia, ani skuteczna. Podobnie jest blokowaniem: przekonanie o jego prostocie i skuteczności bierze się z

niewiedzy.

2. „WEŹMY SIĘ I ZRÓBCIE”, CZYLI PROBLEMY TECHNICZNO-ORGANIZACYJNE

Strony czy usługi internetowe nie mają jednego wyłącznika, który pozwala je blokować. Globalna sieć jest dość złożona, a blokować można na różnych poziomach – np. gospodarstw domowych, instytucji, sieci lokalnych, przedsiębiorców telekomunikacyjnych. Można też naciskać na różnych pośredników takich jak dostawcy hostingu dla celów biznesowych albo dostawcy „konsumenckich” e-usług. Dostawcy hostingu mogą być wzywani do blokowania całych stron lub domen. Dostawcy konkretnych usług (jak np. Google, Facebook czy Microsoft) mogą być zobowiązywani do blokowania treści (jak filmy czy obrazki) czy aplikacji dostarczanych użytkownikom końcowym.

Na gruncie technicznym dostępne są różne rozwiązania. Najbardziej kontrowersyjne oparte są o tzw. Deep Packet Inspection, czyli analizowanie przesyłanych pakietów danych pod kątem ich treści (z takiego narzędzia korzystają Chiny). Pojawia się więc dylemat: czy blokowanie ma być proste, lecz mało skuteczne, czy może bardziej złożone i skuteczniejsze, ale przez to zagrażające podstawowym prawom, takim jak prywatność?

Gdy ktoś rzuca hasło „blokujmy”, prawie nigdy nie mówi, w jaki sposób ma się to odbywać (np. nie wiemy, jak MIB chce blokować Ubera. Możliwe, że chodzi jedynie o skłonienie firm Google i Apple do zablokowania Polakom dostępu do tej aplikacji. Tylko czy to załatwi problem, czy raczej jedynie na chwilę odwróci uwagę od bardziej złożonego zagadnienia sharing economy?). Czasem słyszymy, że wiele państw już blokuje strony. To prawda, ale niemal w każdym państwie blokuje się coś innego i w nieco inny sposób. Nie istnieją żadne naprawdę sprawdzone praktyki, szczególnie w odniesieniu do państw demokratycznych, w których wolność słowa jest szanowaną wartością.

Czarne listy stron, rejestry stron niedozwolonych lub niepoprawnych – te hasła robią furorę wśród polskich decydentów. Ale i tu pojawia się szereg pytań o szczegóły ich funkcjonowania:

– Jawne czy niejawne? (Jawny rejestr jest jak książka telefoniczna ze spisem usług, które mogą interesować poszukiwaczy instrukcji tworzenia bomb domowej roboty, hazardzistów czy amatorów twardej pornografii – czyli tych, którym blokujący chcieliby życie utrudnić, a nie ułatwić. Rejestr niejawny oznacza brak społecznej kontroli nad jego funkcjonowaniem).

– Czy e-usługodawca powinien być ostrzegany, zanim zostanie wpisany do rejestru?

– Jak szybko operatorzy powinni reagować na nowe wpisy do rejestru?

– Jaką postać powinien mieć rejestr, aby spełniał swoją rolę skutecznie i tanio?

– Jak powinna wyglądać procedura odwołania od decyzji o umieszczeniu w rejestrze?

Polski ustawodawca już odpowiedział na część tych pytań, ale nie na wszystkie. Nawet tam, gdzie odpowiedzi udzielono, trudno mówić o rzetelnej legislacji. Po prostu przyjęto pewne rozwiązania i założono, że będą one dobre. A przecież coś może pójść nie tak!

3. POMYŁKI WPISANE W BLOKOWANIE

Na przestrzeni ostatnich lat różne kraje wprowadzały różne mechanizmy blokad. Ale jeszcze nikt nie stworzył systemu, który ani razu by się nie pomylił.

Wielka Brytania zasłynęła dzięki blokowaniu pornografii. Jedną z witryn zablokowanych po wprowadzeniu tego rozwiązania była… strona Claire Perry – konserwatywnej parlamentarzystki, która

sama nawoływała do blokowania treści pornograficznych. Pewien brytyjski operator blokował polski serwis Niebezpiecznik.pl, a filtr rodzinny w jednej z polskich bibliotek i w jednym z wrocławskich liceów blokował stronę panoptykon.org. Niejedną stronę zablokowano omyłkowo w USA w ramach walki z piractwem poprzez tzw. przejmowanie domen.

Jeszcze przed wprowadzeniem nowej ustawy hazardowej Ministerstwo Finansów zablokowało swoją własną stronę z wyszukiwarką organizacji pożytku publicznego, odwiedzaną przez podatników, którzy chcieli przeznaczyć 1% swojego podatku na organizacje społeczne, takie jak choćby Fundacja Panoptykon.

Przyczyny pomyłek są różne. Czasem wchodzi w grę zwykły ludzki błąd. Zdarza się też, że strony legalne i nielegalne korzystają ze wspólnych zasobów, np. z jednego dostawcy hostingu, serwera lub domeny. Czasem jest to efekt nadgorliwości (np. w Polsce służba celna chciała zablokować serwis AntyApps w związku z tym, że znalazła się na nim recenzja aplikacji uznanej za hazardową).

4. ODSZKODOWANIA, KTÓRYCH NIKT NIE CHCE PŁACIĆ

Załóżmy, że omyłkowo zablokowana zostanie strona sklepu internetowego, który z powodu przerwy straci tysiące złotych. Albo gazety, która straci przez to reputację (i pieniądze)? Kto za to zapłaci?

Prawo powinno przewidywać odszkodowania za omyłkowe blokady. Ale jak łatwo przewidzieć, choć wiele instytucji pragnie blokować Internet, to żadna nie jest gotowa płacić za swoje pomyłki.

Na przykład w funkcjonującej już ustawie hazardowej nie przewiduje się odszkodowań za omyłkowe blokowanie, a droga odwołania od decyzji o zablokowaniu jest opisana powierzchownie i stawia właścicieli stron w niekorzystnej pozycji. Prawo w zakresie blokowania stron hazardowych zdaje się zakładać, że podmiot blokujący jest nieomylny. To błąd.

5. KAŻDA AKCJA RODZI REAKCJĘ – KWESTIA BEZPIECZEŃSTWA

Gdy tylko pojawia się mechanizm blokady, równolegle tworzy się zapotrzebowanie na narzędzia do jego obejścia. Wcale nie dlatego, że ludzie są źli. Po prostu wielu obywateli Rzeczypospolitej Polskiej chciałoby mieć dostęp do tego samego Internetu co mieszkańcy innych krajów.

W przeszłości mówiono, że blokowanie stron może prowadzić to tzw. bałlkanizacji Iinternetu. Każdy kraj może blokować coś innego, więc Internet nigdzie nie będzie taki sam. Użytkownikom się to nie podoba, więc stworzenie narzędzi do obejścia każdego nowego mechanizmu blokady jest kwestią czasu.

Trwająca dyskusja o blokowaniu podnosi popularność narzędzi takich jak VPN – a więc sprawia, że rośnie poziom świadomości i kompetencji użytkowników w zakresie bezpiecznego korzystania z sieci. Niestety istnieje również ryzyko, że część obywateli sięgnie po niesprawdzone narzędzia do omijania blokad, być może podsunięte przez oszustów.

Inna rzecz, że stworzenie infrastruktury blokującej na pewno spotka się z próbami jej zaatakowania. Może to mieć związek z chęcią ominięcia rejestru lub manipulowania nim (np. w celu zablokowania strony konkurencji). Warto zauważyć, że strona Komisji Nadzoru Finansowego była już celem ataku, który mógł zagrozić polskim bankom (sprawa wyszła na jaw w lutym br.). Skoro KNF nie umiała upilnować bezpieczeństwa własnej witryny, to czy będzie miała kompetencje do odpierania ataków na stworzoną przez siebie czarną listę stron?

6. PRYWATNOŚĆ

Już wyżej opisaliśmy, jak niektóre mechanizmy blokowania mogą zagrażać prywatności, np. gdy wiążą się z analizą przesyłanych przekazów. W Polsce obecnie nie rozważa się wprowadzania takich mechanizmów, choć nigdy nie wiemy, jak daleko zajdzie trend leczenia przez blokowanie.

W kontekście prywatności trzeba pamiętać, że polscy politycy dwa razy proponowali, aby wprowadzić cenzurę pornografii na poziomie operatorów. Oznaczałoby to, że osoby pragnące dostępu do Internetu niefiltrowanego musiałyby specjalnie się o to ubiegać. Chociaż mogłyby mieć różne motywacje (np. dziennikarzom z zasady zależy na dostępie do Internetu, w którym nie ma blokad informacyjnych), to jest niemal pewne, że wszyscy tacy klienci (także dziennikarze) otrzymaliby łatkę „pornofilów".

7. KOSZTY PO STRONIE OPERATORÓW

Blokowanie samo się nie zrobi.

Nawet jeśli procedury blokowania są zautomatyzowane, to wcześniej trzeba opracować i wdrożyć odpowiednie automaty, sposoby wymiany informacji między uczestnikami ruchu sieciowego itd. Również przy metodach zautomatyzowanych muszą pracować ludzie. To kosztuje, a koszty rosną wraz z liczbą rejestrów, jakich trzeba pilnować. Zależą również od szczegółowości informacji w rejestrze oraz od intensywności wpisywania do nich podmiotów.

Tu objawia się ten sam problem, z którym mamy do czynienia przy odszkodowaniach. Państwo nie chce kosztów i odpowiedzialności, więc spycha je na przedsiębiorców telekomunikacyjnych, nakazując im tworzenie infrastruktury na własny koszt. Tak naprawdę zapłacimy za to wszyscy – w rachunkach za Internet. A państwo jest gotowe karać przedsiębiorców, jeśli będą blokować zbyt wolno lub nie to, co trzeba.

8. MAŁA SKUTECZNOŚĆ, CZYLI CO DOSTAJEMY W ZAMIAN

Jeśli już zgadzamy się na blokowanie i płacimy za to, powinniśmy zapytać: „Co dostajemy w zamian?". W udzieleniu odpowiedzi pomogą dwa spostrzeżenia:

– Eksperci zgadzają się, że niemożliwe jest opracowanie

blokowania w 100% skutecznego.

– Jest wysoce wątpliwe, czy blokowanie rozwiązuje problemy społeczne, które – zgodnie z deklaracjami – ma rozwiązywać.

Skupmy się na tym drugim punkcie. Czy problem nielegalnego hazardu zniknie, gdy zablokujemy strony internetowe? Czy problem nadużyć finansowych może być wyeliminowany poprzez blokowanie stron? Czy można tak wyeliminować problem terroryzmu?

Odpowiedź na każde z powyższych pytań będzie brzmiała „nie”. W istocie każdy z wymienionych problemów ma swoje źródło poza Internetem. Terroryzm to wynik złożonych zjawisk o podłożu społeczno-polityczno-kulturowym. Nadużycia finansowe pojawiły się na długo przed Internetem, a nielegalny hazard można uprawiać także offline.

Powtórzmy: blokowanie stron jest nieskuteczne zarówno na płaszczyźnie technicznej, jak i społecznej. Nie możemy wszystkiego zablokować, a nawet gdybyśmy to zrobili, to nie wyeliminujemy problemu. Co więcej: blokowanie stron może maskować nieporadność państwa w usuwaniu rzeczywistych problemów.

9. MOŻLIWE NADUŻYCIA

Każda infrastruktura cenzurująca stworzona dzisiaj dla celów „dobrych”, może jutro posłużyć do celów „złych”. Nie chodzi nawet o to, czy obecny rząd użyje blokowania, aby np. uciszać przeciwników politycznych, ale o to, że każdy kolejny rząd będzie mógł to zrobić. Jeśli raz stworzymy mechanizmy cenzury, nigdy nie wiemy, w czyje ręce trafią i jak zostaną wykorzystane.

10. PROBLEM AKSJOLOGICZNY

Celowo zostawiliśmy to na koniec jako kwestię najmniej praktyczną, niemniej ważną. Istnieją pewne narzędzia i sposoby

działania, których demokratyczne państwo prawa nie powinno stosować. Jednym z tych narzędzi jest cenzura prewencyjna. Opiera się ona na założeniu, że obywatel jest z natury przestępcą i władza musi pilnować, by do jego umysłu nie dotarły „złe” treści. Bo to władza wie, kto może ujrzeć daną informację.

To nie jest droga myślenia, którą powinniśmy podążać, tworząc społeczeństwo informacyjne w XXI wieku.

Autorstwo: Marcin Maj
Współpraca: Anna Obem, Katarzyna Szymielewicz
Źródło: Panoptykon.org