Dostęp do danych na rzecz skutecznego egzekwowania przepisów

Posted on 2024-11-29

Jak można wykorzystywać dostęp do danych elektronicznych do celów egzekwowania prawa i wymiaru sprawiedliwości w sprawach karnych? W debacie na ten temat eksperci od ochrony danych wielokrotnie ostrzegali przed przyznawaniem organom ścigania nadmiernych uprawnień. Mogłoby to być równoznaczne z masowym nadzorem i powodować poważną ingerencję w prawa podstawowe. Dotyczy to w szczególności zasad i okresu przechowywania danych, a także odpowiedniego zabezpieczenia danych i ich szyfrowania.

Musimy zapewnić równowagę między prawami osób a interesami organów ścigania, które poszukują sprawców przestępstw, zwłaszcza tych popełnionych w internecie. Niedawno wskazał to Trybunał Sprawiedliwości UE[1]. Proponowane środki powinny być zgodne z zasadami ochrony danych i prywatności, a dostęp do danych powinien być przyznawany wyłącznie w kontekście postępowań karnych, indywidualnie rozpatrywany, i zasadniczo podlegać zezwoleniu sądowemu.

Przechowywanie danych

Przechowywanie danych było przedmiotem licznych debat w Unii Europejskiej. Pokazują one złożoność tematu i trudności w znalezieniu właściwej równowagi między potrzebą ochrony osób przed nowoczesnymi formami nadzoru elektronicznego. Z drugiej strony wskazują na konieczność wykorzystania technologii w dochodzeniach karnych. Zakres podmiotowy i przedmiotowy wszelkich przyszłych unijnych ram prawnych dotyczących zatrzymywania danych osobowych i dostępu do nich jest jednym z kluczowych elementów oceny niezbędności i proporcjonalności. W tym względzie TSUE stwierdził już, że uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu jest co do zasady zakazane i może być uzasadnione wyłącznie ochroną bezpieczeństwa narodowego, jeżeli dane państwo członkowskie stoi w obliczu poważnego jego zagrożenia, które jest rzeczywiste i aktualne lub przewidywane[2].

Szeroki i ogólny obowiązek zatrzymywania danych w formie elektronicznej przez podmioty zajmujące się przetwarzaniem danych (tj. wszelkiego rodzaju dostawców usług, którzy mogliby zapewnić dostęp do wszelkich dowodów elektronicznych) rozszerzyłby zakres zatrzymywania danych poza bariery ustanowione w orzecznictwie. Byłby zatem wysoce problematyczny. Niedawny wyrok TSUE w sprawie Hadopi wskazuje[3], że w pewnych okolicznościach ogólne zatrzymywanie adresów IP przypisanych do źródła połączenia internetowego, a także danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej może być zgodne z prawem.

Trybunał wyjaśnił, że uogólnione i niezróżnicowane przechowywanie adresów IP nie stanowi poważnej ingerencji w prawa podstawowe. Może być więc dopuszczalne na mocy prawa Unii w celu zwalczania wszelkiego rodzaju czynów zabronionych. Jednakże jest to ściśle ograniczone. Obejmuje przypadki, gdy wykluczone jest, by przechowywanie danych mogło prowadzić do poważnych ingerencji w życie prywatne danej osoby ze względu na możliwość

wyciągnięcia precyzyjnych wniosków na jej temat. W związku z tym każde połączenie tych adresów IP z innymi przechowywanymi danymi, które pozwalałoby na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego osób, których dane byłyby w ten sposób przechowywane, musi zostać zakazane. Zatrzymywanie adresów IP w sposób ogólny i niezróżnicowany nie może w żaden sposób zostać automatycznie rozszerzone na inne (bardziej wrażliwe) dane o ruchu i lokalizacji, które mogłyby z łatwością umożliwić stworzenie bardziej szczegółowego profilu użytkownika.

Bezpieczeństwo danych i szyfrowanie

Szyfrowanie ma zasadnicze znaczenie dla zapewnienia bezpieczeństwa i poufności danych osobowych i komunikacji elektronicznej. Zapewnia silne techniczne zabezpieczenia przed dostępem do tych informacji przez inne osoby niż użytkownik i wybrani przez niego odbiorcy, w tym dostawcy. W szczególności, w kontekście komunikacji interpersonalnej, prawdziwe szyfrowanie typu end-to-end („E2EE”) obejmujące urządzenia końcowe i zawarte w nich dane, z kluczami deszyfrującymi posiadanymi wyłącznie przez użytkowników, jest podstawowym narzędziem zapewniającym poufność komunikacji elektronicznej. Uniemożliwienie korzystania z szyfrowania lub osłabienie skuteczności zapewnianej przez nie ochrony miałoby poważny wpływ na poszanowanie życia prywatnego i poufności użytkowników, na ich wolność wypowiedzi, a także na innowacje i rozwój gospodarki cyfrowej, która opiera się na wysokim poziomie zaufania i pewności, jakie gwarantują takie technologie.

Dostawcy mogą stanąć przed techniczną koniecznością zastosowania środków osłabiających szyfrowanie w sposób masowy wobec wszystkich użytkowników, aby móc zrealizować prawny nakaz przechwycenia lub dostępu, nawet w przypadkach, gdy pierwotny nakaz

przechwycenia lub dostępu był ograniczony do konkretnej osoby lub konkretnej grupy osób. Takie masowe osłabienie szyfrowania – czy to poprzez środki wymagane od dostawców, czy poprzez osłabienie technicznych standardów szyfrowania – może prowadzić do wysokiego ryzyka naruszenia praw podstawowych osób fizycznych w UE, w szczególności w kontekście łączności elektronicznej. W tym względzie Europejski Trybunał Praw Człowieka stwierdził, że „obowiązek odszyfrowywania zaszyfrowanych komunikatów typu end-to-end może sprowadzać się do wymogu, aby dostawcy takich usług osłabili mechanizm szyfrowania dla wszystkich użytkowników; w związku z tym nie jest on proporcjonalny do zamierzonych uzasadnionych celów". Zasadniczo każdy wymóg techniczny dla dostawców, który może potencjalnie wpływać na podstawowe prawa i wolności osób fizycznych, powinien być ustanowiony przez prawo, które szanuje istotę podstawowych praw i wolności oraz jest uważane za niezbędne i proporcjonalne w demokratycznym społeczeństwie.

Opracowano na podstawie Stanowiska EROD nr 5/2024 w sprawie zaleceń grupy wysokiego szczebla ds. dostępu do danych w celu skutecznego egzekwowania prawa[4]

1. Wyrok Trybunału Sprawiedliwości z dnia 30 kwietnia 2024 r., La Quadrature du Net i in., sprawa C-470/21, ECLI:EU:C:2024:370, pkt 116 i 117 oraz z dnia 4 października 2024 r., Bezirkshauptmannschaft Landeck, C- 548/21, ECLI:EU:C:2024:830, pkt 97 ↩
2. Wyrok Trybunału Sprawiedliwości z dnia 6 października 2020 r., La Quadrature du Net i in., sprawy połączone C-511/18, C-512/18 i C-520/18, ECLI:EU:C:2020:791, pkt 137. ↩
3. Wyrok Trybunału Sprawiedliwości z dnia 30 kwietnia 2024 r., La Quadrature du Net i in., sprawa C-470/21, ECLI:EU:C:2024:370. ↩
4. https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf ↩