Stanowisko Sekcji Bezpieczeństwa Komitetu Informatyki PAN 5.11.2024

w sprawie projektowanych regulacji CSAM

Planowane regulacje powinny brać pod uwagę zarówno realną skuteczność wprowadzanych rozwiązań w kontekście osiągnięcia zakładanych celów jak i skutki uboczne nie związane z realizacją celu podstawowego.

Projektowana regulacja wprowadza obowiązek skanowania treści na urządzeniu użytkownika pod kątem wykrywania treści niepożądanych i blokowaniu ich przesyłania. Mechanizm wykrywania ma być oparty o porównanie hasza treści cyfrowej (zdjęcia, wideo, ...) z haszami obecnymi na czarnej liście treści niedozwolonych.

Zaproponowany mechanizm jest całkowicie nieskuteczny ze względu na możliwość modyfikacji treści cyfrowych tak aby generowany hasz nie wykazywał związku z oryginalnym obrazem a zarazem treść cyfrowa miała te same własności pod względem wizualnym dla ludzkiego oka. Przy obecnym stanie techniki, skonstruowanie takich narzędzi nie stwarza większych trudności, nie wymaga szczególnej wiedzy merytorycznej, zaś algorytmy służące tym celom są publicznie znane.

W przypadku wejścia w życie projektowanej regulacji można spodziewać się pojawienia się aplikacji skutecznie realizującej w/w modyfikacje. Co więcej, mogą one realizować całkowicie legalne cele takie jak ochrona własności intelektualnej poprzez wprowadzanie cyfrowych znaków wodnych i zabezpieczeń steganograficznych.

Osoby i organizacje przesyłające treści niedozwolone, a w szczególności zorganizowana przestępczość, zapewne natychmiast byłyby w stanie dostosować się do sytuacji i wdrożyć stosowanie wyżej wymienionych środków. Ich stosowanie nie wymagałoby od użytkownika właściwie żadnych kompetencji merytorycznych. Z tego względu efekt regulacji w zwalczaniu niepożądanego zjawiska zapewne okazałby się zaniedbywalny.

Jedynym rzeczywistym efektem wprowadzenia obowiązku skanowania byłoby

- spowolnienie działania urządzeń konsumenckich, wyższe zużycie energii i wydatki na dostosowanie software'u do obowiązków wynikających z regulacji,
- zwiększenie podatności urządzeń końcowych na ataki i inwigilację, możliwości te mogłyby być wykorzystane w szczególności przez strony trzecie dla ataków na obywateli i podmioty znajdujące się w UE,
- unijne regulacje stałyby się pretekstem dla wprowadzania analogicznych rozwiązań przez reżimy autorytarne dostarczając efektywnych środków technicznych dla policji politycznej pod hasłem ochrony dzieci.

Z drugiej strony, projektowana regulacja CSAM nie podejmuje tak oczywistych i relatywnie łatwych przedsięwzięć jak stworzenie ekosystemu cyfrowej tożsamości, w którym użytkownik miałby możliwość udowodnienia swego wieku w określonym przedziale w sposób chroniący tożsamość. Mechanizm taki miałby znaczenie praktyczne nie tylko w kontekście tematyki CSAM czy sieci społecznościowych grupujących rówieśników, ale również np. w handlu online dla weryfikacji prawa klienta do zawierania umów kupna-sprzedaży.

Mirosław Kutyłowski, Wiesław Paluszyński, Józef Pieprzyk