Sprawa C-140/20

Streszczenie wniosku o wydanie orzeczenia w trybie prejudycjalnym zgodnie z art. 98 § 1 regulaminu postępowania przed Trybunałem Sprawiedliwości

Data wpływu:

25 marca 2020 r.

Oznaczenie sądu odsyłającego:

Supreme Court (Irlandia)

Data wydania postanowienia o wystąpieniu z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym:

25 marca 2020 r.

Strona powodowa:

G.D.

Strona pozwana:

The Commissioner of the Garda Síochána

Minister for Communications, Energy and Natural Resources

Attorney General

Przedmiot postępowania głównego

Niniejsze postępowanie dotyczy systemu prawnego ustanowionego w Irlandii na mocy Communications (Retention of Data) Act 2011 [ustawy z 2011 r. o łączności (zatrzymywanie danych)], regulującej zatrzymywanie metadanych telekomunikacyjnych i uzyskiwanie do nich dostępu przez krajowe organy Irlandii, w szczególności przez policję irlandzką (zwaną dalej „An Garda Síochána”) w ramach wykrywania, dochodzenia i ścigania poważnych przestępstw.

Przedmiot i podstawa prawna wniosku o wydanie orzeczenia w trybie prejudycjalnym

Czy Communications (Retention of Data) Act 2011 [ustawa z 2011 r. o łączności (zatrzymywanie danych)], w szczególności jej art. 6 ust. 1, jest niezgodna z art. 15 ust. 1 dyrektywy 2002/58/WE?

Pytania prejudycjalne

1) Czy ogólny lub powszechny system zatrzymywania danych – nawet poddany rygorystycznym ograniczeniom w zakresie zatrzymywania i dostępu – jest sam w sobie sprzeczny z art. 15 dyrektywy 2002/58/WE, interpretowanym w świetle karty?

2) Czy przy badaniu ewentualnej niezgodności środka krajowego wprowadzonego na podstawie dyrektywy 2006/24/WE, wprowadzającego ogólny system zatrzymywania danych (z zastrzeżeniem niezbędnych rygorystycznych kontroli w zakresie zatrzymywania danych lub uzyskiwania do nich dostępu), w szczególności przy ocenie proporcjonalności takiego systemu, sąd krajowy może uwzględnić okoliczność, że dane mogą być zgodnie z prawem zatrzymywane przez usługodawców do własnych celów handlowych oraz że ich zatrzymanie może być wymagane ze względów bezpieczeństwa narodowego wyłączonych z przepisów dyrektywy 2002/58/WE?

3) Dokonując oceny, w kontekście stwierdzenia zgodności z prawem Unii, w szczególności z kartą, krajowego środka dostępu do zatrzymanych danych, jakimi kryteriami powinien kierować się sąd krajowy, badając, czy tego rodzaju system dostępu przewiduje uprzednią i niezależną kontrolę wymaganą przez Trybunał Sprawiedliwości w jego orzecznictwie? Czy w tym kontekście sąd krajowy może, przy dokonywaniu takiej oceny, wziąć pod uwagę istnienie kontroli sądowej ex post lub niezależnej kontroli?

4) W każdym razie, czy sąd krajowy jest zobowiązany do stwierdzenia niezgodności środka krajowego z art. 15 dyrektywy 2002/58/WE, jeżeli środek krajowy przewiduje ogólny system zatrzymywania danych na potrzeby zwalczania poważnych przestępstw, a sąd krajowy uznał – na podstawie wszystkich dostępnych dowodów – że takie zatrzymywanie jest zarazem istotne i ściśle niezbędne do realizacji celu polegającego na zwalczaniu poważnej przestępczości?

5) Jeżeli sąd krajowy jest zobowiązany uznać, że środek krajowy jest niezgodny z art. 15 dyrektywy 2002/58/WE, interpretowanym w świetle karty, to czy jest on uprawniony do ograniczenia w czasie skutków takiego uznania, jeśli jest przekonany o tym, że przyjęcie odmiennego podejścia doprowadziłoby do „chaosu i uszczerbku dla interesu ogółu” [zgodnie ze stanowiskiem przyjętym na przykład w sprawie R (National Council for Civil Liberties) przeciwko Secretary

of State for Home Department i Secretary of State for Foreign Affairs [2018] EWHC 975, pkt 46]?

(6) Czy sąd krajowy, do którego zwrócono się o stwierdzenie niezgodności prawa krajowego z art. 15 dyrektywy 2002/58/WE lub o odstąpienie od jego stosowania, lub o stwierdzenie, że stosowanie takiego prawa skutkowało naruszeniem praw jednostki, czy to w ramach postępowania wszczętego w celu ułatwienia polemiki w przedmiocie dopuszczalności dowodów w ramach postępowania karnego, czy w innym celu, może odmówić zastosowania takiego rozwiązania w odniesieniu do danych zatrzymanych na mocy przepisu krajowego ustanowionego na podstawie wynikającego z art. 288 TFUE obowiązku skutecznego wprowadzenia do prawa krajowego przepisów dyrektywy lub ograniczenia takiego stwierdzenia do okresu następującego po stwierdzeniu nieważności dyrektywy 2006/24/WE przez Trybunał Sprawiedliwości Unii Europejskiej w dniu 8 kwietnia 2014 r.?

Powołane przepisy prawa Unii

Traktat o Unii Europejskiej, art. 5 ust. 4 i art. 6 ust. 1 oraz protokół nr 21.

Karta praw podstawowych Unii Europejskiej, art. 7 i 8 oraz art. 52 ust. 1.

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. 1995, L 281, s. 31).

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. 2002, L 201, s. 37).

Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz.U. 2006, L 105, s. 54).

Wyrok z dnia 10 lutego 2009 r., Irlandia/Parlament i Rada, C-301/06, EU:C:2009:68.

Wyrok z dnia 26 listopada 2009 r., Komisja/Irlandia, C-202/09, EU:C:2009:736.

Wyrok z dnia 8 kwietnia 2014 r., Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in., sprawy połączone C-293/12 i C-594/12, EU:C:2014:238.

Wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige AB/Post- och telestyrelsen i Secretary of State for the Home Department/Tom Watson i in., sprawy połączone C-203/15 i C-698/15, EU:C:2016:970.

Powołane przepisy prawa krajowego

Communications (Retention of Data) Act 2011 [ustawa z 2011 r. o łączności (zatrzymywanie danych)] (zwana dalej „ustawą z 2011 r.”)

Ustawa z 2011 r. została przyjęta w jednoznacznym celu wdrożenia dyrektywy z 2006 r. Artykuł 3 ustawy nakłada na wszystkich usługodawców obowiązek zatrzymywania „danych dotyczących telefonii stacjonarnej i telefonii ruchomej” przez okres dwóch lat. Są to dane pozwalające ustalić źródło, odbiorcę, datę i godzinę rozpoczęcia oraz zakończenia połączenia, rodzaj danego połączenia oraz rodzaj i położenie geograficzne wykorzystanych urządzeń komunikacyjnych. Treść połączeń nie należy do tego rodzaju danych.

Dostęp do zatrzymanych danych oraz ich ujawnienie odbywa się na podstawie wniosku o ujawnienie danych. Artykuł 6 ustawy z 2011 r. określa warunki złożenia wniosku o ujawnienie danych, zaś ust. 1 tego artykułu stanowi, że członek An Garda Síochána, który ma co najmniej stopień nadinspektora, może złożyć wniosek o ujawnienie danych, jeżeli stwierdzi on, że dane te są wymagane między innymi do zapobiegania poważnym przestępstwom, a także do ich wykrywania, dochodzenia i ścigania. Termin „poważne przestępstwo” oznacza przestępstwo zagrożone karą co najmniej 5 lat pozbawienia wolności, a także inne przestępstwa wymienione w załączniku nr 1 do ustawy.

Mechanizmy nadzoru przewidziane w ustawie z 2011 r. obejmują postępowanie zażaleniowe określone w art. 10 tej ustawy oraz zadania „wyznaczonego sędziego”, o których mowa w art. 12, który to sędzia jest odpowiedzialny za sprawowanie kontroli nad stosowaniem przepisów tej ustawy.

Na szczeblu wewnętrznym szef An Garda Síochána, komisarz Gardy, zdecydował, że wnioski o ujawnienie danych telefonicznych złożone na podstawie ustawy z 2011 r. powinny być kierowane w sposób scentralizowany do jednego nadinspektora. Za politykę ujawniania danych odpowiedzialny jest nadinspektor policji, który był również szefem wydziału ds. bezpieczeństwa i wywiadu w strukturach An Garda Síochána, i to on ostatecznie decyduje o skierowaniu do podmiotów świadczących usługi komunikacyjne wniosku o ujawnienie danych na podstawie przepisów ustawy z 2011 r. Utworzono niewielką niezależną jednostkę o nazwie Telecommunications Liaison Unit (jednostka ds. koordynacji telekomunikacyjnej, zwana dalej „TLU”), której zadaniem jest wspieranie nadinspektora policji w sprawowaniu jego funkcji i działanie jako jedyny punkt kontaktowy z usługodawcami.

W okresie mającym znaczenie dla postępowania wyjaśniającego będącego przedmiotem niniejszej sprawy wszystkie wnioski o ujawnienie danych podlegały

zatwierdzeniu w pierwszej instancji przez inspektora (lub przez działającego w tym charakterze komisarza), a następnie były przesyłane w celu ich dalszej realizacji przez TLU. Osoby prowadzące postępowanie wyjaśniające miały obowiązek zawrzeć we wniosku informacje na tyle szczegółowe, by umożliwić wydanie decyzji ze znajomością sprawy i mieć na uwadze, że nadinspektor może być zobowiązany do uzasadnienia decyzji w późniejszym postępowaniu sądowym lub przed wyznaczonym sędzią High Court. TLU i nadinspektor policji zobowiązani są do zbadania zgodności z prawem, proporcjonalności i zasadności wniosków o ujawnienie danych składanych przez członków An Garda Síochána. Wnioski uznane za niespełniające wymogów określonych w przepisach prawa lub w protokołach wewnętrznych Gardy podlegały zwrotowi w celu uzyskania wyjaśnień lub dodatkowych informacji. Na mocy protokołu ustaleń przyjętego w maju 2011 r. usługodawcy nie realizują wniosków o przekazanie danych dotyczących połączeń, które nie zostały objęte przedmiotową procedurą. TLU podlega również kontroli ze strony komisarza ds. ochrony danych.

Zwięzłe przedstawienie stanu faktycznego i przebiegu postępowania głównego

1 W marcu 2015 r. ława przysięgłych skazała powoda (zwanego dalej „G.D.”) na karę dożywotniego pozbawienia wolności za zabójstwo O’H. Przez cały czas zaprzeczał on, jakoby był winny. Wyrok skazujący jest przedmiotem wniesionej przez G.D. apelacji, która jest obecnie rozpoznawana przez Court of Appeal (sąd apelacyjny, Irlandia). W toku postępowania G.D. bezskutecznie kwestionował dopuszczalność niektórych dowodów oskarżenia opartych na zatrzymanych danych telefonicznych.

2 Równolegle G.D. wszczął postępowanie cywilne, które jest obecnie w toku, dążąc do zakwestionowania niektórych przepisów ustawy z 2011 r., które stanowiły podstawę zatrzymania przedmiotowych metadanych telefonicznych i uzyskania do nich dostępu. Domaga się on stwierdzenia nieważności odpowiedniego przepisu ustawowego, podnosząc w apelacji zarzut, że w dotyczącym go postępowaniu sąd powinien był odmówić dopuszczenia dowodu w postaci danych telefonicznych, a tym samym że wydany wobec niego wyrok skazujący jest obarczony wadami. Pozwani (zwani dalej „państwem”) domagają się utrzymania spornych przepisów w mocy.

3 Orzeczeniem z dnia 6 grudnia 2018 r., w sprawie Dwyer przeciwko Commissioner of An Garda Síochána i in. [2018] IEHC 685, High Court uwzględnił żądanie G.D. dotyczące stwierdzenia niezgodności art. 6 ust. 1 lit. a) ustawy z 2011 r. z art. 15 ust. 1 dyrektywy 2002/58/WE w związku z art. 7 i 8 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej.

4 Państwo zaskarżyło to orzeczenie do Supreme Court (sąd najwyższy, Irlandia), który wystąpił z niniejszym wnioskiem o wydanie orzeczenia w trybie prejudycjalnym.

5 Supreme Court wskazał, iż ma świadomość tego, że na wykrycie niektórych kategorii poważnych przestępstw oraz na ich ściganie coraz większy wpływ mają dowody takie jak te przedstawione w postępowaniu karnym prowadzonym przeciwko G.D. Z doświadczenia Supreme Court wynika, że rozstrzygnięcie niektórych tego rodzaju spraw możliwe było wyłącznie ze względu na dostępność danych takich jak te, których dotyczy niniejsze postępowanie.

6 Supreme Court stwierdził, że tego rodzaju sprawy często wiążą się z poważnymi przestępstwami popełnianymi przeciwko kobietom, dzieciom i innym osobom wymagającym szczególnego traktowania oraz że wykrycie lub ściganie sprawcy bez dowodów, takich jak będące przedmiotem niniejszej sprawy, byłoby niemożliwe. Jak bowiem zauważył Supreme Court, podobnie jak w sprawie G.D., sama telefonia jest wykorzystywana do nawiązania kontaktu z osobą małoletnią dla celów seksualnych (*grooming*) lub do wykorzystywania w inny sposób osób wymagających szczególnego traktowania.

7 Supreme Court podkreśla, że niemożliwe jest uzyskanie dostępu do tego, co nie stanowiło przedmiotu zatrzymania. Niedopuszczalność powszechnego zatrzymywania metadanych, mimo rygorystycznego charakteru systemu dostępu do nich, prowadziłaby do braku możliwości wykrycia lub skutecznego ścigania wielu ze wspomianych poważnych przestępstw.

8 Supreme Court dokonał następujących ustaleń faktycznych:

(i) alternatywne formy zatrzymywania danych, na podstawie położenia geograficznego lub w inny sposób, byłyby nieskuteczne dla osiągnięcia celów polegających na zapobieganiu co najmniej niektórym rodzajom poważnych przestępstw oraz ich dochodzeniu, wykrywaniu i ściganiu, a także mogłyby prowadzić do potencjalnego naruszenia innych praw jednostki;

(ii) cel zatrzymywania danych w sposób mniej restrykcyjny niż w ramach ogólnego systemu zatrzymywania danych, z zastrzeżeniem zastosowania niezbędnych zabezpieczeń, jest niemożliwy do zrealizowania; oraz

(iii) w braku ogólnego systemu zatrzymywania danych cele polegające na zapobieganiu poważnym przestępstwom oraz ich dochodzeniu, wykrywaniu i ściganiu zostałyby znacznie podważone.

Istotne argumenty stron w postępowaniu głównym

9 Powód twierdzi, że art. 6 ust. 1 lit. a) ustawy z 2011 r., który stanowił podstawę zatrzymania metadanych telefonicznych, uzyskania do nich dostępu i dopuszczenia jako dowodu w prowadzonym przeciwko niemu postępowaniu karnym jest nieważny, bowiem jest niezgodny z art. 15 ust. 1 dyrektywy 2002/58/WE.

10 Twierdzi on, że powszechne zatrzymywanie danych jest niedopuszczalne niezależnie od zabezpieczeń stosowanych w zakresie dostępu do takich danych. Ponadto podnosi on, że system dostępu przewiduje niewystarczającą niezależną ochronę przed niewłaściwym dostępem do danych. Twierdzi on, że zabezpieczenia przewidziane w ustawie z 2011 r. są minimalne i że przepisy te nie przewidują jasnych i precyzyjnych zasad wskazujących, w jakich okolicznościach i na jakich warunkach usługodawcy muszą udzielić organom krajowym dostępu do danych, jak wymaga tego Trybunał Sprawiedliwości Unii Europejskiej. W szczególności obecny system samocertyfikacji wniosków o ujawnienie danych wprowadzony przez An Garda Síochána uważany jest za niespełniający wymogu, by wnioski o udzielenie dostępu były poddane uprzedniej kontroli sądu lub niezależnego organu administracyjnego, zgodnie z pkt 120 wyroku Tele2 Sverige.

11 [Państwo] podnos[i], że sporne przepisy są ważne. Podnoszą oni, że należało przyjąć ogólne podejście w celu ustalenia, czy system prawny chronił prawa do poszanowania życia prywatnego w sposób proporcjonalny.

12 [Państwo] twierdz[i], że w ustawie z 2011 r. ustanowiono szczegółowe ramy regulujące dostęp do zatrzymanych danych. Ponadto państwo podnosi, że TLU, zachowując niezależność funkcjonalną względem An Garda Síochána przy wykonywaniu swoich obowiązków, spełnia wymóg „niezależnego organu administracyjnego”, który przeprowadza kontrolę ex ante wniosków o udzielenie dostępu, i że system ten dodatkowo obwarowany jest nadzorem sądowym, który sprawuje wyznaczony sędzia, przewidzianym postępowaniem zażaleniowym i kontrolą sądową.

13 [Państwo] podnos[i] ponadto, że jeżeli ustawa z 2011 r. zostanie ostatecznie uznana za niezgodną z prawem Unii, to rozstrzygnięcie w tym zakresie wydane przez tutejszy sąd powinno wywoływać skutki jedynie na przyszłość. Twierdz[i] on[o], że stanowisko to jest trafne w wyjątkowych okolicznościach niniejszej sprawy, w której w dniu dostępu do danych będących przedmiotem sporu w postępowaniu głównym pod koniec 2013 r. państwo było zobowiązane, na podstawie prawa Unii, do wdrożenia przepisów dyrektywy z 2006 r. i do utrzymania systemu zatrzymywania danych takiego jak system przewidziany w ustawie z 2011 r. Ponadto państwo podnosi, że jest to właściwe w okolicznościach, w których stwierdzenie niezgodności bez żadnego ograniczenia jego wpływu miałoby poważne konsekwencje dla dochodzenia i ścigania poważnych przestępstw w Irlandii w stosunku do osób, wobec których przeprowadzono postępowanie karne i które uznano za winne, jak również w odniesieniu do prowadzonych postępowań przygotowawczych i karnych.

Zwięzłe uzasadnienie wniosku o wydanie orzeczenia w trybie prejudycjalnym

14 W drodze niniejszego wniosku o wydanie orzeczenia w trybie prejudycjalnym zwrócono się o uzyskanie wyjaśnienia w zakresie wymogów prawa Unii dotyczących zatrzymywania danych na potrzeby zwalczania poważnej

przestępczości, a także niezbędnych zabezpieczeń, które muszą określać ramy dostępu do tych danych, z uwzględnieniem kompetencji państwa członkowskiego w sprawach karnych. Sąd odsyłający zwraca się również o wyjaśnienie w przedmiocie zakresu i skutków w czasie ewentualnego orzeczenia deklaratoryjnego, które mogłoby zostać wydane w okolicznościach niniejszej sprawy.

15 Supreme Court wskazuje, że ustawa z 2011 r. przewidywała zatrzymywanie wszystkich objętych jej zakresem metadanych, co – jak się wydaje – było wówczas wymogiem wynikającym z prawa Unii. Jeżeli jednak, jak twierdzi G.D., powszechne zatrzymywanie danych jest samo w sobie niedozwolone, to ustawa z 2011 r. jest niezgodna z prawem Unii. Jeżeli natomiast, jak twierdzi państwo, właściwe jest przyjęcie szerszego podejścia, wówczas należałoby zbadać cele systemu w ujęciu całościowym, warunki, w jakich dostęp jest dopuszczalny, oraz ustalić, czy ustawa z 2011 r. stanowi proporcjonalną ingerencję w zagwarantowane w prawie Unii i w karcie prawa do prywatności.

16 Supreme Court przyznaje, że kwestia dopuszczalności dowodów w toku postępowania karnego podlega prawu krajowemu. Niemniej jednak kwestia ważności niektórych części ustawy z 2011 r. może zostać podniesiona w ramach postępowania cywilnego. Ponadto sama kwestia dopuszczalności dowodów powinna zostać poddana ocenie w świetle (ewentualnego) stwierdzenia nieważności oraz jego dokładnego charakteru, rozmiaru, zasadności, zakresu i skutków w czasie.

17 Z powyższych względów sąd ten uznaje za konieczne zwrócenie się do Trybunału Sprawiedliwości Unii Europejskiej z powyższymi pytaniami.