Dania oskarżona o rozpowszechnianie fałszywych informacji w celu przeforsowania unijnej ustawy o masowej inwigilacji

W Unii Europejskiej narasta konflikt dotyczący uprawnień w zakresie inwigilacji cyfrowej. Duński minister sprawiedliwości Peter Hummelgaard został oskarżony o wykorzystywanie fałszywych informacji w celu wywarcia presji na niezdecydowane rządy, aby poparły proponowaną przez Komisję Europejską regulację Chat Control 2.0.

W komunikacie prasowym działacz na rzecz praw cyfrowych i były poseł do Parlamentu Europejskiego Patrick Breyer potępił to, co określa jako wywołany kryzys mający na celu przeforsowanie przepisów, które poddałyby całą prywatną komunikację w UE automatycznemu skanowaniu.

Z poufnego protokołu z posiedzenia Rady z 15 września, uzyskanym przez Netzpolitik, wynika, że Hummelgaard, obecnie przewodniczący Rady UE, poinformował ministrów spraw wewnętrznych, że Parlament Europejski zablokuje wszelkie przedłużenia istniejących dobrowolnych ram skanowania, chyba że rządy zgodzą się przyjąć nowe rozporządzenie.

Breyer natychmiast odrzucił to twierdzenie.

„To rażące kłamstwo mające na celu wywołanie kryzysu” – powiedział Breyer.

„Parlament Europejski nie podjął takiej decyzji… Jesteśmy świadkami bezwstydnej kampanii dezinformacyjnej mającej na celu narzucenie 450 milionom Europejczyków bezprecedensowej ustawy o masowym skanowaniu. Wzywam rządy UE, a w szczególności rząd niemiecki, aby nie dały się nabrać na tę rażącą manipulację. Poświęcenie podstawowego prawa do prywatności cyfrowej i bezpiecznego szyfrowania w oparciu o zmyślone informacje byłoby katastrofalną porażką przywództwa politycznego i moralnego”.

Przedmiotowe rozporządzenie, oficjalnie nazwane rozporządzeniem w sprawie wykorzystywania seksualnego dzieci (CSAR), zmusiłoby platformy komunikacyjne, dostawców poczty elektronicznej i usługi przechowywania danych w chmurze do skanowania wszystkich treści użytkowników pod kątem potencjalnych materiałów związanych z wykorzystywaniem dzieci.

Dotyczyłoby to nawet usług wykorzystujących szyfrowanie typu end-to-end, co oznacza, że prywatne rozmowy na platformach takich jak WhatsApp, Signal i iMessage nie byłyby już naprawdę poufne.

Chociaż zwolennicy opisują ten system jako ukierunkowany i ograniczony, ramy prawne pozwalają na szerokie zastosowanie.

Według Breyera i analityków prawnych prawie wszystkie główne usługi komunikacyjne mogłyby zostać zobowiązane do skanowania wiadomości każdego użytkownika.

Krytyce poddano również twierdzenie, że skanowanie byłoby stosowane tylko jako „środek ostateczny”. Progi wydawania takich nakazów są niejasne, a eksperci ds. prywatności twierdzą, że w praktyce dostawcy byliby pod presją, aby wdrożyć skanowanie wszystkich treści.

Sama technologia skanowania jest również bardzo wadliwa, a

odsetek fałszywych alarmów wynosi podobno od 50 do 75 procent.

Niewinne wiadomości, takie jak zdjęcia z rodzinnych wakacji lub prywatne romantyczne wiadomości, mogą zostać nieprawidłowo oznaczone i przekazane organom ścigania.

Jeszcze bardziej niepokojące jest to, że po oznaczeniu przepisy wymagają zgłoszenia nie tylko zidentyfikowanego obrazu lub filmu, ale także całej historii rozmowy.

Cała ta korespondencja byłaby wysyłana do nowej agencji na szczeblu UE i udostępniana organom ścigania, co budzi poważne wątpliwości co do zakresu i nadzoru.

Kolejną kontrowersję wywołał przepis zawarty w projekcie Rady.

Artykuł 7 duńskiego tekstu kompromisowego wyraźnie wyłącza komunikację funkcjonariuszy policji, żołnierzy i agentów wywiadu z zakresu skanowania.

Breyer postrzega to jako rażące przyznanie się do niebezpieczeństw związanych z propozycją. „To cyniczne wyłączenie dowodzi, że doskonale wiedzą, jak niewiarygodne i niebezpieczne są algorytmy szpiegowskie" – powiedział.

„Jeśli komunikacja państwowa zasługuje na poufność, to samo dotyczy komunikacji obywateli, przedsiębiorstw i osób, które korzystają z bezpiecznych kanałów wsparcia i terapii".

Podczas gdy Dania nadal przewodzi wysiłkom zmierzającym do przyjęcia rozporządzenia, w kraju narasta sprzeciw.

Wewnętrzna grupa robocza Rady ma spotkać się 9 października, aby omówić przepisy, a ostateczne głosowanie przewidziane jest na 14 października. Wynik prawdopodobnie będzie zależał od niewielkiej grupy niezdecydowanych krajów, w tym Niemiec i Włoch.

W związku z upływającym czasem obrońcy prywatności wzywają rządy UE, aby nie ulegały presji politycznej opartej na

dezinformacji.

Ostrzegają, że przyjęcie Chat Control 2.0 otworzyłoby drzwi do stałej inwigilacji prywatnej komunikacji i zlikwidowałoby długoletnie zabezpieczenia prywatnego życia cyfrowego w Europie.