Walka z terroryzmem w sieci w rękach firm internetowych?

8 listopada 2018

Prywatyzacja walki z terroryzmem, a jednocześnie wzmocnienie prywatnej cenzury w sieci – do takich skutków mogą prowadzić rozwiązania zaproponowane ostatnio przez Komisję Europejską. A to jeszcze nie wszystko. Przedstawiona w projekcie definicja treści o charakterze terrorystycznym jest tak szeroka, że ofiarą cenzury mogą paść także wypowiedzi, z którymi nie wiąże się żadne realne zagrożenie.

Państwo oddaje kontrolę

Ministerstwo Cyfryzacji zakończyło właśnie konsultacje stanowiska Rzeczpospolitej Polskiej w sprawie przygotowanego przez Komisję projektu rozporządzenia ws. zapobiegania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym. Projekt wprowadza zasady usuwania lub blokowania treści o charakterze terrorystycznym przez dostawców usług hostingowych (czyli np. media społecznościowe, ale także inne portale, które umożliwiają dodawane treści przez użytkowników, choćby w formie komentarzy). Komisja zaproponowała dwie ścieżki eliminowania takich materiałów.

Po pierwsze hostingodawcy mają być zobowiązani do usuwania lub blokowania treści na mocy nakazu wydawanego przez uprawniony organ publiczny. Takie rozwiązanie nie budzi większych wątpliwości, pod warunkiem że blokowanie/usuwanie będzie odbywało się z zachowaniem odpowiednich gwarancji – pod kontrolą sądu (czego projekt niestety wprost nie precyzuje) i zgodnie ze standardami sprawiedliwego procesu (szczęśliwie projekt przewiduje tu procedurę odwoławczą). Bardziej niepokoi natomiast druga, równoległa procedura usuwania lub blokowania treści. Zgodnie z projektem organy państwa powołane do

wykrywania i identyfikacji treści o charakterze terrorystycznym (czyli np. w polskich warunkach Agencja Bezpieczeństwa Wewnętrznego) mogłyby wysłać niewiążące zgłoszenie dotyczące danego materiału do administratora portalu. Administrator następnie sam dokonywałby oceny zgłoszonej treści w oparciu o własny regulamin i ewentualnie decydował o jej zablokowaniu. Potem musiałby poinformować o podjętych działaniach organ zgłaszający. Autor zablokowanej treści mógłby się odwołać od decyzji portalu, ale tylko do jego administratora, na drodze wewnętrznej – nie przewidziano tu żadnego mechanizmu zewnętrznej, niezależnej kontroli.

Taka procedura oznacza, że organ państwa, który „jedynie" sygnalizuje problem administratorowi portalu, nie ponosi żadnej odpowiedzialności za działania podjęte na skutek takiego zgłoszenia. Stawia jednocześnie prywatne firmy w roli arbitrów dozwolonych treści, choć podmioty te mają znacznie mniejsze kompetencje (niż np. ABW) do rzetelnej analizy zgłaszanych materiałów. Z jednej strony jest to więc niebezpieczny przejaw prywatyzacji walki z terroryzmem, która to walka należy do zadań państwa i odpowiedzialność za nią nie powinna być w żadnej mierze delegowana na podmioty prywatne. Z drugiej strony państwo, stosując niewiążący tryb, oddaje kontrolę nad kawałkiem wolności w sieci prywatnym podmiotom, które często działają w sposób nieprzejrzysty, arbitralny, kierując się własnym interesem ekonomicznym i bez odpowiedniego poszanowania praw użytkowników.

Wyobraźmy sobie teraz, że zidentyfikowano w sieci treść o charakterze terrorystycznym. Aby ją usunąć lub zablokować, organy państwa będą mogły zastosować albo obwarowaną gwarancjami i formalnościami twardą procedurę zakończoną wydaniem wiążącego nakazu (obarczoną ryzykiem postępowania odwoławczego), albo wygodniejszą opcję – czyli wysłanie zgłoszenia i przerzucenie decyzji (wraz z odpowiedzialnością) na portal. Którą ścieżkę będą chętniej wybierać?

Terroryzm czy dozwolona krytyka? A może satyra?

W skrajnej sytuacji można sobie wręcz wyobrazić scenariusz, w którym niewiążący tryb, pod pretekstem walki z treściami o charakterze terrorystycznymi, będzie nadużywany przez organy państwa do ograniczania dostępności w Internecie innych niepożądanych materiałów, np. wypowiedzi krytycznych wobec władzy publicznej. Jest to realne ryzyko, biorąc pod uwagę szeroką definicję treści o charakterze terrorystycznym zawartą w projekcie rozporządzenia. Jest nią m.in. „zachęcanie do przyczyniania się do przestępstw terrorystycznych lub propagowanie działalności grupy terrorystycznej, w szczególności poprzez zachęcenie do udziału w grupie terrorystycznej". Definicją treści o charakterze terrorystycznym objęte jest również podżeganie i propagowanie (w tym poprzez gloryfikowanie) przestępstw o charakterze terrorystycznym. Warunkiem zablokowania treści nie jest natomiast to, że jej dalsze rozpowszechnianie może stanowić realne zagrożenie dla bezpieczeństwa.

Tak szeroka definicja, nawet jeśli nie będzie wykorzystywana do celów politycznych, sprzyja nadgorliwemu blokowaniu treści ze szkodą dla interesu publicznego. Niedawno głośno było o nieuzasadnionym blokowaniu w mediach społecznościowych materiałów dokumentujących zbrodnie wojenne i naruszenia praw człowieka w Syrii, które omyłkowo zakwalifikowano jako mające związek z terroryzmem. Rozporządzenie w obecnym kształcie może spowodować wzrost liczby takich przypadków – tym bardziej że projekt przewiduje (w pewnych sytuacjach obowiązkowe) stosowanie tzw. proaktywnych środków kontroli treści przez hostingodawców (czyli np. automatycznych filtrów), które stwarzają szczególne ryzyko nadmiernego blokowania.

Projekt zawiera szereg gwarancji, które mają minimalizować zagrożenia dla praw podstawowych, np. transparentność blokowania treści przez portale czy obowiązek uzasadniania

podejmowanych decyzji i informowania autora treści o jej zablokowaniu. Z naszej perspektywy w tym przypadku kluczowe jest jednak zawężenie definicji treści, które mogą być zablokowane, i rezygnacja z niewiążącego trybu zgłaszania ich portalom do usunięcia. Mamy nadzieję, że polski rząd przychyli się do tego stanowiska w ramach konsultacji z Komisją Europejską.

Autorstwo: Dorota Głowacka
Źródło: Panoptykon.org