Zbiór Orzeczeń

WYROK TRYBUNAŁU (pierwsza izba)

z dnia 7 września 2023 r.*

Odesłanie prejudycjalne – Telekomunikacja – Przetwarzanie danych osobowych w sektorze łączności elektronicznej – Dyrektywa 2002/58/WE – Zakres stosowania – Artykuł 15 ust. 1 – Dane zatrzymywane przez dostawców usług łączności elektronicznej i udostępniane organom odpowiedzialnym za postępowania karne – Późniejsze wykorzystanie tych danych w trakcie dochodzenia w sprawie przewinienia dyscyplinarnego

W sprawie C-162/22

mającej za przedmiot wniosek o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożony przez Lietuvos vyriausiasis administracinis teismas (najwyższy sąd administracyjny Litwy) postanowieniem z dnia 24 lutego 2022 r., które wpłynęło do Trybunału w dniu 3 marca 2022 r., w postępowaniu wszczętym z inicjatywy

A.G.

przy udziale:

Lietuvos Respublikos generalinė prokuratūra,

TRYBUNAŁ (pierwsza izba),

w składzie: A. Arabadjiev, prezes izby, P.G. Xuereb (sprawozdawca), T. von Danwitz, A. Kumin i I. Ziemele, sędziowie,

rzecznik generalny: M. Campos Sánchez-Bordona,

sekretarz: A. Lamote, administratorka,

uwzględniając pisemny etap postępowania i po przeprowadzeniu rozprawy w dniu 2 lutego 2023 r.,

rozważywszy uwagi, które przedstawili:

– w imieniu A.G. – G. Danėlius, advokatas,

– w imieniu rządu litewskiego – S. Grigonis, V. Kazlauskaitė-Švenčionienė i V. Vasiliauskienė, w charakterze pełnomocników,

* Język postępowania: litewski.

– w imieniu rządu czeskiego – O. Serdula, M. Smolek i J. Vláčil, w charakterze pełnomocników,

– w imieniu rządu estońskiego – M. Kriisa, w charakterze pełnomocnika,

– w imieniu Irlandii – M. Browne, A. Joyce i M. Tierney, w charakterze pełnomocników, których wspierał D. Fennelly, BL,

– w imieniu rządu francuskiego – R. Bénard, w charakterze pełnomocnika,

– w imieniu rządu włoskiego – G. Palmieri, w charakterze pełnomocnika, którą wspierał A. Grumetto, avvocato dello Stato,

– w imieniu rządu węgierskiego – Zs. Biró-Tóth i M.Z. Fehér, w charakterze pełnomocników,

– w imieniu Komisji Europejskiej – S.L. Kalėda, H. Kranenborg, P.-J. Loewenthal i F. Wilman, w charakterze pełnomocników,

po zapoznaniu się z opinią rzecznika generalnego na posiedzeniu w dniu 30 marca 2023 r.,

wydaje następujący

Wyrok

1 Wniosek o wydanie orzeczenia w trybie prejudycjalnym dotyczy wykładni art. 15 ust. 1 dyrektywy Parlamentu Europejskiego i Rady 2002/58/WE z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywy o prywatności i łączności elektronicznej) (Dz.U. 2002, L 201, s. 37), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. (Dz.U. 2009, L 337, s. 11) (zwanej dalej „dyrektywą 2002/58”).

2 Wniosek ten został złożony w ramach postępowania wszczętego z inicjatywy A.G. w przedmiocie zgodności z prawem decyzji Lietuvos Respublikos generalinė prokuratūra (prokuratury generalnej Republiki Litewskiej) (zwanej dalej „prokuraturą generalną”) odwołującej go z urzędu prokuratora.

Ramy prawne

Prawo Unii

3 Artykuł 1 dyrektywy 2002/58, zatytułowany „Zakres i cel”, stanowi:

„1. Niniejsza dyrektywa przewiduje harmonizację przepisów krajowych wymaganych do zapewnienia równoważnego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do prywatności i poufności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej oraz w celu zapewnienia swobodnego przepływu we Wspólnocie tego typu danych oraz urządzeń i usług łączności elektronicznej.

[…]

3. Niniejsza dyrektywa nie ma zastosowania do działalności, która wykracza poza zakres Traktatu ustanawiającego Wspólnotę Europejską, takiej jak działalność określona w tytułach V i VI Traktatu o Unii Europejskiej, ani, w żadnym wypadku do działalności dotyczącej bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając dobrobyt gospodarczy państwa, gdy działalność odnosi się do spraw bezpieczeństwa państwa) i działalności państwa w dziedzinie prawa karnego".

4 Artykuł 5 tej dyrektywy, zatytułowany „Poufność komunikacji", w ust. 1 stanowi:

„Państwa członkowskie zapewniają, poprzez ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. W szczególności zakazują słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników, z wyjątkiem upoważnienia zgodnego z art. 15 ust. 1. Niniejszy ustęp nie zabrania technicznego przechowywania, które jest niezbędne do przekazania komunikatu bez uszczerbku dla zasady poufności".

5 Artykuł 15 wspomnianej dyrektywy, zatytułowany „Stosowanie niektórych przepisów dyrektywy 95/46/WE", w ust. 1 stanowi:

„Państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4 i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (i.e. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania [ścigania] przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy 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)]. W tym celu państwa członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie [zatrzymywanie] danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 [TUE]".

Prawo litewskie

Ustawa o łączności elektronicznej

6 Artykuł 65 ust. 2 Lietuvos Respublikos elektroninių ryšių įstatymas (ustawy Republiki Litewskiej o łączności elektronicznej) z dnia 15 kwietnia 2004 r. (Žin. 2004, nr 69-2382), w brzmieniu mającym zastosowanie do okoliczności faktycznych w postępowaniu głównym (zwanej dalej „ustawą o łączności elektronicznej"), zobowiązuje dostawców usług łączności elektronicznej do zatrzymywania danych, o których mowa w załączniku 1 do tej ustawy, oraz, w razie potrzeby, do ich udostępnienia właściwym organom, aby organy te mogły je wykorzystać dla celów zwalczania poważnej przestępczości.

7 Zgodnie z załącznikiem 1 do ustawy o łączności elektronicznej zatrzymywane mają być następujące kategorie danych:

„1. Dane niezbędne do określenia źródła komunikatu: […] 2. Dane niezbędne do określenia przeznaczenia komunikatu: […] 3. Dane dotyczące daty, godziny i czasu trwania komunikatu: […] 4. Dane niezbędne do określenia rodzaju komunikatu: […] 5. Dane niezbędne do określenia urządzenia komunikacyjnego użytkowników lub tego, jakie może być ich urządzenie: […] 6. Danie niezbędne do identyfikacji lokalizacji urządzenia komunikacji ruchomej: […]".

8 Zgodnie z art. 77 ust. 4 tejże ustawy, jeżeli istnieje uzasadnione orzeczenie sądowe lub inna podstawa prawna przewidziana ustawą, dostawcy usług łączności elektronicznej muszą zapewnić, w szczególności organom wywiadu kryminalnego i organom prowadzącym postępowanie przygotowawcze, zgodnie z zasadami przewidzianymi w Lietuvos Respublikos baudžiamojo proceso kodeksas (kodeksie postępowania karnego Republiki Litewskiej, zwanym dalej „kodeksem postępowania karnego"), techniczną możliwość kontroli treści informacji przekazywanych za pośrednictwem sieci łączności elektronicznej.

Ustawa o wywiadzie kryminalnym

9 Artykuł 6 ust. 3 pkt 1 Lietuvos Respublikos kriminalinės žvalgybos Įstatymas (ustawy Republiki Litewskiej o wywiadzie kryminalnym) z dnia 2 października 2012 r. (Žin. 2012, nr 122-6093), w brzmieniu mającym zastosowanie do okoliczności faktycznych w postępowaniu głównym (zwanej dalej „ustawą o wywiadzie kryminalnym"), stanowi, że jeżeli spełnione są określone w tej ustawie przesłanki uzasadniające przeprowadzenie działania wywiadu kryminalnego oraz na podstawie zezwolenia prokuratora lub sądu, organom wywiadu kryminalnego przysługuje, oprócz uprawnień wymienionych w ust. 1 i 2 tego artykułu, uprawnienie do uzyskiwania informacji od dostawców usług łączności elektronicznej.

10 Artykuł 8 ust. 1 wspomnianej ustawy przewiduje, że organy wywiadu kryminalnego przeprowadzają dochodzenie, w przypadku gdy – w szczególności – dostępne są informacje o przygotowywaniu lub popełnieniu bardzo poważnego, poważnego lub stosunkowo poważnego przestępstwa lub o osobach, które przygotowują, popełniają lub popełniły takie przestępstwo. Artykuł 8 ust. 3 tejże ustawy uściśla, że jeżeli takie dochodzenie ujawni istnienie przesłanek wskazujących na popełnienie przestępstwa, niezwłocznie wszczyna się karne postępowanie przygotowawcze.

11 Zgodnie z art. 19 ust. 1 pkt 5 ustawy o wywiadzie kryminalnym informacje uzyskane w wyniku działań wywiadu kryminalnego mogą zostać wykorzystane w przypadkach określonych w ust. 3 i 4 tego artykułu oraz w innych przypadkach przewidzianych ustawą. Zgodnie z art. 19 ust. 3 tejże ustawy pochodzące z działań wywiadu kryminalnego informacje dotyczące czynu noszącego znamiona przestępstwa związanego z korupcją mogą zostać odtajnione za zgodą prokuratury i wykorzystane w ramach dochodzenia dotyczącego przewinień służbowych lub dyscyplinarnych.

Kodeks postępowania karnego

12 Artykuł 154 kodeksu postępowania karnego stanowi, że w oparciu o decyzję sędziego śledczego wydaną na wniosek prokuratora osoba prowadząca postępowanie może słuchać rozmów prowadzonych za pośrednictwem sieci łączności elektronicznej, zlecać ich zapisywanie, kontrolować inne informacje przekazywane za pośrednictwem sieci łączności elektronicznej,

nagrywać je i zatrzymywać, jeżeli istnieją w szczególności podstawy do przypuszczenia, że umożliwi to uzyskanie danych dotyczących bardzo poważnego lub poważnego przestępstwa, które jest przygotowywane lub popełniane, lub które zostało popełnione, lub dotyczących stosunkowo poważnego przestępstwa lub przestępstwa mniejszej wagi.

13 Artykuł 177 ust. 1 tego kodeksu stanowi, że dane uzyskane w wyniku postępowania przygotowawczego są poufne i do czasu rozpoznania sprawy przez sąd mogą zostać ujawnione jedynie za zgodą prokuratury i tylko w uzasadnionym zakresie.

14 Do celów wykonania art. 177 owego kodeksu zastosowanie mają Ikiteisminio tyrimo duomenų teikimo ir panaudojimo ne Baudžiamojo persekiojimo tikslais ir ikiteisminio tyrimo duomenų apsaugos rekomendacijos (zalecenia dotyczące przekazywania i wykorzystywania danych pochodzących z postępowania przygotowawczego w celach innych niż ściganie oraz ochrony tych danych), zatwierdzone dekretem nr I-279 prokuratora generalnego z dnia 17 sierpnia 2017 r. (TAR, 2017, nr 2017-13413), ostatnio zmienione dekretem nr I-211 z dnia 25 czerwca 2018 r.

15 Punkt 23 tych zaleceń stanowi, że po otrzymaniu wniosku o dostęp do danych pochodzących z postępowania przygotowawczego prokurator podejmuje decyzję, czy dostarczyć te dane. W przypadku podjęcia decyzji o ich dostarczeniu prokurator określa, w jakim zakresie można dostarczyć dane, których dotyczy wniosek.

Postępowanie główne i pytanie prejudycjalne

16 Prokuratura generalna wszczęła dochodzenie administracyjne przeciwko skarżącemu w postępowaniu głównym, zajmującemu wówczas stanowisko prokuratora w litewskiej prokuraturze, ponieważ istniały przesłanki wskazujące na to, że w ramach prowadzonego przez siebie postępowania dostarczył on w sposób niezgodny z prawem informacje istotne dla tego postępowania podejrzanemu i jego adwokatowi.

17 W sprawozdaniu z tego dochodzenia komisja prokuratury generalnej stwierdziła, że skarżący w postępowaniu głównym rzeczywiście dopuścił się przewinienia dyscyplinarnego.

18 Zgodnie z tym sprawozdaniem owo przewinienie dyscyplinarne zostało wykazane za pomocą dowodów zebranych w dochodzeniu administracyjnym. W szczególności informacje uzyskane podczas działań wywiadu kryminalnego oraz dane zebrane w toku dwóch karnych postępowań przygotowawczych potwierdziły istnienie rozmów telefonicznych między skarżącym w postępowaniu głównym a adwokatem podejrzanego w postępowaniu przygotowawczym dotyczącego tego podejrzanego, które prowadził skarżący w postępowaniu głównym. Ze wspomnianego sprawozdania wynika ponadto, że postanowieniem sądowym dopuszczone zostało przechwytywanie i nagrywanie treści informacji przekazywanych poprzez sieci łączności elektronicznej, dotyczących danego adwokata, i że innym postanowieniem sądowym dopuszczony został ten sam środek w odniesieniu do skarżącego w postępowaniu głównym.

19 Na podstawie tegoż sprawozdania prokuratura generalna wydała dwa dekrety, w których, po pierwsze, nałożyła na skarżącego w postępowaniu głównym karę polegającą na odwołaniu go ze stanowiska, a po drugie, odwołała go ze stanowiska.

20 Skarżący w postępowaniu głównym wniósł do Vilniaus apygardos administracinis teismas (sądu administracyjnego pierwszej instancji w Wilnie, Litwa) skargę o stwierdzenie, w szczególności, nieważności tych dwóch dekretów.

21 Wyrokiem z dnia 16 lipca 2021 r. sąd ów oddalił skargę skarżącego w postępowaniu głównym, w szczególności na tej podstawie, że działania wywiadu kryminalnego przeprowadzone w niniejszym przypadku były zgodne z prawem i że informacje zebrane zgodnie z przepisami ustawy o wywiadzie kryminalnym zostały wykorzystane zgodnie z prawem, aby ocenić, czy zaistniało przewinienie dyscyplinarne popełnione ewentualnie przez skarżącego w postępowaniu głównym.

22 Skarżący w postępowaniu głównym odwołał się do Lietuvos vyriausiasis administracinis teismas (najwyższego sądu administracyjnego Litwy), będącego sądem odsyłającym, podnosząc, że dostęp organów wywiadu, w ramach działań wywiadu kryminalnego, do danych o ruchu i do samej treści komunikatów elektronicznych, stanowił naruszenie praw podstawowych na tyle poważne, że ze względu na przepisy dyrektywy 2002/58 i Kartę praw podstawowych Unii Europejskiej (zwanej dalej „kartą") dostęp ten mógł zostać przyznany jedynie dla celów zwalczania poważnych przestępstw. Tymczasem art. 19 ust. 3 ustawy o wywiadzie kryminalnym stanowi, że takie dane mogą być wykorzystywane przy badaniu nie tylko poważnych przestępstw, lecz również przewinień służbowych lub dyscyplinarnych związanych z aktami korupcji.

23 Zdaniem sądu odsyłającego kwestie podniesione przez skarżącego w postępowaniu głównym dotyczą dwóch elementów, mianowicie z jednej strony dostępu do danych zatrzymywanych przez dostawców usług łączności elektronicznej w celach innych niż zwalczanie poważnych przestępstw i zapobieganie poważnym zagrożeniom dla bezpieczeństwa publicznego, a z drugiej strony, po uzyskaniu tego dostępu, wykorzystania tych danych do badania przewinień dyscyplinarnych związanych z korupcją.

24 Sąd ów przypomina, że z orzecznictwa Trybunału, w szczególności z wyroku z dnia 6 października 2020 r., Privacy International (C-623/17, EU:C:2020:790, pkt 39), wynika, po pierwsze, że art. 15 ust. 1 w związku z art. 3 dyrektywy 2002/58 należy interpretować w ten sposób, iż do zakresu stosowania tej dyrektywy należy nie tylko środek ustawodawczy, który nakłada na dostawców usług łączności elektronicznej obowiązek zatrzymywania danych o ruchu i danych dotyczących lokalizacji, lecz również środek ustawodawczy zobowiązujący ich do udzielenia właściwym organom krajowym dostępu do tych danych. Po drugie, zdaniem sądu odsyłającego z orzecznictwa tego, w szczególności z wyroku z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej) (C-746/18, EU:C:2021:152, pkt 33, 35), wynika, że jeśli chodzi o cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu przestępstw, to zgodnie z zasadą proporcjonalności jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniom dla bezpieczeństwa publicznego mogą uzasadniać poważne ingerencje w prawa podstawowe ustanowione w art. 7 i 8 karty, takie jak te, które są związane z zatrzymywaniem danych o ruchu i danych dotyczących lokalizacji, niezależnie od tego, czy jest ono uogólnione i niezróżnicowane, czy ukierunkowane.

25 Sąd odsyłający wskazuje jednak, że Trybunał nie wypowiedział się jeszcze w przedmiocie wpływu późniejszego wykorzystania przedmiotowych danych na ingerencję w prawa podstawowe. W tych okolicznościach sąd odsyłający zastanawia się, czy takie późniejsze wykorzystanie należy również uznać za stanowiące tak poważną ingerencję w prawa podstawowe ustanowione w art. 7 i 8 karty,

że jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniom dla bezpieczeństwa publicznego mogą ją uzasadniać, co wykluczałoby możliwość wykorzystywania tych danych w dochodzeniach dotyczących przewinień dyscyplinarnych związanych z korupcją.

26 W tych okolicznościach Lietuvos vyriausiasis administracinis teismas (najwyższy sąd administracyjny Litwy) postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„Czy art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8, 11 i art. 52 ust. 1 [karty] należy interpretować w ten sposób, że zakazuje on właściwym organom publicznym wykorzystywania danych zatrzymywanych przez dostawców usług łączności elektronicznej, które mogą dostarczać informacji o danych użytkownika środków łączności elektronicznej i o połączeniach realizowanych przez takiego użytkownika, w dochodzeniach, które dotyczą przewinień związanych z korupcją podczas sprawowania urzędu publicznego, niezależnie od tego, czy dostępu do tych danych udzielono w konkretnej sprawie na potrzeby zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego?”.

W przedmiocie pytania prejudycjalnego

27 W swoim pytaniu sąd odsyłający zastanawia się w istocie, czy art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11, a także art. 52 ust. 1 karty należy interpretować w ten sposób, że stoi on na przeszkodzie temu, aby dane osobowe dotyczące łączności elektronicznej, które na podstawie środka ustawowego przyjętego na mocy tego przepisu zostały zatrzymane przez dostawców usług łączności elektronicznej i które zostały następnie udostępnione na podstawie tego środka właściwym organom dla celów zwalczania poważnej przestępczości, mogły być wykorzystywane w ramach dochodzeń dotyczących przewinień dyscyplinarnych związanych z korupcją.

28 Na wstępie należy zauważyć, że z postanowienia odsyłającego wynika, iż chociaż akta postępowania administracyjnego zakończonego dekretami rozpatrywanymi w postępowaniu głównym, o których mowa w pkt 19 niniejszego wyroku, zawierały również informacje zebrane przez właściwe organy dzięki przechwytywaniu i nagrywaniu komunikatów elektronicznych dozwolonym, do celów ścigania karnego, dwoma postanowieniami sądowymi, niemniej jednak sąd odsyłający zastanawia się nie nad wykorzystaniem danych osobowych uzyskanych bez udziału dostawców usług łączności elektronicznej, lecz nad późniejszym wykorzystaniem danych osobowych zatrzymanych przez owych dostawców na podstawie środka ustawodawczego państwa członkowskiego nakładającego na nich taki obowiązek zatrzymywania na podstawie art. 15 ust. 1 dyrektywy 2002/58.

29 W tym względzie z informacji zawartych we wniosku o wydanie orzeczenia w trybie prejudycjalnym wynika, że danymi, o których mowa w przedłożonym pytaniu, są dane zatrzymane na podstawie art. 65 ust. 2 ustawy o łączności elektronicznej w związku z załącznikiem 1 do tej ustawy, nakładającego na dostawców usług łączności elektronicznej obowiązek zatrzymywania, w sposób uogólniony i niezróżnicowany, danych o ruchu i danych dotyczących lokalizacji związanych z taką łącznością dla celów zwalczania poważnej przestępczości.

30 W odniesieniu do warunków, w jakich dane te mogą zostać wykorzystane w postępowaniu administracyjnym dotyczącym przewinień dyscyplinarnych związanych z korupcją, należy przede wszystkim przypomnieć, że dostęp do tych danych może zostać przyznany na podstawie środka

przyjętego na mocy art. 15 ust. 1 dyrektywy 2002/58 tylko wtedy, gdy owe dane zostały zatrzymane przez tych dostawców w sposób zgodny z tym przepisem [zob. podobnie wyrok z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), (C-746/18, EU:C:2021:152, pkt 29 i przytoczone tam orzecznictwo)]. Następnie późniejsze wykorzystanie danych o ruchu i danych dotyczących lokalizacji związanych z taką łącznością dla celów zwalczania poważnej przestępczości jest możliwe tylko pod warunkiem, z jednej strony, że zatrzymywanie danych przez dostawców usług łączności elektronicznej było zgodne z art. 15 ust. 1 dyrektywy 2002/58, tak jak jest on interpretowany w orzecznictwie Trybunału, a z drugiej strony, że dostęp do owych danych udzielony właściwym organom był również zgodny z tym przepisem.

31 W tym względzie Trybunał orzekł już, że z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty sprzeczne są środki ustawodawcze przewidujące, dla celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych dotyczących lokalizacji (wyrok z dnia 20 września 2022 r., SpaceNet i Telekom Deutschland, C-793/19 i C-794/19, EU:C:2022:702, pkt 74, 131 i przytoczone tam orzecznictwo). Trybunał uściślił natomiast, że ów art. 15 ust. 1 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty nie stoi na przeszkodzie środkom ustawodawczym przewidującym, dla celów 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 kategorii osób, których dane dotyczą, lub za pomocą kryterium geograficznego, przez okres ograniczony do tego, co ściśle niezbędne, ale odnawialny;

– uogólnione i niezróżnicowane zatrzymywanie adresów IP przydzielonych źródłu połączenia, przez okres ograniczony do tego, co ściśle niezbędne;

– uogólnione i niezróżnicowane zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej; oraz

– posłużenie się skierowanym do dostawców usług łączności elektronicznej, w drodze decyzji właściwego organu poddanej skutecznej kontroli sądowej, nakazem szybkiego zatrzymania przez określony czas danych o ruchu i danych dotyczących lokalizacji, którymi dysponują ci dostawcy usług,

o ile środki te, za pomocą jasnych i precyzyjnych przepisów, zapewniają, 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 (wyrok z dnia 20 września 2022 r., SpaceNet i Telekom Deutschland, C-793/19 i C-794/19, EU:C:2022:702, pkt 75 i przytoczone tam orzecznictwo).

32 Co się tyczy celów mogących uzasadniać wykorzystanie przez organy władzy publicznej danych zatrzymanych przez dostawców usług łączności elektronicznej na podstawie środka ustawodawczego zgodnego z tymi przepisami, należy przypomnieć, że art. 15 ust. 1 dyrektywy 2002/58 pozwala państwom członkowskim na wprowadzenie wyjątków od ustanowionego w art. 5 ust. 1 tej dyrektywy zasadniczego obowiązku zapewnienia poufności danych osobowych, a także od odpowiadających im obowiązków wymienionych w szczególności w art. 6 i 9 omawianej dyrektywy, kiedy takie ograniczenie jest niezbędne, właściwe i proporcjonalne w społeczeństwie

demokratycznym do ochrony bezpieczeństwa narodowego, obronności i bezpieczeństwa publicznego lub do zapobiegania, dochodzenia, wykrywania i ścigania przestępstw lub niedozwolonego używania systemu łączności elektronicznej. W tym celu państwa członkowskie mogą między innymi przyjmować środki ustawodawcze przewidujące zatrzymywanie danych przez określony czas, jeśli jest to uzasadnione jednym z tych względów (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 110).

33 Jednakże art. 15 ust. 1 dyrektywy 2002/58 nie może uzasadniać tego, że odstępstwo od mającego zasadnicze znaczenie obowiązku zapewnienia poufności łączności elektronicznej i danych z nią związanych, a w szczególności od zakazu zatrzymywania tych danych, przewidzianego w art. 5 wspomnianej dyrektywy, stanie się regułą, gdyż pozbawiłoby to w znacznym stopniu ten przepis jego znaczenia (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 40).

34 Jeśli chodzi o cele, które mogą uzasadniać ograniczenie praw i obowiązków przewidzianych w szczególności w art. 5, 6 i 9 dyrektywy 2002/58, Trybunał orzekł już, że wyliczenie celów dokonane w art. 15 ust. 1 zdanie pierwsze tej dyrektywy ma charakter wyczerpujący, wobec czego środek ustawodawczy przyjęty na podstawie tego przepisu powinien odpowiadać rzeczywiście i ściśle jednemu z tych celów (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 41).

35 Jeśli chodzi o cele interesu ogólnego mogące uzasadniać środek przyjęty na podstawie art. 15 ust. 1 dyrektywy 2002/58, z orzecznictwa Trybunału wynika, że zgodnie z zasadą proporcjonalności istnieje hierarchia wśród tych celów w zależności od znaczenia każdego z nich oraz że znaczenie celu przyświecającego takiemu środkowi musi pozostawać w związku z wagą ingerencji, która z niego wynika (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 56).

36 W tym względzie cel ochrony bezpieczeństwa narodowego, w świetle art. 4 ust. 2 TUE, zgodnie z którym ochrona bezpieczeństwa narodowego pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego, przewyższa znaczeniem inne cele, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, w szczególności cele zwalczania przestępstw w ogólności, choćby poważnych, a także ochrony bezpieczeństwa publicznego. Z zastrzeżeniem poszanowania innych wymogów przewidzianych w art. 52 ust. 1 karty cel ochrony bezpieczeństwa narodowego może więc uzasadniać środki związane z dalej idącą ingerencją w prawa podstawowe niż środki, które mogłyby być uzasadnione tymi innymi celami (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 57 i przytoczone tam orzecznictwo).

37 Jeśli chodzi o cel polegający na zapobieganiu przestępstwom, ich dochodzeniu, wykrywaniu i ściganiu, Trybunał zauważył, że zgodnie z zasadą proporcjonalności jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniom dla bezpieczeństwa publicznego mogą uzasadniać poważne ingerencje w prawa podstawowe ustanowione w art. 7 i 8 karty, takie jak te, które są związane z zatrzymywaniem danych o ruchu i danych o lokalizacji. A zatem jedynie takie ingerencje we wspomniane prawa podstawowe, które nie mają poważnego charakteru, mogą być uzasadnione przez cel polegający na zapobieganiu przestępstwom w ogólności, ich dochodzeniu, wykrywaniu i ściganiu (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 59 i przytoczone tam orzecznictwo).

38 Z orzecznictwa tego wynika, iż chociaż zwalczanie poważnej przestępczości i zapobieganie poważnym zagrożeniom dla bezpieczeństwa publicznego mają w hierarchii celów interesu ogólnego mniejsze znaczenie niż ochrona bezpieczeństwa narodowego (zob. podobnie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 99), ich znaczenie jest jednak większe niż znaczenie zwalczania przestępstw kryminalnych w ogólności i zapobiegania zagrożeniom mniejszej wagi dla bezpieczeństwa publicznego.

39 W tym kontekście należy jednak przypomnieć, że jak wynika również z pkt 31 niniejszego wyroku, możliwość uzasadnienia przez państwa członkowskie ograniczenia praw i obowiązków przewidzianych w szczególności w art. 5, 6 i 9 dyrektywy 2002/58 należy oceniać w drodze badania wagi ingerencji, jaką stanowi takie ograniczenie, oraz sprawdzenia, czy znaczenie celu interesu ogólnego, do którego zmierza to ograniczenie, pozostaje w relacji do tej wagi (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 131).

40 Ponadto Trybunał orzekł już, że dostęp do danych o ruchu i do danych dotyczących lokalizacji zatrzymywanych przez dostawców w zastosowaniu środka przyjętego na podstawie art. 15 ust. 1 dyrektywy 2002/58, co musi mieć miejsce w pełnym poszanowaniu warunków wynikających z orzecznictwa, w którym dokonano wykładni tej dyrektywy, może co do zasady być uzasadniony jedynie celem interesu ogólnego, dla którego dostawcy ci zostali zobowiązani do takiego zatrzymywania. Inaczej jest jedynie wtedy, gdy znaczenie celu przyświecającego dostępowi jest większe niż znaczenie celu, który uzasadniał zatrzymywanie danych (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 98 i przytoczone tam orzecznictwo).

41 Rozważania te mają zastosowanie mutatis mutandis do późniejszego wykorzystania danych o ruchu i danych dotyczących lokalizacji zatrzymywanych przez dostawców usług łączności elektronicznej w zastosowaniu środka przyjętego na podstawie art. 15 ust. 1 dyrektywy 2002/58 dla celów zwalczania poważnej przestępczości. Dane takie nie mogą bowiem, po tym jak zostały zatrzymane i udostępnione właściwym organom dla celów zwalczania poważnej przestępczości, zostać przekazane innym organom i wykorzystane do osiągnięcia celów – takich, tak jak w niniejszym przypadku, zwalczanie przewinień dyscyplinarnych związanych z korupcją – których znaczenie w hierarchii celów interesu ogólnego jest mniejsze niż znaczenie zwalczania poważnej przestępczości i zapobieganie poważnym zagrożeniom dla bezpieczeństwa publicznego. Zezwolenie w takiej sytuacji na dostęp do zatrzymanych danych pozostawałoby bowiem w sprzeczności z tą hierarchią celów interesu ogólnego, przypomnianą w pkt 33, 35–37 i 40 niniejszego wyroku (zob. podobnie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 99).

42 Co się tyczy argumentu podniesionego przez rząd czeski i Irlandię w ich uwagach na piśmie, zgodnie z którym postępowanie dyscyplinarne dotyczące przewinień dyscyplinarnych związanych z korupcją może wiązać się z ochroną bezpieczeństwa publicznego, wystarczy zauważyć, że w postanowieniu odsyłającym sąd odsyłający nie wskazał poważnego zagrożenia dla bezpieczeństwa publicznego.

43 Ponadto, o ile prawdą jest, że dochodzenia administracyjne dotyczące przewinień służbowych lub dyscyplinarnych związanych z aktami korupcji mogą odgrywać istotną rolę w zwalczaniu takich czynów, o tyle środek ustawodawczy przewidujący takie dochodzenia nie odpowiada rzeczywiście i ściśle celowi ścigania i karania przestępstw, o którym mowa w art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58, który dotyczy wyłącznie ścigania karnego.

44 W świetle powyższych rozważań na zadane pytanie trzeba odpowiedzieć, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11, a także art. 52 ust. 1 karty należy interpretować w ten sposób, iż stoi on na przeszkodzie temu, aby dane osobowe dotyczące łączności elektronicznej, które na podstawie środka ustawowego przyjętego na mocy tego przepisu zostały zatrzymane przez dostawców usług łączności elektronicznej i które zostały następnie udostępnione na podstawie tego środka właściwym organom dla celów zwalczania poważnej przestępczości, mogły być wykorzystywane w ramach dochodzeń dotyczących przewinień dyscyplinarnych związanych z korupcją.

W przedmiocie kosztów

45 Dla stron w postępowaniu głównym niniejsze postępowanie ma charakter incydentalny, dotyczy bowiem kwestii podniesionej przed sądem odsyłającym, do niego zatem należy rozstrzygnięcie o kosztach. Koszty poniesione w związku z przedstawieniem uwag Trybunałowi, inne niż koszty stron w postępowaniu głównym, nie podlegają zwrotowi.

Z powyższych względów Trybunał (pierwsza izba) orzeka, co następuje:

Artykuł 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywy o prywatności i łączności elektronicznej), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r., w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej

należy interpretować w ten sposób, że:

stoi on na przeszkodzie temu, aby dane osobowe dotyczące łączności elektronicznej, które na podstawie środka ustawowego przyjętego na mocy tego przepisu zostały zatrzymane przez dostawców usług łączności elektronicznej i które zostały następnie udostępnione na podstawie tego środka właściwym organom dla celów zwalczania poważnej przestępczości, mogły być wykorzystywane w ramach dochodzeń dotyczących przewinień dyscyplinarnych związanych z korupcją.

Podpisy