

Bruksela, 3 października 2025 r.
(OR. en)

13029/25

COPEN 272
CYBER 252
ENFOPOL 330
JAI 1275
DATAPROTECT 222
COSI 163
IXIM 199
CATS 46
FREMP 241
TELECOM 310
CT 117

NOTA

Od:	Sekretariat Generalny Rady
Do:	Komitety Stałych Przedstawicieli / Rada
Dotyczy:	Dostęp do danych do celów skutecznych postępowań przygotowawczych – Aktualna sytuacja

Zapewnienie uprawnionego dostępu do danych na temat łączności elektronicznej do celów egzekwowania prawa i prowadzenia postępowań przygotowawczych stanowi dla Rady priorytet i jest szczególnie konieczne w kontekście walki z poważną i zorganizowaną przestępczością oraz terroryzmem.

W następstwie prac grupy wysokiego szczebla ds. dostępu do danych do celów skutecznego egzekwowania prawa (zwanej dalej „grupą wysokiego szczebla”), która w maju 2024 r. wydała zalecenia¹, a w listopadzie 2024 r. – sprawozdanie końcowe², oraz konkluzji Rady z 12 grudnia 2024 r. w sprawie dostępu do danych do celów skutecznego egzekwowania prawa³ z 24 czerwca 2025 r. Komisja przedstawiła Plan działania na rzecz zgodnego z prawem i skutecznego dostępu organów ścigania do danych⁴ (zwany dalej „planem działania”). W konkluzjach z 26 czerwca 2025 r. Rada Europejska zwróciła się do instytucji UE i państw członkowskich, by podjęły dalsze działania w celu wzmocnienia współpracy organów ścigania i organów wymiaru sprawiedliwości, w tym w zakresie skutecznego dostępu do danych na potrzeby egzekwowania prawa⁵.

W szczególności prezydencja chciałaby zwrócić uwagę ministrów sprawiedliwości na następujące kwestie: (1) zatrzymywanie danych, (2) uprawnione przechwytywanie komunikacji oraz (3) szyfrowanie będące wyzwaniem horyzontalnym.

1. Zatrzymywanie danych

„Zatrzymywanie danych” dotyczy spoczywającego na dostawcach usług obowiązku zatrzymywania danych niedotyczących treści (informacji o abonentach, adresów IP, metadanych o ruchu i lokalizacji) przez pewien okres, tak aby możliwe było ich udostępnianie organom ścigania do celów postępowań przygotowawczych.

Zatrzymywaniu danych poświęcony jest jeden z trzech rozdziałów sprawozdania końcowego przygotowanego przez grupę wysokiego szczebla. W sprawozdaniu za kluczowe kwestie uznano m.in. obecną fragmentację przepisów krajowych i dodatkowe wyzwania związane z dostawcami usług OTT (*‘over-the-top’ services*), w tym z powszechnie używanymi komunikatorami w telefonach komórkowych. Według grupy wysokiego szczebla odpowiedzią na te problemy może być ustanowienie zharmonizowanych minimalnych zasad zatrzymywania i dostępu. Grupa opowiada się także za zacieśnieniem współpracy między dostawcami usług a praktykami.

¹ Dok. 11281/24.

² Dok. 15941/2/24 REV2.

³ Dok. 16448/24.

⁴ Dok. 10806/25.

⁵ EUCO 12/25.

W planie działania Komisja zapowiedziała, że przygotowuje ocenę skutków z myślą o zaktualizowaniu, w stosownych przypadkach, unijnych przepisów dotyczących zatrzymywania danych. Ocenę tę rozpoczęto w maju 2025 r., a jej zakończenie przewidywane jest na pierwszy kwartał 2026 r. Komisja wezwała także Europol i Eurojust do dalszych prac nad usprawnieniem współpracy z dostawcami usług łączności i do opracowania wraz z nimi katalogu danych, które dostawcy przetwarzają do celów biznesowych.

W Radzie na posiedzeniu 19 maja 2025 r. Grupa Robocza ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (COPEN) zajęła się kwestią zatrzymywania danych, a przede wszystkim ewentualnego przyszłego unijnego wniosku ustawodawczego w tej sprawie. Na drugim posiedzeniu, które odbyło się 25 września 2025 r., grupa COPEN omówiła odpowiednie treści i kryteria dotyczące tego aktu, także w świetle wymogów określonych w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej. Celem obu posiedzeń była wymiana poglądów i wniesienie wkładu w bieżące prace Komisji.

Zależnie od wyniku oceny skutków, którą prowadzi Komisja, jednym z kluczowych kroków w 2026 r. może być, zdaniem prezydencji, rozpoczęcie dyskusji na temat wniosku ustawodawczego dotyczącego unijnych przepisów o zatrzymywaniu danych.

2. Uprawnione przechwytywanie komunikacji

Uprawnione przechwytywanie pozwala organom uzyskiwać w sposób niejawnny dostęp do komunikacji w czasie rzeczywistym⁶.

W sprawozdaniu końcowym grupa wysokiego szczebla odnotowała: „Chociaż legalne przechwytywanie tradycyjnej telekomunikacji pozostaje podstawowym narzędziem w wielu postępowaniach przygotowawczych, skuteczność tego środka drastycznie spadła, ponieważ usługi telekomunikacyjne są obecnie świadczone głównie przez inne podmioty: według różnych źródeł około 97% wszystkich wiadomości mobilnych jest obecnie przesyłanych za pośrednictwem komunikatorów, takich jak WhatsApp, Facebook Messenger i WeChat, podczas gdy tradycyjne wiadomości SMS i MMS stanowią jedynie około 3% wiadomości”.

⁶ Obejmuje to także dostęp do komunikacji z niewielkim opóźnieniem, jak wyjaśniono w sprawozdaniu końcowym grupy wysokiego szczebla.

Grupa wysokiego szczebla wydała szereg zaleceń; m.in. postuluje, by wnioski o uprawnione przechwytywanie stały się możliwe do wyegzekwowania w odniesieniu do wszystkich rodzajów dostawców usług łączności elektronicznej. Zalecenia grupy dotyczą m.in. doprecyzowania definicji i zakresu uprawnionego przechwytywania; wskazania niezbędnych zabezpieczeń, doprecyzowania pojęcia właściwości miejscowej w odniesieniu do danych; zbadania, jak europejski nakaz dochodzeniowy mógłby zwiększać skuteczność transgranicznych wniosków w sprawie uprawnionego przechwytywania; a także wspierania opracowywania umów dwustronnych z państwami trzecimi w sprawie dostępu do danych w czasie rzeczywistym. W dłuższym terminie eksperci zalecają, na podstawie dalszej analizy i oceny skutków, opracowanie unijnego instrumentu dotyczącego uprawnionego przechwytywania (składającego się z prawa miękkiego lub wiążących instrumentów prawnych) do celów egzekwowania prawa, który nałożyłby możliwe do wyegzekwowania obowiązki na działających w UE dostawców usług łączności elektronicznej.

W planie działania Komisja zapowiada, że zaproponuje środki w celu poprawy skuteczności transgranicznych wniosków, wzmacniając istniejące instrumenty, takie jak europejski nakaz dochodzeniowy (do 2027 r.), a także że przeanalizuje środki umożliwiające stworzenie równych warunków działania dla wszystkich rodzajów dostawców usług łączności, określając najskuteczniejsze podejście do problemu niechęci dostawców usług łączności do współpracy.

Podczas prezydencji duńskiej państwa członkowskie zostaną poproszone o przedstawienie swoich praktyk i obecnych ograniczeń w zakresie wdrażania środków transgranicznego uprawnionego przechwytywania, w szczególności w kontekście europejskiego nakazu dochodzeniowego oraz porozumień dwustronnych i wielostronnych.

3. Szyfrowanie jako kwestia horyzontalna

Należy także zwrócić uwagę na wyzwanie, jakie w kontekście dostępu do danych do celów skutecznych postępowań przygotowawczych stanowi szyfrowanie; wiąże się to również ze wspomnianymi wyżej kwestiami zatrzymywania danych i uprawnionego przechwytywania. Liczne usługi wykorzystują teraz pełne szyfrowanie, aby chronić poufność komunikacji i prywatność i ze względów dotyczących cyberbezpieczeństwa – z tego powodu uzyskiwanie przez organy ścigania uprawnionego dostępu do nadających się do odczytu danych komunikacyjnych może być skrajnie trudne.

W planie działania Komisja zapowiedziała, że w 2026 r. przedstawi szczegółowy plan działania w zakresie technologii dotyczący szyfrowania w celu wskazania i oceny rozwiązań, które umożliwią uprawniony dostęp do zaszyfrowanych danych, a zarazem zapewnią cyberbezpieczeństwo i ochronę praw podstawowych. Aby osiągnąć ten cel, Komisja tworzy grupę ekspertów, która ma zacząć pracę jesienią 2025 r.

Komisja będzie także wspierać badanie i rozwój nowych zdolności w zakresie deszyfrowania, aby wyposażyć Europol w zdolności nowej generacji w zakresie deszyfrowania (od 2030 r.).

Dalsze działania i koordynacja

Kwestia dostępu do danych do celów skutecznych postępowań przygotowawczych jest złożona i wymaga podejścia multidyscyplinarnego. Chcąc zapewnić efektywność przyszłych prac oraz uwzględnienie wszystkich aspektów, prezydencja duńska za konieczne uznaje zaangażowanie różnych organów przygotowawczych Rady, w tym organów odpowiedzialnych za bezpieczeństwo wewnętrzne i współpracę organów ścigania, współpracę w sprawach karnych i cyberbezpieczeństwo. W konkluzjach z 12 grudnia 2024 r. Rada zleciła Stałemu Komitetowi Współpracy Operacyjnej w zakresie Bezpieczeństwa Wewnętrznego (COSI), by we współpracy z Komitetem Koordynacyjnym w dziedzinie Współpracy Policyjnej i Wymiaru Sprawiedliwości w Sprawach Karnych (CATS) koordynował, omawiał i monitorował realizację planu działania. Prezydencja duńska przygotowała szczegółowy przegląd planowanych działań dotyczących dostępu do danych do celów skutecznego egzekwowania prawa, zawierający podział zadań i harmonogram; COSI przeanalizował ten dokument 18 września 2025 r.⁷

Prezydencja duńska uważa za bardzo ważne stałe dbanie o to, by ministrowie spraw wewnętrznych i ministrowie sprawiedliwości ściśle monitorowali sytuację w zakresie dostępu do danych do celów skutecznego egzekwowania prawa, z myślą o zapewnieniu organom ścigania niezbędnych narzędzi do skutecznego ścigania przestępstw przy pełnym poszanowaniu praw podstawowych. W tym celu pod koniec swojej kadencji prezydencja zamierza przygotować notę informacyjną dla Rady na temat działań przeprowadzonych w ramach poszczególnych struktur Rady.

⁷ Dok. 12381/25.