TRYBUNAŁ SPRAWIEDLIWOŚCI
UNII EUROPEJSKIEJ

1952 – 2022

KOMUNIKAT PRASOWY nr 156/22
Luksemburg, 20 września 2022 r.

Wyrok Trybunału w sprawach połączonych C-793/19 | SpaceNet i C-794/19 | Telekom Deutschland

Trybunał Sprawiedliwości potwierdził, że unijne prawo sprzeciwia się uogólnionemu i niezróżnicowanemu zatrzymywaniu danych o ruchu i danych dotyczących lokalizacji, z wyjątkiem przypadków poważnego zagrożenia dla bezpieczeństwa narodowego

Państwa członkowskie mogą jednak, w celu walki z poważną przestępczością i w ścisłym poszanowaniu zasady proporcjonalności, przewidzieć w szczególności ukierunkowane czy też szybkie zatrzymywanie takich danych, jak również uogólnione i niezróżnicowane zatrzymywanie adresów IP

SpaceNet i Telekom Deutschland świadczą w Niemczech publicznie dostępne usługi dostępu do Internetu, zaś Telekom Deutschland świadczy ponadto usługi telefoniczne. Spółki te zakwestionowały przed sądami niemieckimi nałożony na nich w niemieckiej ustawie Prawo telekomunikacyjne (TKG) obowiązek zatrzymywania, począwszy od dnia 1 lipca 2017 r., związanych z telekomunikacją danych o ruchu i danych o lokalizacji ich klientów.

Poza kilkoma wyjątkami, TKG nakłada na dostawców publicznie dostępnych usług łączności elektronicznej, w szczególności w celu ścigania poważnych przestępstw lub zapobiegania konkretnemu zagrożeniu dla bezpieczeństwa narodowego, obowiązek uogólnionego i niezróżnicowanego zatrzymywania na okres kilku tygodni istotnych danych o ruchu i danych dotyczących lokalizacji użytkowników końcowych tych usług.

Niemiecki federalny sąd administracyjny dąży do ustalenia, czy prawo Unii, w wykładni przyjętej przez Trybunał Sprawiedliwości[1], stoi na przeszkodzie takim przepisom krajowym.

Jego wątpliwości powstały w szczególności na gruncie tego, że przewidziany w TKG obowiązek zatrzymywania dotyczył mniejszej liczby danych i krótszego (4 lub 10 tygodniowego) okresu przechowywania niż przewidywały to przepisy krajowe rozpatrywane w sprawach, w których wydano wcześniejsze wyroki. Te charakterystyczne cechy tego obowiązku zmniejszają prawdopodobieństwo tego, że zatrzymywane dane mogłyby umożliwić sformułowanie bardzo dokładnych wniosków dotyczących życia prywatnego osób, których dane zostały zatrzymane. Ponadto TKG zapewnia skuteczną ochronę zatrzymywanych danych przed prawdopodobieństwem popełnienia nadużyć i uzyskania nielegalnego dostępu.

W wydanym dziś wyroku Trybunał potwierdził swe wcześniejsze orzecznictwo.

Udzielił on niemieckiemu federalnemu sądowi administracyjnemu odpowiedzi, że **sprzeczne z prawem Unii są krajowe środki ustawodawcze przewidujące, do celów zwalczania poważnej przestępczości i zapobiegania**

[1] Zobacz w szczególności wyroki z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20 (zobacz również komunikat prasowy nr 58/22), a także z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18 (zobacz również komunikat prasowy nr 123/20).

poważnym zagrożeniom dla bezpieczeństwa *publicznego*, prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych dotyczących lokalizacji.

Prawo unijne nie sprzeciwia się natomiast przepisom krajowym

– umożliwiającym, w celu ochrony bezpieczeństwa *narodowego*, nakazanie dostawcom usług łączności elektronicznej **uogólnionego i niezróżnicowanego zatrzymywania** danych o ruchu i danych dotyczących lokalizacji, **w sytuacjach, gdy dane państwo członkowskie napotyka poważne zagrożenie dla bezpieczeństwa *narodowego*,** które okazuje się rzeczywiste i aktualne lub możliwe do przewidzenia. Taki nakaz może podlegać kontroli sądu lub niezależnego organu administracyjnego i może zostać wydany jedynie na określony czas, ograniczony do tego, co ściśle niezbędne, jednak z możliwością przedłużenia w przypadku utrzymywania się tego zagrożenia;

– przewidującym, w celu ochrony bezpieczeństwa narodowego, zwalczania *poważnej* przestępczości i zapobiegania *poważnym* zagrożeniom dla bezpieczeństwa publicznego, **ukierunkowane zatrzymywanie** danych o ruchu i danych dotyczących lokalizacji, którego granice zostają wyznaczone na podstawie obiektywnych i niedyskryminacyjnych przesłanek w zależności od kręgu osób, których dane dotyczą, lub kryterium geograficznego; dane te są zatrzymywane na okres ograniczony do tego, co ściśle niezbędne, ale odnawialny;

– przewidującym, w tym samym celu, **uogólnione i niezróżnicowane zatrzymywanie adresów IP** przypisanych do źródła połączenia na określony czas ograniczony do tego, co ściśle konieczne;

– przewidującym, w celu ochrony bezpieczeństwa narodowego, zwalczania przestępczości i ochrony bezpieczeństwa publicznego, **uogólnione i niezróżnicowane zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników** środków łączności elektronicznej; oraz

– umożliwiającym, w celu zwalczania *poważnej* przestępczości oraz, a fortiori, ochrony bezpieczeństwa narodowego, nakazanie dostawcom usług łączności elektronicznej **szybkiego zatrzymywania** przez określony czas danych o ruchu i danych dotyczących lokalizacji, którymi dysponują ci dostawcy usług.

Takie przepisy winny ponadto, poprzez jasne i precyzyjne uregulowania, zapewniać, by odnośne zatrzymywanie danych było uzależnione od spełnienia związanych z nim materialnych i proceduralnych przesłanek oraz by osoby, których dane dotyczą, dysponowały skutecznymi gwarancjami chroniącymi przed ryzykiem nadużyć.

W zakresie dotyczącym TKG Trybunał stwierdził, iż z postanowienia odsyłającego wynika, że określony w tej ustawie obowiązek zatrzymywania obejmuje w szczególności dane niezbędne do ustalenia źródła oraz odbiorcy połączenia, daty i godziny jego rozpoczęcia i zakończenia lub – w przypadku komunikacji za pomocą SMS, wiadomości multimedialnej lub podobnej – moment wysłania i otrzymania wiadomości, a także datę i godzinę rozpoczęcia i zakończenia połączenia, lub – w przypadku komunikacji za pomocą telefonii mobilnej – oznaczenie komórek, które zostały wykorzystane przez numer wywołujący i wywołany na początku połączenia.

W ramach świadczenia usług dostępu do Internetu obowiązek zatrzymywania obejmuje między innymi przypisany abonentowi adres IP, datę i godzinę rozpoczęcia i zakończenia korzystania z Internetu z przypisanego adresu IP oraz, – w przypadku korzystania z Internetu mobilnego – oznaczenie komórki wykorzystanej na początku połączenia internetowego. Zatrzymywane są również dane wskazujące na położenie geograficzne i kierunki wiązki głównej anten radiowych obsługujących daną komórkę.

Choć prawdą jest, że dane dotyczące usług poczty elektronicznej nie są objęte przewidzianym w TKG obowiązkiem zatrzymywania, to stanowią jedynie niewielką część rozpatrywanych danych. Ponadto w szczególności zaś zatrzymywane są dane użytkowników objętych tajemnicą zawodową, takich jak adwokaci, lekarze i dziennikarze.

Tak więc **przewidziany w TKG obowiązek zatrzymywania obejmuje bardzo duży zbiór danych o ruchu i danych dotyczących lokalizacji, który to zbiór odpowiada w istocie tym danym, w przedmiocie których wydano ww.**

wcześniejsze wyroki.

Ten całościowy zbiór danych o ruchu lub danych dotyczących lokalizacji, zatrzymywanych, odpowiednio, na dziesięć tygodni i na cztery tygodnie, **może zaś dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, których dane są zatrzymywane, takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazyjnie pokonywane trasy, podejmowane czynności, relacje społeczne i środowiska społeczne, w których osoby te się obracają i, w szczególności, pozwolić na sporządzenie na ich podstawie profilu tych osób.**

Jeśli chodzi o przewidziane w TKG gwarancje mające na celu ochronę zatrzymywanych danych przed prawdopodobieństwem zaistnienia nadużyć i przed udzieleniem jakiegokolwiek bezprawnego dostępu do nich, Trybunał wskazał, że zatrzymywanie tych danych i dostęp do nich stanowią odrębne ingerencje w prawa podstawowe osób, których te dane dotyczą; co za tym idzie, wymagają one odrębnego uzasadnienia. Wynika z tego, że przepisy krajowe zapewniające pełne poszanowanie warunków wynikających z orzecznictwa w dziedzinie dostępu do zatrzymywanych danych nie mogą jako takie ani ograniczyć, ani zaradzić poważnej ingerencji, która wynikałaby z uogólnionego zatrzymywania tych danych.

UWAGA: Odesłanie prejudycjalne pozwala sądom państw członkowskich, w ramach rozpatrywanego przez nie sporu, zwrócić się do Trybunału z pytaniem o wykładnię prawa Unii lub o ocenę ważności aktu Unii. Trybunał nie rozpoznaje sporu krajowego. Do sądu krajowego należy rozstrzygnięcie sprawy zgodnie z orzeczeniem Trybunału. Orzeczenie to wiąże w ten sam sposób inne sądy krajowe, które spotkają się z podobnym problemem.

Pełny tekst i streszczenie wyroku jest publikowany na stronie internetowej CURIA w dniu ogłoszenia.

Osoba odpowiedzialna za kontakty z mediami: Jarosław Zasada ✆ (+352) 4303 2793

Nagranie wideo z ogłoszenia wyroku jest dostępne przez „Europe by Satellite” ✆ (+32) 22964106.