Rada
Unii Europejskiej

Bruksela, 24 listopada 2020 r.
(OR. en)

13084/1/20
REV 1

LIMITE

JAI 999
COSI 216
CATS 90
ENFOPOL 314
COPEN 329
DATAPROTECT 131
CYBER 239
IXIM 122

NOTA

Od:	Prezydencja
Do:	Delegacje
Nr poprz. dok.:	12863/20
Dotyczy:	Rezolucja Rady w sprawie szyfrowania – Bezpieczeństwo dzięki szyfrowaniu i bezpieczeństwo pomimo szyfrowania

Delegacje otrzymują w załączeniu rezolucję Rady w sprawie szyfrowania.

ZAŁĄCZNIK

Rezolucja Rady w sprawie szyfrowania
Bezpieczeństwo dzięki szyfrowaniu i bezpieczeństwo pomimo szyfrowania

1. Preambuła: Bezpieczeństwo dzięki szyfrowaniu i bezpieczeństwo pomimo szyfrowania

Unia Europejska w pełni popiera rozwój, wdrażanie i stosowanie silnego szyfrowania. Unia Europejska podkreśla potrzebę zapewnienia pełnego poszanowania praw podstawowych i praw człowieka oraz praworządności we wszystkich działaniach związanych z niniejszą rezolucją, zarówno w internecie, jak i poza nim. Szyfrowanie jest niezbędnym środkiem ochrony praw podstawowych oraz bezpieczeństwa cyfrowego rządów, przemysłu i społeczeństwa. Jednocześnie Unia Europejska musi zadbać o to, by właściwe organy w obszarze bezpieczeństwa i wymiaru sprawiedliwości w sprawach karnych, np. organy ścigania i organy sądowe, mogły wykonywać swoje legalne uprawnienia, zarówno w internecie, jak i poza nim, chroniąc nasze społeczeństwa i naszych obywateli.

Zgodnie z konkluzjami Rady Europejskiej z 1–2 października 2020 (EUCO 13/20) „UE będzie wykorzystywać swoje narzędzia i uprawnienia regulacyjne do kształtowania globalnych przepisów i standardów". Uzgodniono, że środki finansowe w ramach Instrumentu na rzecz Odbudowy i Zwiększania Odporności zostaną wykorzystane na realizację celów takich jak „zwiększenie zdolności UE w zakresie zabezpieczenia się przed zagrożeniami dla cyberbezpieczeństwa, zapewnienia bezpiecznego środowiska łączności, zwłaszcza poprzez kryptografię kwantową, oraz zapewnienia dostępu do danych do celów sądowych i egzekwowania prawa".

2. Obecna sytuacja, jeśli chodzi o stosowanie / zaawansowanie szyfrowania

W dzisiejszym świecie technologia szyfrowania jest coraz częściej wykorzystywana we wszystkich dziedzinach życia publicznego i prywatnego. Służy ona ochronie osób fizycznych, społeczeństwa obywatelskiego, infrastruktury krytycznej, mediów i dziennikarzy, przemysłu i rządów poprzez zapewnienie prywatności, poufności, integralności danych oraz dostępności łączności i danych osobowych: nie ulega wątpliwości, że technologia szyfrowania przynosi korzyści wszystkim. Szyfrowanie zostało uznane przez unijne organy ds. ochrony danych i cyberbezpieczeństwa za ważne narzędzie przyczyniające się na przykład do ochrony danych osobowych, które są przekazywane poza UE, ale są objęte wymogiem zapewnienia zasadniczo równoważnego stopnia ochrony, co zdaniem Trybunału Sprawiedliwości jest jednym z wymogów prawnych w przypadku przekazywania danych[1]. Nie tylko urządzenia i aplikacje elektroniczne są coraz częściej programowane w celu domyślnego szyfrowania przechowywanych danych użytkownika, ale też coraz więcej kanałów komunikacyjnych i usług przechowywania danych jest również zabezpieczanych za pomocą szyfrowania end-to-end (E2E). Znajduje to pozytywne odzwierciedlenie w nasilającej się reakcji ze strony branży komunikacyjnej i aplikacyjnej, w której większość aplikacji do komunikacji natychmiastowej i innych platform internetowych również wdrożyła szyfrowanie end-to-end.

3. Wyzwania związane z zapewnianiem bezpieczeństwa

„Życie cyfrowe” i cyberprzestrzeń stwarzają nie tylko ogromne możliwości, ale również poważne wyzwania: cyfryzacja nowoczesnych społeczeństw wiąże się z pewnymi słabościami i może być wykorzystywana do celów przestępczych. Przestępcy mogą zatem uwzględniać w swoich sposobach działania łatwo dostępne, gotowe do użytku rozwiązania w zakresie szyfrowania zaprojektowane do prawnie uzasadnionych celów[2].

Jednocześnie, aby skutecznie zwalczać terroryzm, przestępczość zorganizowaną, niegodziwe traktowanie dzieci w celach seksualnych (zwłaszcza jego aspekty internetowe), a także cały szereg innych cyberprzestępstw i przestępstw wykorzystujących cyberprzestrzeń, organy ścigania muszą w coraz większym stopniu polegać na dostępie do dowodów elektronicznych. Dla właściwych organów dostęp do dowodów elektronicznych może mieć zasadnicze znaczenie, nie tylko po to, by mogły skutecznie prowadzić postępowania przygotowawcze, a tym samym stawiać przestępców przed wymiarem sprawiedliwości, ale także po to, by mogły chronić ofiary i przyczyniać się do zapewniania bezpieczeństwa.

---

[1] Wyrok z dnia 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commissioner przeciwko Facebook Ireland Ltd i Maximillianowi Schremsowi, ECLI:EU:C:2020:559:

[2] iOCTA 2020, s. 25

Istnieją jednak przypadki, w których szyfrowanie sprawia, że dostęp do komunikatów i analizowanie ich treści w ramach dostępu do dowodów elektronicznych są niezwykle trudne lub praktycznie niemożliwe, mimo że dostęp do takich danych byłby zgodny z prawem. Niezależnie od otoczenia technologicznego w danym okresie kluczowe jest zatem, aby zachować uprawnienia właściwych organów w obszarze bezpieczeństwa i wymiaru sprawiedliwości w sprawach karnych opierające się na zgodnym z prawem dostępie do wykonywania ich zadań, zgodnie z tym, co przewidują i dopuszczają przepisy. Takie przepisy przewidujące uprawnienia w zakresie egzekwowania muszą zawsze w pełni respektować należyte procedury i inne zabezpieczenia, a także prawa podstawowe, w szczególności prawo do poszanowania życia prywatnego i komunikowania się oraz prawo do ochrony danych osobowych.

4. Wypracowanie właściwej równowagi

Należy w pełni przestrzegać zasady bezpieczeństwa dzięki szyfrowaniu i bezpieczeństwa pomimo szyfrowania. Unia Europejska nadal popiera silne szyfrowanie. Szyfrowanie jest jedną z podstaw zaufania do cyfryzacji i do ochrony praw podstawowych i powinno być promowane i rozwijane.

Ochrona prywatności i bezpieczeństwa łączności poprzez szyfrowanie, a jednocześnie dalsze zapewnienie właściwym organom w obszarze bezpieczeństwa i wymiaru sprawiedliwości w sprawach karnych możliwości legalnego dostępu do odpowiednich danych w uzasadnionych, jasno określonych celach w walce z poważną lub zorganizowaną przestępczością i terroryzmem, w tym w świecie cyfrowym, oraz podtrzymanie praworządności, są niezwykle ważne. Wszelkie podejmowane działania muszą starannie wyważyć te interesy względem zasad konieczności, proporcjonalności i pomocniczości.

5. Połączenie sił z sektorem technologicznym

Podejmując kolejne kroki, Unia Europejska dąży do nawiązania aktywnej dyskusji z sektorem technologicznym, angażując jednocześnie środowiska naukowe i akademickie, aby zapewnić dalsze wdrażanie i stosowanie silnej technologii szyfrowania. Właściwe organy muszą mieć możliwość dostępu do danych w sposób zgodny z prawem i ukierunkowany, w pełnym poszanowaniu praw podstawowych i odpowiednich przepisów o ochronie danych, przy jednoczesnym utrzymaniu cyberbezpieczeństwa. Rozwiązania techniczne umożliwiające uzyskanie dostępu do zaszyfrowanych danych muszą być zgodne z zasadami legalności, przejrzystości, konieczności i proporcjonalności, w tym z ochroną danych osobowych w fazie projektowania i ochroną domyślną.

Ponieważ nie istnieje jeden sposób osiągnięcia wyznaczonych celów, rządy, przemysł, środowiska naukowe i akademickie muszą współpracować w sposób przejrzysty, aby strategicznie osiągnąć tę równowagę.

6. Ramy regulacyjne

Można by jeszcze bardziej szczegółowo przeanalizować potrzebę opracowania ogólnounijnych ram regulacyjnych, które umożliwiałyby właściwym organom skuteczne wykonywanie ich zadań operacyjnych przy jednoczesnej ochronie prywatności, praw podstawowych i bezpieczeństwa łączności.

Potencjalne rozwiązania techniczne będą musiały umożliwiać organom korzystanie z ich uprawnień do przeprowadzania dochodzenia, które na mocy ich przepisów krajowych podlegają zasadzie proporcjonalności i konieczności oraz nadzorowi sądowemu, przy jednoczesnym poszanowaniu wspólnych europejskich wartości, podtrzymaniu praw podstawowych oraz zachowaniu korzyści z szyfrowania. Możliwe rozwiązania należy opracować w sposób przejrzysty we współpracy z krajowymi i międzynarodowymi dostawcami usług łączności oraz z innymi odpowiednimi zainteresowanymi stronami. Takie rozwiązania i normy techniczne – oraz, w perspektywie ogólnej, szybki rozwój technologii – wymagałyby również ciągłego doskonalenia wśród właściwych organów umiejętności technicznych i operacyjnych oraz wiedzy fachowej, aby wykonując swoją pracę, organy te mogły skutecznie sprostać wyzwaniom związanym z cyfryzacją na skalę globalną.

7. Innowacyjne zdolności dochodzeniowe

Ponadto ogromne znaczenie ma poprawa koordynacji na szczeblu UE, która ma na celu:

1) połączenie wysiłków wszystkich państw członkowskich oraz instytucji i organów UE;

2) zdefiniowanie i ustanowienie innowacyjnych sposobów podejścia z myślą o nowych technologiach;

3) analizowanie odpowiednich rozwiązań technicznych i operacyjnych; oraz

4) zapewnienie dostosowanych do indywidualnych potrzeb szkoleń wysokiej jakości.

Rozwiązania techniczne i operacyjne zakorzenione w ramach regulacyjnych opartych na zasadach legalności, konieczności i proporcjonalności należy opracowywać w ścisłym porozumieniu z usługodawcami, innymi odpowiednimi zainteresowanymi stronami i wszystkimi odpowiednimi właściwymi organami, przy czym nie powinno istnieć wyłącznie jedno zalecane rozwiązanie techniczne zapewniające dostęp do zaszyfrowanych danych.