Zbiór Orzeczeń

WYROK TRYBUNAŁU (wielka izba)

z dnia 20 września 2022 r.*

[sprostowany postanowieniem z dnia 27 października 2022 r.]

Odesłanie prejudycjalne – Przetwarzanie danych osobowych w sektorze łączności elektronicznej – Poufność komunikacji – Dostawcy usług łączności elektronicznej – Uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych dotyczących lokalizacji – Dyrektywa 2002/58/WE – Artykuł 15 ust. 1 – Karta praw podstawowych Unii Europejskiej – Artykuły 6, 7, 8 i 11 oraz art. 52 ust. 1 – Artykuł 4 ust. 2 TUE

W sprawach połączonych C-793/19 i C-794/19

mających za przedmiot wnioski o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożone przez Bundesverwaltungsgericht (federalny sąd administracyjny, Niemcy) postanowieniami z dnia 25 września 2019 r., które wpłynęły do Trybunału w dniu 29 października 2019 r., w postępowaniach:

Bundesrepublik Deutschland, którą reprezentowała Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

przeciwko

SpaceNet AG (C-793/19),

Telekom Deutschland GmbH (C-794/19),

TRYBUNAŁ (wielka izba),

w składzie: K. Lenaerts, prezes, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis i I. Ziemele, prezesi izb, T. von Danwitz, M. Safjan, F. Biltgen, P.G. Xuereb (sprawozdawca), N. Piçarra, L.S. Rossi i A. Kumin, sędziowie,

rzecznik generalny: M. Campos Sánchez-Bordona,

sekretarz: D. Dittert, kierownik wydziału,

uwzględniając pisemny etap postępowania i po przeprowadzeniu rozprawy w dniu 13 września 2021 r.,

* Język postępowania: niemiecki.

rozważywszy uwagi, które przedstawili:

– w imieniu Bundesrepublik Deutschland, reprezentowanej przez Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen – C. Mögelin, w charakterze pełnomocnika,

– [tekst sprostowany postanowieniem z dnia 27 października 2022 r.] w imieniu SpaceNet AG – M. Bäcker, Universitätsprofessor,

– w imieniu Telekom Deutschland GmbH – T. Mayen, Rechtsanwalt,

– w imieniu rządu niemieckiego – J. Möller, F. Halibi, M. Hellmann, D. Klebs oraz E. Lankenau, w charakterze pełnomocników,

– w imieniu rządu duńskiego – M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen oraz M. Søndahl Wolff, w charakterze pełnomocników,

– w imieniu rządu estońskiego – A. Kalbus oraz M. Kriisa, w charakterze pełnomocników,

– w imieniu Irlandii – A. Joyce oraz J. Quaney, w charakterze pełnomocników, których wspierali D. Fennelly, BL, oraz P. Gallagher, SC,

– w imieniu rządu hiszpańskiego – L. Aguilera Ruiz, w charakterze pełnomocnika,

– w imieniu rządu francuskiego – A. Daniel, D. Dubois, J. Illouz, E. de Moustier oraz T. Stéhelin, w charakterze pełnomocników,

– w imieniu rządu cypryjskiego – I. Neophytou, w charakterze pełnomocnika,

– w imieniu rządu niderlandzkiego – M.K. Bulterman, A. Hanje oraz C.S. Schillemans, w charakterze pełnomocników,

– w imieniu rządu polskiego – B. Majczyna, D. Lutostańska oraz J. Sawicka, w charakterze pełnomocników,

– w imieniu rządu finlandzkiego – A. Laine oraz M. Pere, w charakterze pełnomocników,

– w imieniu rządu szwedzkiego – H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson i H. Shev, w charakterze pełnomocników,

– w imieniu Komisji Europejskiej – G. Braun, S.L. Kalėda, H. Kranenborg, M. Wasmeier oraz F. Wilman, w charakterze pełnomocników,

– w imieniu Europejskiego Inspektora Ochrony Danych – A. Buchta, D. Nardi, N. Stolič oraz K. Ujazdowski, w charakterze pełnomocników,

po zapoznaniu się z opinią rzecznika generalnego na posiedzeniu w dniu 18 listopada 2021 r.,

wydaje następujący

Wyrok

1 Niniejsze wnioski o wydanie orzeczenia w trybie prejudycjalnym dotyczą wykładni art. 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 (dyrektywa 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") w związku z art. 6–8, 11 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą") oraz art. 4 ust. 2 TUE.

2 Wnioski te zostały złożone w ramach sporów, jakie powstały pomiędzy Bundesrepublik Deutschland (Republiką Federalną Niemiec), reprezentowaną przez Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (federalną agencję do spraw sieci energii elektrycznej, gazu, telekomunikacji, poczty i kolei, Niemcy), a SpaceNet AG (sprawa C-793/19) oraz Telekom Deutschland GmbH (sprawa C-794/19) w przedmiocie nałożonego na te podmioty obowiązku zatrzymywania dotyczących ich klientów danych o ruchu i danych dotyczących lokalizacji związanych z telekomunikacją.

Ramy prawne

Prawo Unii

Dyrektywa 95/46/WE

3 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) została zastąpiona, ze skutkiem od dnia 25 maja 2018 r., rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46 (ogólnym rozporządzeniem o ochronie danych) (Dz.U. 2016, L 119, s. 1; sprostowanie Dz.U. 2018, L 127, s. 2).

4 Artykuł 3 ust. 2 dyrektywy 95/46 stanowił:

„Niniejsza dyrektywa nie ma zastosowania do przetwarzania danych osobowych:

– w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. dane, o których stanowi tytuł V i VI Traktatu o Unii Europejskiej, a w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarcza państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności państwa w obszarach prawa karnego,

– przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze".

Dyrektywa 2002/58

5 Motywy 2, 6, 7 i 11 dyrektywy 2002/58 mają następujące brzmienie:

„(2) Niniejsza dyrektywa dąży do poszanowania fundamentalnych praw i jest zgodna z zasadami uznanymi w szczególności przez [kartę]. Dyrektywa ta zmierza w szczególności do zapewnienia pełnego poszanowania praw określonych w art. 7 i 8 tej karty.

[…]

(6) Internet przekształca tradycyjne struktury rynkowe przez udostępnienie ogólnej, globalnej infrastruktury dostarczającej szerokiego spektrum usług łączności elektronicznej. Usługi łączności elektronicznej ogólnodostępne za pośrednictwem Internetu stwarzają nowe możliwości użytkownikom, ale również powodują powstanie nowych zagrożeń dotyczących ich danych osobowych i prywatności.

(7) W przypadku publicznych sieci łączności należy wprowadzić szczególne przepisy prawne, wykonawcze i techniczne w celu ochrony podstawowych praw i wolności osób fizycznych oraz uzasadnionego interesu osób prawnych, w szczególności w odniesieniu do zwiększonej pojemności automatycznego przechowywania i przetwarzania danych odnoszących się do abonentów i użytkowników.

[…]

(11) Niniejsza dyrektywa, podobnie jak dyrektywa [95/46], nie odnosi się do kwestii ochrony podstawowych praw i wolności związanych z działalnością, która nie jest regulowana prawem wspólnotowym. Dyrektywa nie zmienia zatem istniejącej równowagi między prawem do prywatności osoby fizycznej a [przysługującą państwom członkowskim] możliwością podejmowania środków, określonych w art. 15 ust. 1 niniejszej dyrektywy, niezbędnych do ochrony bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając gospodarczy dobrobyt państwa, gdy działania dotyczą zagadnień bezpieczeństwa państwa) i wykonywania prawa karnego. Wskutek tego niniejsza dyrektywa nie wpływa na możliwości państw członkowskich do zgodnego z prawem przejmowania danych w łączności elektronicznej lub podejmowania innych środków, jeżeli jest to konieczne dla któregokolwiek z tych celów i zgodne z europejską Konwencją o ochronie praw człowieka i podstawowych wolności [podpisaną w Rzymie dnia 4 listopada 1950 r.], dla której wykładnię stanowi orzecznictwo Europejskiego Trybunału Praw Człowieka. Środki tego rodzaju muszą być właściwe, współmierne do zamierzonego celu i niezbędne w ramach społeczeństwa demokratycznego. Środki te powinny podlegać stosownym zabezpieczeniom zgodnie z europejską Konwencją o ochronie praw człowieka i podstawowych wolności”.

6 Artykuł 1 tej dyrektywy, 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.

2. Przepisy niniejszej dyrektywy dookreślają i uzupełniają dyrektywę [95/46] zgodnie z celami przedstawionymi w ust. 1. Ponadto zapewniają ochronę uzasadnionych interesów abonentów będących osobami prawnymi.

3. Niniejsza dyrektywa nie ma zastosowania do działalności, która wykracza poza zakres [traktatu FUE], takiej jak działalność określona w tytułach V i VI traktatu [UE], 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".

7 Zgodnie z art. 2 tej dyrektywy, zatytułowanym „Definicje":

„Z zastrzeżeniem innych przepisów stosuje się definicje z dyrektywy [95/46] i dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) [(Dz.U. 2002, L 108, s. 33)].

Stosuje się również następujące definicje:

a) »użytkownik« oznacza każdą osobę fizyczną korzystającą z publicznie dostępnych usług łączności elektronicznej, do celów prywatnych lub handlowych, niekoniecznie na podstawie abonamentu za te usługi;

b) »dane o ruchu« oznaczają wszelkie dane przetwarzane do celów przekazywania komunikatu w sieci łączności elektronicznej lub naliczania opłat za te usługi;

c) »dane dotyczące lokalizacji« oznaczają wszelkie dane przetwarzane w sieci łączności elektronicznej lub w ramach usług łączności elektronicznej wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług łączności elektronicznej;

d) »komunikat« oznacza każdą informację wymienianą lub przekazaną między określoną liczbą stron za pośrednictwem usług publicznie dostępnej łączności elektronicznej. Nie obejmuje on informacji przekazanej jako część publicznych usług nadawczych przez sieć łączności elektronicznej, z wyjątkiem zakresu, w jakim informacja może się odnosić do możliwego do zidentyfikowania abonenta lub użytkownika otrzymującego informację;

[…]".

8 Artykuł 3 dyrektywy 2002/58, zatytułowany „Usługi", stanowi:

„Niniejsza dyrektywa ma zastosowanie do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności we Wspólnocie, włącznie z publicznymi sieciami łączności służącymi do zbierania danych i obsługi urządzeń identyfikacyjnych".

9 Zgodnie z art. 5 dyrektywy 2002/58, zatytułowanym „Poufność komunikacji":

„1. 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.

[…]

3. Państwa członkowskie zapewniają, aby przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym abonenta lub użytkownika było dozwolone wyłącznie pod warunkiem, że dany abonent lub użytkownik wyraził zgodę zgodnie z dyrektywą [95/46], po otrzymaniu jasnych i wyczerpujących informacji, między innymi o celach przetwarzania. Nie stanowi to przeszkody dla każdego technicznego przechowywania danych ani dostępu do nich jedynie w celu wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej lub gdy jest to ściśle niezbędne w celu świadczenia usługi przez dostawcę usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika”.

10 Artykuł 6 dyrektywy 2002/58, zatytułowany „Dane o ruchu”, stanowi:

„1. Dane o ruchu dotyczące abonentów i użytkowników przetwarzane i przechowywane przez dostawcę publicznej sieci łączności lub publicznie dostępnych usług łączności elektronicznej muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu, bez uszczerbku dla przepisów ust. 2, 3 i 5 niniejszego artykułu oraz art. 15 ust. 1.

2. Można przetwarzać dane o ruchu niezbędne do celów naliczania opłat abonenta i opłat rozliczeń międzyoperatorskich. Przetwarzanie takie jest dozwolone tylko do końca okresu, w którym rachunek może być zgodnie z prawem zakwestionowany lub w którym należy uiścić opłatę.

3. Do celów wprowadzania na rynek usług łączności elektronicznej lub świadczenia usług tworzących wartość wzbogaconą dostawca publicznie dostępnych usług łączności elektronicznej może przetwarzać dane określone w ust. 1, w zakresie i przez czas niezbędny dla tego rodzaju usług lub wprowadzania ich na rynek, jeżeli abonent lub użytkownik, których dane dotyczą, uprzednio wyraził na to zgodę. Użytkownicy lub abonenci mają w każdej chwili możliwość odwołania swojej zgody na przetwarzanie danych o ruchu.

[…]

5. Przetwarzanie danych o ruchu, zgodnie z ust. 1–3 i 4, musi być ograniczone do osób działających z upoważnienia dostawców publicznych sieci łączności i publicznie dostępnych usług łączności elektronicznej, zajmujących się naliczaniem opłat lub ruchem, obsługą klienta, systemem wykrywania nadużyć finansowych, marketingiem usług łączności elektronicznej lub świadczeniem usług tworzących wartość dodaną, oraz musi być ograniczone do celów niezbędnych przy takich działaniach.

[…]”.

11 Artykuł 9 tej dyrektywy, zatytułowany „Dane dotyczące lokalizacji inne niż dane o ruchu", przewiduje w ust. 1:

„W przypadku gdy dane dotyczące lokalizacji inne niż dane o ruchu, odnoszące się do użytkowników lub abonentów publicznych sieci łączności lub publicznie dostępnych usług łączności elektronicznej, mogą być przetwarzane, przetwarzanie może mieć miejsce tylko wówczas, gdy dane te są anonimowe, lub za zgodą użytkowników lub abonentów, w zakresie i przez okres niezbędny do świadczenia usługi tworzącej wartość dodaną. Przed uzyskaniem zgody użytkowników lub abonentów dostawca usług musi ich poinformować o rodzaju danych dotyczących lokalizacji innych niż dane o ruchu, które będą przetwarzane, o celach i okresie ich przetwarzania oraz o tym, czy dane zostaną przekazane stronie trzeciej do celów świadczenia usługi tworzącej wartość dodaną […]".

12 Artykuł 15 dyrektywy 2002/58, zatytułowany „Stosowanie niektórych przepisów dyrektywy [95/46]", stanowi w ust. 1:

„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 (tj. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy [95/46]. W tym celu państwa członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie 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 niemieckie

TKG

13 Paragraf 113a ust. 1 zdanie pierwsze Telekommunikationsgesetz (ustawy o telekomunikacji) z dnia 22 czerwca 2004 r. (BGBl. 2004 I, s. 1190) w wersji mającej zastosowanie do sporu w postępowaniu głównym (zwanej dalej „TKG") ma następujące brzmienie:

„Obowiązki dotyczące zatrzymywania, wykorzystywania i bezpieczeństwa danych dotyczących ruchu określone w § 113b–113g dotyczą operatorów świadczących użytkownikom końcowym publicznie dostępne usługi telekomunikacyjne".

14 Zgodnie z § 113b TKG:

„(1) Operatorzy, o których mowa w § 113a ust. 1, dokonują zatrzymywania danych na terytorium kraju w następujący sposób:

1. przez okres dziesięciu tygodni w odniesieniu do danych, o których mowa w ust. 2 i 3,

2. przez okres czterech tygodni w odniesieniu do danych, o których mowa w ust. 4,

(2) Dostawcy publicznie dostępnych usług telefonicznych zatrzymują następujące dane:

1. numer linii wywołującej lub inny identyfikator nadawcy lub odbiorcy połączenia oraz w przypadku przekierowywania lub przełączania połączenia numer, na który połączenie jest przekierowywane lub przełączane;

2. data i godzina rozpoczęcia i zakończenia połączenia ze wskazaniem danej strefy czasowej;

3. informacje dotyczące wykorzystanej usługi, w przypadku gdy można korzystać z różnych usług w ramach usługi telefonii stacjonarnej;

4. ponadto, w przypadku usług telefonii komórkowej:
   a) międzynarodowy numer tożsamości telefonicznej abonenta mobilnego nadawcy i odbiorcy połączenia;
   b) międzynarodowy numer fabryczny aparatu telefonicznego nadawcy i odbiorcy połączenia;
   c) data i godzina pierwszej aktywacji usługi wraz ze wskazaniem bazowej strefy czasowej, w przypadku gdy usługi zostały opłacone z góry;

5. w przypadku usług telefonii internetowej również adresy IP nadawcy i odbiorcy połączenia oraz przypisany identyfikator użytkownika.

Pierwszy akapit stosuje się odpowiednio:

1. w przypadku połączenia za pomocą wiadomości SMS, wiadomości multimedialnej lub podobnej wiadomości; w takim przypadku informacje, o których mowa w pkt 2 akapitu pierwszego, zastępuje się informacją o czasie wysłania i odebrania wiadomości;

2. w przypadku połączeń bez odpowiedzi lub nieudanych z powodu interwencji operatora sieci […].

(3) Dostawcy publicznie dostępnych usług dostępu do Internetu zatrzymują następujące dane:

1. adres IP przypisany abonentowi w celu korzystania z Internetu;

2. jednoznaczny identyfikator łącza, przez które następuje korzystanie z Internetu, oraz przypisany identyfikator użytkownika;

3. data i godzina rozpoczęcia i zakończenia korzystania z Internetu pod przypisanym adresem IP ze wskazaniem rozpatrywanej strefy czasowej.

(4) W przypadku korzystania z usług telefonii komórkowej zatrzymywane są oznaczenia komórek używanych przez linię wywołującą i linię wywoływaną na początku połączenia. Co się tyczy publicznie dostępnych usług dostępu do Internetu, w przypadku korzystania z telefonii komórkowej zatrzymywane jest oznaczenie komórki używanej na początku połączenia z Internetem. Należy również zatrzymywać dane wskazujące na położenie geograficzne i kierunki wiązki głównej anten radiowych obsługujących daną komórkę.

(5) Na podstawie niniejszego przepisu nie można zatrzymywać treści komunikatów, danych dotyczących przeglądanych stron internetowych i danych usług poczty elektronicznej.

(6) Na mocy niniejszego przepisu nie można zatrzymywać danych leżących u podstaw połączeń, o których mowa w § 99 ust. 2. Dotyczy to mutatis mutandis połączeń telefonicznych od podmiotów, o których mowa w § 99 ust. 2. Przepisy § 99 ust. 2 zdania od drugiego do siódmego stosuje się odpowiednio.

[…]".

15 Połączenia, o których mowa w § 99 ust. 2 TKG, do których odsyła § 113b ust. 6 TKG, to połączenia z osobami, organami i organizacjami o charakterze społecznym lub religijnym, które oferują wyłącznie lub głównie osobom, które pozostają co do zasady anonimowe, usługi pomocy telefonicznej w nagłych przypadkach, w razie kryzysu psychologicznego lub społecznego, które same lub których współpracownicy podlegają szczególnemu obowiązkowi zachowania poufności w tym względzie. Zgodnie z § 99 ust. 2 zdania od drugiego do czwartego TKG przyznanie tego wyjątku jest uzależnione od wpisania podmiotów, do których wykonywane są połączenia, na ich wniosek na listę prowadzoną przez federalną agencję do spraw sieci energii elektrycznej, gazu, telekomunikacji, poczty i kolei, pod warunkiem potwierdzenia przez abonentów posiadających numery charakteru świadczonych usług w drodze zaświadczenia wydanym przez podmiot, instytucję lub fundację prawa publicznego.

16 Zgodnie z brzmieniem § 113c ust. 1 i 2 TKG:

„(1) Dane zatrzymywane na podstawie § 113b mogą:

1. zostać przekazane organom ścigania, w przypadku gdy występują one o to przekazanie, powołując się na przepis prawny zezwalający im na gromadzenie danych, o których mowa w § 113b, w celu ścigania szczególnie poważnych przestępstw;

2. zostać przekazane organom bezpieczeństwa krajów związkowych, w przypadku gdy występują one o to przekazanie, powołując się na przepis prawny zezwalający im na gromadzenie danych, o których mowa w § 113b, w celu zapobiegania konkretnemu zagrożeniu dla zdrowia, życia lub wolności osoby lub istnienia państwa federalnego lub kraju związkowego;

[…]

(2) Dane zatrzymywane na podstawie § 113b nie mogą być wykorzystywane przez osoby odpowiedzialne za wypełnianie obowiązków określonych w § 113a ust. 1 do celów innych niż te, o których mowa w ust. 1".

17 Paragraf 113d TKG stanowi:

„Osoba odpowiedzialna za wypełnianie obowiązku wynikającego z § 113a ust. 1 zapewnia, by dane zatrzymywane zgodnie z § 113b ust. 1 w ramach obowiązku zatrzymywania danych były chronione za pomocą zgodnych z aktualnym stanem techniki środków technicznych i organizacyjnych przed ich nieuprawnioną kontrolą i wykorzystaniem. Środki te obejmują w szczególności:

1. zastosowanie szczególnie bezpiecznego procesu szyfrowania;

2. przechowywanie w przeznaczonej do tego celu infrastrukturze, odrębnej od tej, która jest wykorzystywana do bieżących funkcji operacyjnych;

3. przechowywanie, z zachowaniem wysokiego poziomu ochrony przed cyberatakami, w niepowiązanych systemach informatycznych przetwarzania danych;

4. ograniczenie dostępu do instalacji wykorzystywanych do przetwarzania danych do osób, które zostały do tego w szczególny sposób upoważnione przez zobowiązanego; oraz

5. obowiązek zaangażowania przy dostępie do danych co najmniej dwóch osób, które zostały do tego w szczególny sposób upoważnione przez zobowiązanego".

18 Paragraf 113e TKG ma następujące brzmienie:

„(1) Osoba odpowiedzialna za wypełnianie obowiązku ustanowionego w § 113a ust. 1 zapewnia, aby, w celu monitorowania ochrony danych, każdy dostęp, w szczególności odczyt, kopiowanie, zmiana, usuwanie i blokowanie danych zatrzymanych na mocy § 113b ust. 1, był, w ramach obowiązku zatrzymywania danych, rejestrowany. Rejestrowane są następujące dane:

1. godzina uzyskania dostępu;

2. osoby uzyskujące dostęp do danych;

3. przedmiot i rodzaj dostępu.

(2) Zarejestrowane dane nie mogą być wykorzystywane do celów innych niż kontrola ochrony danych.

(3) Osoba odpowiedzialna za wypełnianie obowiązku wynikającego z § 113a ust. 1 zapewnia, aby zarejestrowane dane zostały usunięte po upływie jednego roku".

19 W celu zapewnienia szczególnie wysokiego poziomu bezpieczeństwa i jakości danych niemiecka federalna agencja ds. sieci ustanawia, zgodnie z § 113f ust. 1 TKG, szereg wymogów, które zgodnie z § 113f ust. 2 tej dyrektywy mają być poddawane stałej ocenie i w razie potrzeby dostosowywane. W § 113g TKG ustanowiony został wymóg, aby koncepcja polityki bezpieczeństwa, którą powinna przedstawić osoba odpowiedzialna za wypełnianie obowiązku ustanowionego w § 113a TKG, obejmowała szczególne środki bezpieczeństwa.

StPO

20 Paragraf 100g ust. 2 zdanie pierwsze Strafprozessordnung (niemieckiego kodeksu postępowania karnego, zwanego dalej „StPO") ma następujące brzmienie:

„Jeżeli pewne fakty dają podstawę do podejrzeń, że dana osoba popełniła, jako sprawca lub współsprawca, jedno ze szczególnie poważnych przestępstw, o których mowa w zdaniu drugim, lub, w przypadkach, w których usiłowanie popełnienia przestępstwa jest karalne, usiłowała popełnić takie przestępstwo i przestępstwo to jest również w danym przypadku szczególnie poważne, dane dotyczące ruchu zatrzymane zgodnie z § 113b [TKG] mogą być gromadzone, jeżeli ustalenie faktów lub miejsca pobytu osoby objętej dochodzeniem byłoby znacznie utrudnione lub niewykonalne przy zastosowaniu innych środków oraz jeżeli gromadzenie danych jest proporcjonalne do wagi sprawy".

21 W § 101a ust. 1 StPO gromadzenie danych o ruchu zostało uzależnione, zgodnie z § 100g StPO, od udzielenia zgody przez sąd. Zgodnie z § 101a ust. 2 StPO uzasadnienie decyzji zawiera istotne względy dotyczące niezbędności i odpowiedniości środka w danym konkretnym przypadku. W § 101a ust. 6 StPO przewidziany został obowiązek poinformowania uczestników danej telekomunikacji.

Postępowania główne i pytanie prejudycjalne

22 SpaceNet i Telekom Deutschland świadczą w Niemczech publicznie dostępne usługi dostępu do Internetu. Telekom Deutschland świadczy ponadto, również w Niemczech, publicznie dostępne usługi telefoniczne.

23 Usługodawcy ci zakwestionowali przed Verwaltungsgericht Köln (sądem administracyjnym w Kolonii, Niemcy) nałożony na nich na mocy § 113a ust. 1 w związku z § 113b TKG obowiązek zatrzymywania dotyczących ich klientów danych o ruchu i danych dotyczących lokalizacji związanych z telekomunikacją począwszy od dnia 1 lipca 2017 r.

24 W wyrokach z dnia 20 kwietnia 2018 r. Verwaltungsgericht Köln (sąd administracyjny w Kolonii) orzekł, że SpaceNet i Telekom Deutschland nie były zobowiązane do zatrzymywania danych o ruchu związanych z telekomunikacją, o których mowa w § 113b ust. 3 TKG, które to dane dotyczą klientów, którym świadczą one usługi dostępu do Internetu, oraz że Telekom Deutschland nie była ponadto zobowiązana do zatrzymywania danych o ruchu związanych z telekomunikacją, o których mowa w § 113b ust. 2 zdania pierwsze i drugie TKG, dotyczących klientów, którym świadczy ona publicznie dostępne usługi telefonii. Sąd ten uznał bowiem, w świetle wyroku z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970), że ów obowiązek zatrzymywania danych jest sprzeczny z prawem Unii.

25 Republika Federalna Niemiec wniosła skargę rewizyjną od tych wyroków do Bundesverwaltungsgericht (federalnego sądu administracyjnego, Niemcy), czyli sądu odsyłającego.

26 Sąd ten jest zdania, że rozstrzygnięcie kwestii tego, czy ustanowiony na mocy § 113a ust. 1 w związku z § 113b TKG obowiązek zatrzymywania danych jest sprzeczny z prawem Unii, zależy od wykładni dyrektywy 2002/58.

27 W tym względzie sąd odsyłający wskazuje, że Trybunał ustalił już w sposób ostateczny w wyroku z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970), że uregulowania dotyczące zatrzymywania danych o ruchu i danych dotyczących lokalizacji oraz uzyskiwania dostępu do tych danych przez organy krajowe są co do zasady objęte zakresem zastosowania dyrektywy 2002/58

28 Sąd ten wskazuje również, że rozpatrywany w postępowaniu głównym obowiązek zatrzymywania danych, w zakresie, w jakim ogranicza on prawa wynikające z art. 5 ust. 1, art. 6 ust. 1 i z art. 9 ust. 1 dyrektywy 2002/58, może być uzasadniony jedynie na gruncie art. 15 ust. 1 tej dyrektywy.

29 W tym względzie sąd ten przypomina, iż z wyroku z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970) wynika, że 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, iż stoi on na przeszkodzie uregulowaniu krajowemu przewidującemu do celów zwalczania przestępczości

uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej.

30 Zgodnie zaś ze zdaniem sądu odsyłającego, podobnie jak ma to miejsce w przypadku przepisów krajowych rozpatrywanych w sprawach, w których zapadł wspomniany wyrok, rozpatrywane w postępowaniu głównym uregulowanie krajowe nie ustanawia wymogu istnienia jakiegokolwiek uzasadnienia dla zatrzymywania danych ani też jakiegokolwiek związku między zatrzymywanymi danymi a przestępstwem lub zagrożeniem dla bezpieczeństwa publicznego. Te przepisy krajowe ustanawiają bowiem obowiązek zatrzymywania, bez uzasadnionego powodu, w uogólniony i niezróżnicowany z punktu widzenia osobistego, czasowego i geograficznego sposób, większości związanych z telekomunikacją istotnych danych o ruchu.

31 Sąd odsyłający uważa jednak, że nie jest wykluczone, iż obowiązek zatrzymywania danych rozpatrywany w postępowaniu głównym może okazać się być uzasadniony na podstawie art. 15 ust. 1 dyrektywy 2002/58.

32 W pierwszej kolejności sąd odsyłający podnosi, że, w przeciwieństwie do uregulowań krajowych rozpatrywanych w sprawach zakończonych wyrokiem z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970), w rozpatrywanym w postępowaniu głównym uregulowaniu krajowym nie ustanowiono wymogu zatrzymywania wszystkich danych o ruchu, które dotyczą telekomunikacji wszystkich abonentów i zarejestrowanych użytkowników w odniesieniu do wszystkich środków łączności elektronicznej. Z obowiązku zatrzymywania danych wyłączona ma być nie tylko treść komunikatów, ale nie mogłyby być też zatrzymywane dane dotyczące odwiedzanych stron internetowych, dane dotyczące usług poczty elektronicznej oraz dane leżące u podstaw połączeń z lub do określonych numerów należących do sfer społecznej lub religijnej, co wynika z § 113b ust. 5 i 6 TKG.

33 W drugiej kolejności sąd ten wskazuje, że w § 113b ust. 1 TKG przewiduje czterotygodniowy okres zatrzymywania danych dotyczących lokalizacji i dziesięciotygodniowy okres w odniesieniu do danych o ruchu, zaś dyrektywa Parlamentu Europejskiego i Rady 2006/24/WE 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 zmieniającej dyrektywę 2002/58/WE (Dz.U. 2006, L 105, s. 54), na której opierały się przepisy krajowe rozpatrywane w sprawach, w których wydano wyrok z dnia 21 grudnia 2016 r. Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970), przewidywała okres zatrzymywania mieszczący się w przedziale od sześciu miesięcy do dwóch lat.

34 Sąd odsyłający stoi zaś na stanowisku, że choć wyłączenie niektórych środków łączności lub niektórych kategorii danych oraz ograniczenie okresu przechowywania nie wystarczą do wyeliminowania prawdopodobieństwa stworzenia pełnego profilu osób, których dane dotyczą, to prawdopodobieństwo to jest przynajmniej, w ramach stosowania uregulowania krajowego rozpatrywanego w postępowaniu głównym, znacznie ograniczone.

35 W trzeciej kolejności – uregulowanie to przewiduje ścisłe ograniczenia w zakresie ochrony zatrzymywanych danych i uzyskiwania do nich dostępu. Z jednej strony bowiem zapewnia ono skuteczną ochronę zatrzymywanych danych przed prawdopodobieństwem zaistnienia nadużyć, jak również przed uzyskaniem nieuprawnionego dostępu do tych danych, a z drugiej strony

zatrzymywane dane mogą być wykorzystywane wyłącznie do celów walki z poważnymi przestępstwami lub do zapobiegania konkretnemu zagrożeniu dla zdrowia, życia lub wolności danej osoby czy też dla istnienia państwa federalnego lub kraju związkowego.

36 W czwartej kolejności – przyjęcie takiej wykładni art. 15 ust. 1 dyrektywy 2002/58, która idzie w kierunku uogólnionej niezgodności z prawem Unii jakiegokolwiek przechowywania danych bez uzasadnionego powodu, mogłoby kolidować z istniejącym po stronie państw członkowskich obowiązkiem działania, wynikającym z ustanowionego w art. 6 karty prawa do bezpieczeństwa.

37 W piątej kolejności sąd odsyłający uważa, że taka wykładnia art. 15 dyrektywy 2002/58, zgodnie z którą sprzeciwia się on uogólnionemu zatrzymywaniu danych, znacznie ograniczałaby zakres swobody, jaka przysługuje ustawodawcy krajowemu w dziedzinie zwalczania przestępstw i zapewnienia bezpieczeństwa publicznego, która to dziedzina objęta jest, zgodnie z art. 4 ust. 2 TUE, wyłączną odpowiedzialnością poszczególnych państw członkowskich.

38 W szóstej kolejności sąd odsyłający zauważa, że należy uwzględnić orzecznictwo Europejskiego Trybunału Praw Człowieka, i podnosi, że sąd ten orzekł, iż art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności (zwanej dalej „EKPC") nie stoi na przeszkodzie przepisom krajowym przewidującym masowe przechwytywanie transgranicznego przepływu danych, a to ze względu na zagrożenia, na jakie obecnie napotyka szereg państw, oraz ze względu na narzędzia technologiczne, z których obecnie mogą korzystać terroryści i przestępcy, aby dopuszczać się nagannych czynów.

39 W tych okolicznościach Bundesverwaltungsgericht (federalny sąd administracyjny, Niemcy) postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującym pytaniem prejudycjalnym:

„W świetle art. 7, 8 i 11 oraz art. 52 ust. 1 [karty] z jednej strony i art. 6 [karty] oraz art. 4 TUE z drugiej strony – czy art. 15 dyrektywy [2002/58] należy interpretować w ten sposób, że nie stoi on na przeszkodzie uregulowaniu krajowemu, które nakłada na operatorów dostępnych publicznie usług łączności elektronicznej obowiązek zatrzymywania danych o ruchu i lokalizacji użytkowników końcowych tych usług, jeżeli obowiązek ten:

1) nie wymaga żadnego szczególnego powodu pod względem miejscowym, czasowym lub przestrzennym,

2) przedmiotem obowiązku przechowywania przy świadczeniu dostępnych publicznie usług telefonicznych – w tym transmisji krótkich wiadomości tekstowych, wiadomości multimedialnych lub podobnych wiadomości oraz w przypadku połączeń nieodebranych lub nieudanych – są następujące dane:
   a) numer linii wywołującej lub inny identyfikator nadawcy lub odbiorcy połączenia oraz w przypadku przekierowywania lub przełączania połączenia numer, na który połączenie jest przekierowywane lub przełączane;
   b) data i godzina rozpoczęcia i zakończenia połączenia lub w przypadku transmisji krótkiej wiadomości tekstowej, wiadomości multimedialnej lub podobnej wiadomości – data wysłania i otrzymania informacji ze wskazaniem bazowej strefy czasowej;
   c) informacje dotyczące wykorzystanej usługi, w przypadku gdy można korzystać z różnych usług w ramach usługi telefonii stacjonarnej;
   d) ponadto w przypadku usług telefonii komórkowej:

i) międzynarodowy numer tożsamości telefonicznej abonenta mobilnego nadawcy i odbiorcy połączenia;
ii) międzynarodowy numer fabryczny aparatu telefonicznego nadawcy i odbiorcy połączenia;
iii) data i godzina pierwszej aktywacji usługi wraz ze wskazaniem bazowej strefy czasowej, w przypadku gdy usługi zostały opłacone z góry;
iv) oznaczenie komórek, które zostały wykorzystane przez numer wywołujący i wywołany na początku połączenia;

e) w przypadku usług telefonii internetowej również adresy IP nadawcy i odbiorcy połączenia oraz przypisany identyfikator użytkownika;

3) przedmiotem obowiązku przechowywania przy świadczeniu dostępnych publicznie usług dostępu do Internetu są następujące dane:
a) adres IP przypisany abonentowi w celu korzystania z Internetu;
b) jednoznaczny identyfikator łącza, przez które następuje korzystanie z Internetu, oraz przypisany identyfikator użytkownika;
c) data i godzina rozpoczęcia i zakończenia korzystania z Internetu pod przypisanym adresem IP ze wskazaniem bazowej strefy czasowej;
d) w przypadku korzystania mobilnego – oznaczenie komórki wykorzystanej na początku połączenia internetowego;

4) nie mogą być przechowywane następujące dane:
a) treść komunikatu;
b) dane dotyczące przeglądanych stron internetowych;
c) organów i organizacji działających w sferach społecznych lub religijnych;
d) dane leżące u podstaw połączeń z lub do określonych numerów osób, organów i organizacji działających w sferach społecznych lub religijnych;

5) okres zatrzymywania danych wynosi w przypadku danych dotyczących lokalizacji, czyli oznaczenia wykorzystanej komórki, cztery tygodnie, a w przypadku pozostałych danych – dziesięć tygodni;

6) zapewniona jest skuteczna ochrona zatrzymywanych danych przed ryzykiem nadużyć oraz przed nieuprawnionym dostępem; oraz

7) zatrzymywane dane mogą być wykorzystywane wyłącznie w celu ścigania szczególnie ciężkich przestępstw oraz zapobiegania konkretnym zagrożeniom dla zdrowia, życia lub wolności danej osoby lub dla istnienia państwa federalnego lub kraju związkowego, z wyjątkiem adresu IP przypisanego abonentowi w celu korzystania z Internetu, którego używanie jest dozwolone w ramach udzielania informacji na temat zgromadzonych danych w celu ścigania wszystkich przestępstw, w celu zapobiegania zagrożeniom dla bezpieczeństwa i porządku publicznego oraz w celu wykonywania zadań służb wywiadowczych?”.

Postępowanie przed Trybunałem

40 Postanowieniem prezesa Trybunału z dnia 3 grudnia 2019 r. sprawy C-793/19 i C-794/19 zostały połączone do celów przeprowadzenia pisemnego i ustnego etapu postępowania oraz wydania wyroku.

41 Decyzją prezesa Trybunału z dnia 14 lipca 2020 r. postępowanie w sprawach połączonych C-793/19 i C-794/19 zostało zawieszone na podstawie art. 55 § 1 lit. b) regulaminu postępowania przed Trybunałem do czasu ogłoszenia wyroku La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18).

42 Po wydaniu przez Trybunał w dniu 6 października 2020 r. wyroku w sprawie La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791) prezes Trybunału zarządził w dniu 8 października 2020 r. podjęcie postępowania w sprawach połączonych C-793/19 i C-794/19.

43 Sąd krajowy, do którego wiadomości sekretariat Trybunału przekazał ten wyrok, wskazał, że podtrzymuje swój wniosek o wydanie orzeczenia w trybie prejudycjalnym.

44 W tym względzie sąd odsyłający zauważył przede wszystkim, że przewidziany w uregulowaniu rozpatrywanym w postępowaniu głównym obowiązek zatrzymywania dotyczy mniejszej liczby danych i krótszego okresu przechowywania niż przewidywały to przepisy krajowe rozpatrywane w sprawach zakończonych wyrokiem 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). Jego zdaniem te charakterystyczne cechy zmniejszają prawdopodobieństwo tego, że zatrzymywane dane umożliwiłyby sformułowanie bardzo dokładnych wniosków dotyczących życia prywatnego osób, których dane zostały zatrzymane.

45 Następnie sąd ten ponownie wskazał, że uregulowanie krajowe rozpatrywane w postępowaniu głównym zapewnia skuteczną ochronę zatrzymywanych danych przed prawdopodobieństwem popełnienia nadużyć i uzyskania nielegalnego dostępu.

46 Wreszcie sąd odsyłający podkreślił, że istnieją wątpliwości co do kwestii zgodności z prawem Unii zatrzymywania adresów IP przewidzianego w uregulowaniu krajowym rozpatrywanym w postępowaniu głównym, a to ze względu na brak spójności między pkt 155 i 168 wyroku 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). Tak więc zdaniem sądu odsyłającego wyrok ten nie rozwiewa niepewności co do kwestii tego, czy w przypadku zatrzymywania adresów IP Trybunał ustanawia wymóg istnienia uzasadnionego powodu tego zatrzymywania, który byłby związany z celem ochrony bezpieczeństwa narodowego, zwalczania poważnej przestępczości lub zapobiegania poważnym zagrożeniom bezpieczeństwa publicznego, jak ma to wynikać z pkt 168 tego wyroku, czy też takie zatrzymywanie adresów IP jest dozwolone nawet w braku uzasadnionych powodów, ponieważ to wykorzystywanie zatrzymywanych danych jest ograniczone do przypadków, gdy jest dokonywane w tych właśnie celach, jak wynika z pkt 155 tego wyroku.

W przedmiocie pytania prejudycjalnego

47 Zadając swe pytanie prejudycjalne, sąd odsyłający dąży w istocie do ustalenia, czy art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 6–8 i 11 oraz art. 52 ust. 1 karty oraz art. 4 ust. 2 TUE należy interpretować w ten sposób, że sprzeczny z nim jest krajowy środek prawny, który, aby zapewnić realizację celów wymienionych w art. 15 ust. 1 tej dyrektywy, w szczególności tych polegających na ściganiu poważnych przestępstw lub zapobieganiu konkretnemu zagrożeniu dla bezpieczeństwa narodowego, nakłada, poza pewnymi wyjątkami, na dostawców ogólnie dostępnych usług łączności elektronicznej obowiązek uogólnionego i niezróżnicowanego zatrzymywania istotnych danych o ruchu oraz tych dotyczących lokalizacji użytkowników końcowych tych usług, przewidując w tym względzie kilkutygodniowy okres zatrzymywania, a także ustanawiając zasady

mające na celu zapewnienie zatrzymywanym danym skutecznej ochrony przed prawdopodobieństwem nadużyć, jak również przed uzyskaniem nieuprawnionego dostępu do tych danych.

W przedmiocie możliwości zastosowania dyrektywy 2002/58

48 Co się tyczy argumentacji podnoszonej przez Irlandię oraz rządy francuski, niderlandzki, polski i szwedzki, zgodnie z którą przepisy krajowe rozpatrywane w postępowaniu głównym, ze względu na to, że zostały przyjęte w szczególności w celu ochrony bezpieczeństwa narodowego, nie są objęte zakresem stosowania dyrektywy 2002/58, wystarczy przypomnieć, że uregulowanie krajowe nakładające na dostawców usług łączności elektronicznej obowiązek zatrzymywania danych o ruchu i danych dotyczących lokalizacji dla celów ochrony bezpieczeństwa narodowego i zwalczania przestępczości, takie jak rozpatrywane w postępowaniu głównym, jest objęte zakresem stosowania dyrektywy 2002/58 (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 104).

W przedmiocie wykładni art. 15 ust. 1 dyrektywy 2002/58

Przypomnienie zasad wynikających z orzecznictwa Trybunału

49 Zgodnie z utrwalonym orzecznictwem przy dokonywaniu wykładni przepisu prawa Unii należy uwzględniać nie tylko jego brzmienie, lecz także jego kontekst oraz cele aktu prawnego, którego jest on częścią, oraz w szczególności genezę tego uregulowania (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 32 i przytoczone tam orzecznictwo).

50 Z samego brzmienia art. 15 ust. 1 dyrektywy 2002/58 wynika, że środki ustawodawcze, do których przyjmowania upoważnia państwa członkowskie ta dyrektywa na określonych w niej warunkach, mogą mieć jedynie na celu „ograniczeni[e] zakresu" praw i obowiązków przewidzianych między innymi w art. 5, 6 i 9 dyrektywy 2002/58 (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 33).

51 W odniesieniu do systemu ustanowionego przez tę dyrektywę, w który wpisuje się także art. 15 ust. 1 tej dyrektywy, należy przypomnieć, że na podstawie art. 5 ust. 1 zdania pierwsze i drugie wspomnianej dyrektywy państwa członkowskie są zobowiązane zapewnić, 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 ciąży na nich zobowiązanie do zakazania 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, chyba że osoby te są do tego upoważnione przez prawo zgodnie z art. 15 ust. 1 tej samej dyrektywy (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 34).

52 W tym względzie Trybunał rozstrzygnął już, że w art. 5 ust. 1 dyrektywy 2002/58 ustanowiono zasadę poufności zarówno łączności elektronicznej, jak i związanych z nią danych o ruchu, co oznacza w szczególności zakaz – nałożony co do zasady na każdą osobę inną niż użytkownicy – zatrzymywania tych komunikatów i tych danych bez ich zgody (wyroki: 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 107; a także z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 35).

53 Przepis ten odzwierciedla cel, który przyświecał prawodawcy Unii przy wydawaniu dyrektywy 2002/58. Z uzasadnienia wniosku odnoszącego się do dyrektywy Parlamentu Europejskiego i Rady dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej [COM(2000) 385 wersja ostateczna], leżącego u podstaw dyrektywy 2002/58, wynika bowiem, że prawodawca Unii zamierzał „zapewnić, aby wysoki poziom ochrony danych osobowych i życia prywatnego był nadal zagwarantowany w odniesieniu do wszystkich usług łączności elektronicznej, bez względu na zastosowaną technologię". Wspomniana dyrektywa ma zatem na celu, jak wynika w szczególności z jej motywów 6 i 7, ochronę użytkowników usług łączności elektronicznej przed zagrożeniami wynikającymi dla ich danych osobowych i ich życia prywatnego z nowych technologii, a w szczególności ze zwiększonej zdolności do automatycznego przechowywania i przetwarzania danych. W szczególności, jak wskazuje motyw 2 tej dyrektywy, wolą prawodawcy Unii jest zapewnienie pełnego poszanowania praw określonych w art. 7 i 8 karty, dotyczących, odpowiednio, ochrony życia prywatnego oraz ochrony danych osobowych (zob. podobnie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 36 i przytoczone tam orzecznictwo).

54 Przyjmując dyrektywę 2002/58, prawodawca Unii skonkretyzował zatem te prawa w taki sposób, że użytkownicy środków łączności elektronicznej mają prawo co do zasady oczekiwać, że ich komunikacja i związane z nią dane pozostaną anonimowe i nie będą mogły być rejestrowane bez ich zgody (wyroki: 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 109; a także z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 37).

55 Jeśli chodzi o przetwarzanie i przechowywanie przez dostawców usług łączności elektronicznej danych o ruchu dotyczących abonentów i użytkowników, w art. 6 ust. 1 dyrektywy 2002/58 przewidziano, że dane te muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu, zaś w ust. 2 tego artykułu uściślono, że dane o ruchu, które są niezbędne do celów naliczania opłat abonenta i opłat rozliczeń międzyoperatorskich, można przetwarzać tylko do końca okresu, w którym rachunek może być zgodnie z prawem zakwestionowany lub w którym można dochodzić zapłaty. W odniesieniu do danych dotyczących lokalizacji innych niż dane o ruchu w art. 9 ust. 1 rzeczonej dyrektywy przewidziano, że dane te mogą być przetwarzane wyłącznie po spełnieniu pewnych warunków i po ich anonimizacji lub za zgodą użytkowników lub abonentów.

56 Wobec tego dyrektywa 2002/58 nie ogranicza się do określenia ram dostępu do takich danych za pomocą gwarancji mających na celu zapobieganie nadużyciom, ale także ustanawia w szczególności zasadę zakazu ich przechowywania przez osoby trzecie (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 39).

57 W zakresie, w jakim art. 15 ust. 1 dyrektywy 2002/58 pozwala państwom członkowskim przyjmować środki ustawodawcze mające na celu „ograniczeni[e] zakresu" praw i obowiązków przewidzianych w szczególności w art. 5, 6 i 9 tej dyrektywy, wynikających z zasad poufności komunikacji i zakazu przechowania związanych z nią danych, przypomnianych w pkt 52 niniejszego wyroku, przepis ten ustanawia wyjątek od ogólnej reguły przewidzianej w szczególności w tych art. 5, 6 i 9 i powinien w konsekwencji – zgodnie z utrwalonym orzecznictwem – być interpretowany ściśle. Taki przepis nie może zatem uzasadniać uczynienia

reguły z odstępstwa od tego mającego zasadnicze znaczenie obowiązku zapewnienia poufności łączności elektronicznej i danych z nią związanych, a szczególności od zakazu przechowywania tych danych, ustanowionego w art. 5 tej dyrektywy, gdyż w znacznym stopniu pozbawiłoby to 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 i przytoczone tam orzecznictwo).

58 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 i przytoczone tam orzecznictwo).

59 Ponadto z art. 15 ust. 1 zdanie trzecie dyrektywy 2002/58 wynika, że środki ustawodawcze przyjmowane przez państwa członkowskie na podstawie tego przepisu muszą być zgodne z zasadami ogólnymi prawa Unii, do których należy zasada proporcjonalności, i zapewniać poszanowanie praw podstawowych gwarantowanych w karcie. W tym względzie Trybunał orzekł już, że nałożony przez państwo członkowskie na dostawców usług łączności elektronicznej w przepisach krajowych obowiązek zatrzymywania danych o ruchu w celu udzielenia właściwym organom krajowym dostępu do nich w razie potrzeby budzi wątpliwości co do zgodności nie tylko z art. 7 i 8 karty, lecz również z art. 11 karty, dotyczącym wolności wypowiedzi, ponieważ to prawo podstawowe jest jednym z istotnych fundamentów pluralistycznego i demokratycznego społeczeństwa, stanowiąc część wartości, na jakich zgodnie z art. 2 TUE opiera się Unia Europejska (zob. podobnie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 42, 43 i przytoczone tam orzecznictwo).

60 Należy uściślić w tym względzie, że zatrzymywanie danych o ruchu i danych dotyczących lokalizacji stanowi samo w sobie z jednej strony odstępstwo od przewidzianego w art. 5 ust. 1 dyrektywy 2002/58 zakazu przechowywania tych danych przez inne osoby niż użytkownicy, a z drugiej strony ingerencję w prawa podstawowe do poszanowania życia prywatnego i do ochrony danych osobowych, o których mowa w art. 7 i 8 karty, bez względu na to, czy rozpatrywane informacje dotyczące życia prywatnego są danymi szczególnie chronionymi, czy nie, ani czy osoby, których dane dotyczą, ucierpiały z powodu ewentualnych niedogodności wynikających z tej ingerencji, jak również bez względu na to, czy zatrzymane dane są następnie wykorzystywane (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 44 i przytoczone tam orzecznictwo).

61 Wniosek ten jest uzasadniony tym bardziej, że dane o ruchu i dane dotyczących lokalizacji mogą ujawnić informacje o wielu aspektach życia prywatnego osób, których dane dotyczą, w tym informacje newralgiczne, takie jak orientacja seksualna, poglądy polityczne, przekonania religijne, filozoficzne, społeczne lub inne, jak również stan zdrowia, podczas gdy takie dane korzystają ponadto ze szczególnej ochrony w prawie Unii. Całokształt omawianych danych umożliwia wyciągnięcie bardzo precyzyjnych wniosków dotyczących życia prywatnego osób, których dane są zatrzymywane, takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazyjnie pokonywane trasy, prowadzona działalność, relacje towarzyskie tych osób i środowiska społeczne, w których osoby te się obracają. W szczególności dane te dają możność ustalenia profilu danych osób, która to informacja jest z punktu widzenia prawa do poszanowania życia prywatnego równie newralgiczna co sama treść komunikatów (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 45 i przytoczone tam orzecznictwo).

62 W związku z tym, po pierwsze, zatrzymywanie danych o ruchu i danych dotyczących lokalizacji w celach policyjnych może samo w sobie naruszać prawo do poszanowania komunikowania się, ustanowione w art. 7 karty, i wpłynąć zniechęcająco na wykonywanie przez użytkowników środków łączności elektronicznej ich wolności wypowiedzi zagwarantowanej w jej art. 11, zaś skutki te są tym dotkliwsze, że zatrzymywane dane są bardzo obszerne i zróżnicowane. Po drugie, biorąc pod uwagę okoliczność, że znaczna liczba danych o ruchu i danych dotyczących lokalizacji może być zatrzymywana w sposób ciągły przy użyciu środka uogólnionego i niezróżnicowanego zatrzymywania oraz że informacje wynikające z tych danych są szczególnie chronione, samo zatrzymywanie omawianych danych przez dostawców usług łączności elektronicznej grozi nadużyciem i nieuprawnionym dostępem (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 46 i przytoczone tam orzecznictwo).

63 Niemniej jednak, w zakresie, w jakim art. 15 ust. 1 dyrektywy 2002/58 pozwala państwom członkowskim na ograniczenie praw i obowiązków, o których mowa w pkt 51–54 niniejszego wyroku, odzwierciedla on okoliczność, że prawa ustanowione w art. 7, 8 i 11 karty nie wydają się stanowić prerogatyw o charakterze absolutnym, lecz należy je rozważać z uwzględnieniem ich funkcji społecznej. Jak bowiem wynika z art. 52 ust. 1 karty, dopuszcza ona ograniczenia wykonywania tych praw, o ile ograniczenia te są przewidziane ustawą, szanują istotę omawianych praw oraz – z zastrzeżeniem zasady proporcjonalności – są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. A zatem wykładnia art. 15 ust. 1 dyrektywy 2002/58 w świetle karty wymaga uwzględnienia również znaczenia praw ustanowionych w art. 3, 4, 6 i 7 karty oraz znaczenia, jakie mają cele ochrony bezpieczeństwa narodowego i walki z poważną przestępczością, przyczyniające się do ochrony praw i wolności innych osób (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 48 i przytoczone tam orzecznictwo).

64 Natomiast jeśli chodzi w szczególności o skuteczną walkę z przestępstwami, których ofiarami są zwłaszcza małoletni i inne osoby podatne na zagrożenia, należy uwzględnić okoliczność, że z art. 7 karty mogą wynikać pozytywne obowiązki przyjęcia przez organy publiczne środków prawnych w celu ochrony życia prywatnego i rodzinnego. Takie obowiązki mogą również wynikać ze wspomnianego art. 7 w zakresie ochrony domu i komunikowania się, a także z art. 3 i 4 w odniesieniu do ochrony integralności fizycznej i psychicznej osób, jak również zakazu tortur i nieludzkiego lub poniżającego traktowania (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 49 i przytoczone tam orzecznictwo).

65 W obliczu tych różnych pozytywnych obowiązków należy zatem pogodzić ze sobą różne wchodzące w rachubę uzasadnione interesy i prawa oraz ustanowić umożliwiające to pogodzenie ramy prawne (zob. podobnie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 50 i przytoczone tam orzecznictwo).

66 W tych ramach z samego brzmienia art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 wynika, że państwa członkowskie mogą uchwalić środek stanowiący odstępstwo od zasady poufności komunikacji wspomnianej w pkt 52 niniejszego wyroku, gdy taki środek jest „niezbędny, właściwy i proporcjonalny w ramach społeczeństwa demokratycznego”, podczas gdy motyw 11 tej dyrektywy wskazuje w tym względzie, iż środek tego rodzaju musi być „ściśle” proporcjonalny do zamierzonego celu.

67 W tym względzie należy przypomnieć, że ochrona prawa podstawowego do poszanowania życia prywatnego zgodnie z utrwalonym orzecznictwem Trybunału wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia mieściły się w ramach tego, co ściśle niezbędne.

Ponadto nie można dążyć do celu interesu ogólnego bez uwzględnienia okoliczności, że należy pogodzić go z prawami podstawowymi, których dotyczy środek, dokonując zbilansowanego wyważenia między celem interesu ogólnego z jednej strony a rozpatrywanymi prawami z drugiej strony (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 52 i przytoczone tam orzecznictwo).

68 Konkretniej rzecz ujmując, z orzecznictwa Trybunału wynika, że możliwość uzasadnienia przez państwa członkowskie ograniczenia praw i obowiązków przewidzianych w szczególności w art. 5, 6 i 9 dyrektywy 2002/58 należy oceniać, badając wagę ingerencji, jaką stanowi takie ograniczenie, oraz sprawdzając, czy znaczenie celu interesu ogólnego, do którego zmierza to ograniczenie, pozostaje w relacji do tej wagi (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 53 i przytoczone tam orzecznictwo).

69 Aby spełniać wymóg proporcjonalności, uregulowanie krajowe musi zawierać jasne i precyzyjne przepisy regulujące zakres i sposób stosowania rozpatrywanego środka oraz ustanawiające minimalne wymogi służące temu, aby osoby, o których dane osobowe chodzi, miały wystarczające gwarancje pozwalające na skuteczną ochronę tych danych przed prawdopodobieństwem dopuszczenia się nadużyć. Uregulowanie to musi być prawnie wiążące w prawie wewnętrznym i w szczególności wskazywać, w jakich okolicznościach i pod jakimi warunkami można przyjąć środek przewidujący przetwarzanie takich danych, gwarantując w ten sposób, że ingerencja zostanie ograniczona do tego, co ściśle niezbędne. Konieczność dysponowania takimi gwarancjami jest tym istotniejsza w sytuacji, gdy dane osobowe podlegają automatycznemu przetwarzaniu, w szczególności kiedy występuje znaczne ryzyko nieuprawnionego dostępu do tych danych. Rozważania te dotyczą zwłaszcza sytuacji, gdy w grę wchodzi ochrona tej szczególnej kategorii danych osobowych, jakimi są dane szczególnie chronione (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 54 i przytoczone tam orzecznictwo).

70 Zatem uregulowanie krajowe przewidujące zatrzymywanie danych osobowych powinno zawsze spełniać obiektywne kryteria wykazujące związek między danymi podlegającymi zatrzymaniu a zamierzonym celem (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 55 i przytoczone tam orzecznictwo).

71 Jeśli chodzi o cele interesu ogólnego mogące uzasadniać środek przyjęty na podstawie art. 15 ust. 1 dyrektywy 2002/58, z orzecznictwa Trybunału, w szczególności z wyroku 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) 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).

72 Tak więc jeśli chodzi o cel polegający na ochronie bezpieczeństwa narodowego, który przewyższa znaczeniem inne cele, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, Trybunał uznał, że przepis ten, w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, nie stoi na przeszkodzie przepisom ustawodawczym umożliwiającym, w celu ochrony bezpieczeństwa narodowego, posłużenie się skierowanym do dostawców usług łączności elektronicznej nakazem 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, przy czym decyzja o wydaniu takiego nakazu może być przedmiotem skutecznej kontroli sądu lub

niezależnego organu administracyjnego, którego decyzja wywiera wiążący skutek, mającej na celu weryfikację występowania jednej z takich sytuacji oraz poszanowania warunków i gwarancji, które powinny zostać przewidziane, zaś wspomniany nakaz można wydać jedynie na określony czas, ograniczony do tego, co ściśle niezbędne, jednak z możliwością przedłużenia w przypadku utrzymywania się tego zagrożenia (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 58 i przytoczone tam orzecznictwo).

73 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 dotyczących lokalizacji. A zatem jedynie ingerencje we wspomniane prawa podstawowe, które nie mają poważnego charakteru, mogą być uzasadnione celem polegającym 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).

74 W odniesieniu do celu polegającego na zwalczaniu poważnej przestępczości Trybunał orzekł już, że uregulowanie krajowe przewidujące w związku z tym uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych dotyczących lokalizacji wykracza poza granice tego, co absolutnie niezbędne, i nie może być uważane za uzasadnione w społeczeństwie demokratycznym. Z uwagi bowiem na to, że informacje mogące wynikać z danych o ruchu i danych dotyczących lokalizacji są szczególnie chronione, ich poufność ma zasadnicze znaczenie dla prawa do poszanowania życia prywatnego. A zatem, z uwagi na, po pierwsze, zniechęcający wpływ na wykonywanie praw podstawowych ustanowionych w art. 7 i 11 karty, o którym mowa w pkt 62 niniejszego wyroku, jaki może wywrzeć zatrzymywanie tych danych, a po drugie, wagę ingerencji, jaką pociąga za sobą takie zatrzymywanie, w społeczeństwie demokratycznym ważne jest, jak przewiduje system ustanowiony przez dyrektywę 2002/58, aby było ono wyjątkiem, a nie regułą, i aby dane te nie mogły być zatrzymywane w sposób systemowy i stały. Wniosek ten nasuwa się nawet z uwzględnieniem celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego oraz wagi, jaką należy im nadać (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 65 i przytoczone tam orzecznictwo).

75 Natomiast Trybunał uściślił, że wspomniany art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty nie stoi na przeszkodzie środkom ustawodawczym przewidującym, do 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, w okresie ograniczonym 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 (*quick freeze*) przez określony czas danych o ruchu i danych dotyczących lokalizacji, którymi dysponują ci dostawcy usług,

jeśli środki te zawierają jasne i precyzyjne przepisy zapewniające, że rozpatrywane zatrzymywanie danych jest uzależnione od spełnienia związanych z nim materialnych i proceduralnych warunków oraz że osoby, których dane dotyczą, dysponują skutecznymi gwarancjami chroniącymi przed prawdopodobieństwem popełnienia nadużyć (wyroki: 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 168; a także z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258 , pkt 67).

W przedmiocie środka przewidującego uogólnione i niezróżnicowane zatrzymywanie przez kilkutygodniowy okres większości danych o ruchu i danych dotyczących lokalizacji

76 To właśnie w świetle tych mających zasadnicze znaczenie względów należy zbadać te cechy charakterystyczne rozpatrywanego w postępowaniu głównym uregulowania krajowego, na które zwrócił uwagę sąd odsyłający.

77 W pierwszej kolejności, jeśli chodzi o zakres zatrzymywanych danych, z postanowienia odsyłającego wynika, że, w ramach świadczenia usług telefonicznych, przewidziany w tym uregulowaniu 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.

78 Choć zgodnie z rozpatrywanym w postępowaniu głównym uregulowaniem krajowym z obowiązku zatrzymywania wyłączone są treść komunikatu i dane dotyczące przeglądanych stron internetowych, zaś obowiązek zatrzymania identyfikatora komórki dotyczy jedynie początku połączenia, należy jednak zauważyć, że to samo miało w istocie miejsce w przypadku transponujących dyrektywę 2006/24 przepisów krajowych, w przedmiocie których wydano 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). Pomimo istnienia tych ograniczeń Trybunał orzekł zaś w tym wyroku, że kategorie danych zatrzymywanych na podstawie wspomnianej dyrektywy i uregulowań krajowych mogą rzeczywiście pozwolić na wyciągnięcie precyzyjnych, a nawet bardzo precyzyjnych wniosków 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 towarzyskie i środowiska społeczne, w których osoby te się obracają i, w szczególności, na umożliwienie ustalenia profilu tych osób.

79 Należy ponadto stwierdzić, że chociaż rozpatrywane w postępowaniu głównym uregulowanie nie obejmuje danych dotyczących przeglądanych stron internetowych, to jednak przewiduje ono zatrzymywanie adresów IP. Skoro zaś adresy IP mogą być wykorzystywane w szczególności do wyczerpującego prześledzenia poruszania się internauty w sieci i, w konsekwencji, jego działalności on-line, dane te pozwalają na ustalenie jego szczegółowego profilu. Tak więc zatrzymywanie i analizowanie wspomnianych adresów IP, jakiego wymaga takie śledzenie, stanowi poważną ingerencję w prawa podstawowe internauty ustanowione w art. 7 i 8 karty (zob. podobnie 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 153).

80 Ponadto, jak zauważyła SpaceNet w uwagach na piśmie, dane dotyczące usług poczty elektronicznej, które nie są objęte obowiązkiem zatrzymywania przewidzianym w uregulowaniu rozpatrywanym w postępowaniu głównym, stanowią jedynie niewielką część rozpatrywanych danych.

81 Jak zatem zauważył w istocie rzecznik generalny w pkt 60 opinii, przewidziany w uregulowaniu krajowym rozpatrywanym w postępowaniu głównym obowiązek zatrzymywania obejmuje bardzo duży zbiór danych o ruchu i danych dotyczących lokalizacji, który odpowiada w istocie tym danym, w przedmiocie których wydano wyroki składające się na utrwalone orzecznictwo przypomniane w pkt 78 niniejszego wyroku.

82 Ponadto, w odpowiedzi na pytanie zadane na rozprawie, rząd niemiecki wyjaśnił, że do wykazu osób, organów lub organizacji o charakterze społecznym lub religijnym, których dane związane z łącznością elektroniczną nie są zatrzymywane na mocy art. 99 ust. 2 i § 113b ust. 6 TKG zostało wpisanych jedynie 1300 podmiotów, co w oczywisty sposób stanowi niewielką część zbioru wszystkich użytkowników usług telekomunikacyjnych w Niemczech, których dane objęte są obowiązkiem zatrzymywania przewidzianym w będącym przedmiotem postępowania przed sądem krajowym uregulowaniu. W szczególności zaś zatrzymywane są dane użytkowników objętych tajemnicą zawodową, takich jak adwokaci, lekarze i dziennikarze.

83 Z postanowienia odsyłającego wynika zatem, że przewidziane w tym uregulowaniu krajowym zatrzymywanie danych o ruchu i danych dotyczących lokalizacji dotyczy niemal wszystkich osób składających się na populację, nawet wtedy, gdy nie ma wobec nich żadnych podstaw, nawet pośrednich, do wszczęcia postępowania karnego. Podobnie w uregulowaniu tym ustanowiony został wymóg zatrzymywania bez uzasadnionego powodu, w uogólniony i niezróżnicowany z punktu widzenia osobowego, czasowego i geograficznego, istotnych danych o ruchu i danych dotyczących lokalizacji, których zakres odpowiada w istocie zakresowi danych zatrzymywanych w sprawach, w których wydano wyrok składający się na orzecznictwo, o którym mowa w pkt 78 niniejszego wyroku.

84 W związku z tym, ze względu na orzecznictwo przytoczone w pkt 75 niniejszego wyroku i wbrew temu, co twierdzi rząd niemiecki, obowiązek zatrzymywania danych taki jak ten rozpatrywany w postępowaniu głównym nie może zostać uznany za ukierunkowane zatrzymywanie danych.

85 W drugiej kolejności, w odniesieniu do okresu zatrzymywania danych, z art. 15 ust. 1 zdanie drugie dyrektywy 2002/58 wynika, że okres przechowywania przewidziany w środku krajowym ustanawiającym obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych jest niewątpliwie jednym z istotnych czynników służących ustaleniu tego, czy taki środek jest sprzeczny z prawem Unii, ponieważ wspomniane zdanie ustanawia wymóg, aby okres ten był „określony”.

86 Prawdą jest, że w niniejszej sprawie okresy te, które, zgodnie z § 113b ust. 1 TKG wynoszą cztery tygodnie w przypadku danych dotyczących lokalizacji oraz dziesięć tygodni w przypadku innych danych, są znacznie krótsze niż te przewidziane w przepisach krajowych formułujących obowiązek ogólnego i niezróżnicowanego zatrzymywania danych, które zostały przeanalizowane przez Trybunał w wyrokach z dnia 21 grudnia 2016 r., Tele2 Sverige oraz Watson i in. (C-203/15 i C-698/15, EU:C:2016:970), 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); a także z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in. (C-140/20, EU:C:2022:258).

87 Jednakże jak wynika z orzecznictwa przytoczonego w pkt 61 niniejszego wyroku, waga ingerencji wynika z prawdopodobieństwa, że zatrzymywane dane, w szczególności ze względu na ich ilość i różnorodność, rozpatrywane jako całość, pozwalają na wyciągnięcie bardzo precyzyjnych wniosków dotyczących życia prywatnego osoby lub osób, których dane zostały zatrzymane, a w szczególności dostarczają środków pozwalających na ustalenie profilu osoby lub osób, których dane dotyczą, która to informacja jest z punktu widzenia prawa do poszanowania życia prywatnego równie newralgiczna co sama treść komunikatów.

88 Tak więc zatrzymywanie danych o ruchu lub danych dotyczących lokalizacji, które mogą dostarczyć informacji na temat połączeń wykonywanych przez użytkownika środka łączności elektronicznej lub lokalizacji używanych przez niego urządzeń końcowych, ma w każdym wypadku poważny charakter, niezależnie od długości okresu, na jaki te dane są zatrzymywane, oraz od ilości lub rodzaju zatrzymywanych danych, jeżeli ten zbiór danych może pozwolić na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego osoby lub osób, których dane dotyczą [zob. odnośnie do dostępu do takich danych wyrok z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C-746/18, EU:C:2021:152, pkt 39].

89 W tym względzie nawet zatrzymywanie ograniczonej ilości danych o ruchu lub danych dotyczących lokalizacji lub zatrzymywanie tych danych na krótki okres może dostarczyć dokładnych informacji na temat życia prywatnego użytkownika środka łączności elektronicznej. Ponadto ilość dostępnych danych i wynikające z nich konkretne informacje na temat życia prywatnego osoby, której dane dotyczą, są okolicznościami, które można ocenić dopiero po zapoznaniu się ze wspomnianymi danymi. Ingerencja wynikająca z zatrzymywania takich danych ma siłą rzeczy miejsce przed zapoznaniem się z tymi danymi i wynikającymi z nich informacjami. Ocena wagi ingerencji, jaką stanowi takie zatrzymywanie danych, musi być zatem dokonywana w oparciu o ryzyko dla życia prywatnego zainteresowanych osób, które jest ogólnie związane z kategorią zatrzymywanych danych, przy czym nie ma ponadto znaczenia, czy wynikające z nich informacje dotyczące życia prywatnego mają, konkretnie rzecz biorąc, poufny charakter, czy też nie [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 40].

90 W niniejszym przypadku, jak wynika z pkt 77 niniejszego wyroku i co zostało potwierdzone na rozprawie, całościowy zbiór danych o ruchu lub danych dotyczących lokalizacji, zatrzymywanych, odpowiednio, na dziesięć tygodni i na cztery tygodnie, może bowiem 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.

91 W trzeciej kolejności, jeśli chodzi o gwarancje przewidziane w uregulowaniu krajowym rozpatrywanym w postępowaniu głównym mające na celu ochronę zatrzymywanych danych przed prawdopodobieństwem zaistnienia nadużyć i przed udzieleniem jakiegokolwiek bezprawnego dostępu do nich, należy zauważyć, że zatrzymywanie tych danych i dostęp do nich stanowią – jak wynika z orzecznictwa przypomnianego w pkt 60 niniejszego wyroku – odrębne ingerencje w prawa podstawowe zagwarantowane w art. 7 i 11 karty, z których każda wymaga odrębnego uzasadnienia na podstawie art. 52 ust. 1 karty. Wynika stąd, że przepisy krajowe zapewniające pełne poszanowanie warunków wynikających z orzecznictwa, w którym dokonano wykładni dyrektywy 2002/58 w dziedzinie dostępu do zatrzymanych danych, nie mogą jako takie ani ograniczyć, ani zaradzić poważnej ingerencji, która wynikałaby z uogólnionego zatrzymywania tych danych przewidzianego w tych przepisach krajowych, w prawa zagwarantowane w art. 5 i 6 tej dyrektywy oraz prawa podstawowe, których te artykuły stanowią konkretyzację (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 47).

92 W czwartej i ostatniej kolejności, jeśli chodzi o argument Komisji Europejskiej, zgodnie z którym szczególnie poważna przestępczość mogłaby zostać zrównana z zagrożeniem dla bezpieczeństwa narodowego, Trybunał orzekł już, że cel ochrony bezpieczeństwa narodowego odpowiada nadrzędnemu interesowi polegającemu na ochronie podstawowych funkcji państwa i podstawowych interesów społeczeństwa, poprzez zapobieganie i ściganie działalności mogącej poważnie zdestabilizować podstawowe struktury konstytucyjne, polityczne lub społeczne kraju, w szczególności bezpośrednio zagrozić społeczeństwu, ludności lub państwu jako takiemu, zwłaszcza takiej jak działalność terrorystyczna (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 61 i przytoczone tam orzecznictwo).

93 W odróżnieniu od przestępczości, nawet szczególnie poważnej, zagrożenie dla bezpieczeństwa narodowego musi być rzeczywiste i aktualne lub przynajmniej przewidywalne, co zakłada wystąpienie wystarczająco konkretnych okoliczności, aby móc uzasadnić środek w postaci uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych dotyczących lokalizacji przez określony czas. Takie zagrożenie różni się zatem – ze względu na swój charakter, wagę i szczególny charakter składających się na nie okoliczności – od ogólnego i stałego ryzyka, jakim jest prawdopodobieństwowystąpienia napięć lub zakłóceń, nawet poważnych, dla bezpieczeństwa publicznego lub ryzyko poważnych przestępstw (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 62 i przytoczone tam orzecznictwo).

94 A zatem przestępczości, nawet szczególnie poważnej, nie można utożsamiać z zagrożeniem dla bezpieczeństwa narodowego. Takie utożsamienie mogłoby bowiem skutkować wprowadzeniem kategorii pośredniej między bezpieczeństwem narodowym a bezpieczeństwem publicznym w celu zastosowania do tego drugiego wymogów właściwych dla tego pierwszego (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 63).

W przedmiocie środków przewidujących zatrzymywanie ukierunkowane, zatrzymywanie szybkie lub zatrzymywanie adresów IP

95 Szereg rządów, w tym rząd francuski, podkreśliło, że jedynie uogólnione i niezróżnicowane zatrzymywanie umożliwia skuteczne osiągnięcie celów zamierzonych przez środki realizujące cel ochrony, podczas gdy rząd niemiecki w istocie wyjaśnił, że wniosku takiego nie podważa okoliczność, iż państwa członkowskie mogą stosować środki polegające na zatrzymywaniu ukierunkowanym i zatrzymywaniu szybkim, o których mowa w pkt 75 niniejszego wyroku.

96 W tym względzie w pierwszej kolejności należy zauważyć, że skuteczność ścigania karnego zależy zazwyczaj nie od jednego instrumentu dochodzeniowego, lecz od wszystkich instrumentów dochodzeniowych, jakimi dysponują właściwe organy krajowe w tym celu (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 69).

97 W drugiej kolejności – art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, zgodnie z jego wykładnią dokonaną w orzecznictwie przypomnianym w pkt 75 niniejszego wyroku, pozwala państwom członkowskim przyjmować – w celu zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego – nie tylko przepisy ustanawiające ukierunkowane zatrzymywanie i szybkie zatrzymywanie, ale także przepisy przewidujące uogólnione i niezróżnicowane zatrzymywanie, po pierwsze, danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej, a po drugie, adresów IP przypisanych do źródła połączenia (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 70).

98 W tym względzie jest bezsporne, że zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej może przyczynić się do zwalczania poważnej przestępczości, pod warunkiem że dane te pozwalają zidentyfikować osoby, które korzystały z takich środków w ramach przygotowywania lub popełnienia poważnego przestępstwa (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 71).

99 Otóż dyrektywa 2002/58 nie stoi na przeszkodzie uogólnionemu zatrzymywaniu danych dotyczących tożsamości cywilnej do celów ogólnego zwalczania przestępczości. W tych okolicznościach należy uściślić, że ani ta dyrektywa, ani żaden inny akt prawa Unii nie stoją na przeszkodzie uregulowaniu krajowemu mającemu na celu zwalczanie poważnej przestępczości, na podstawie którego nabycie środka łączności elektronicznej, takiego jak opłaconej z góry karty SIM, jest uzależnione od sprawdzenia urzędowych dokumentów ustalających tożsamość nabywcy i od zarejestrowania przez sprzedawcę wynikających z nich informacji, gdyż sprzedawca jest w stosownym wypadku zobowiązany do udzielenia dostępu do tych informacji właściwym organom krajowym (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 72).

100 Ponadto należy przypomnieć, że uogólnione zatrzymywanie adresów IP źródła połączenia stanowi poważną ingerencję w prawa podstawowe ustanowione w art. 7 i 8 karty, ponieważ te adresy IP mogą pozwolić na wyciągnięcie dokładnych wniosków na temat życia prywatnego użytkownika danego środka łączności elektronicznej, i może ono mieć zniechęcające skutki dla wykonywania prawa wolności wypowiedzi zagwarantowanego w art. 11 karty. Niemniej w odniesieniu do takiego zatrzymywania Trybunał stwierdził, że do celów wymaganego przez orzecznictwo koniecznego pogodzenia wchodzących w rachubę praw i uzasadnionych interesów, o którym mowa w pkt 65–68 niniejszego wyroku, należy uwzględnić okoliczność, iż w przypadku przestępstwa popełnionego w Internecie, zwłaszcza w przypadku nabywania, rozpowszechniania, przekazywania lub udostępniania w Internecie pornografii dziecięcej w rozumieniu art. 2 lit. c) dyrektywy Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującej decyzję ramową Rady 2004/68/WSiSW (Dz.U. 2011, L 335, s. 1, sprostowanie Dz.U. 2012, L 18, s. 7), adres IP może stanowić jedyny środek dochodzeniowy umożliwiający ustalenie tożsamości osoby, której adres ten był przypisany w chwili popełnienia tego przestępstwa (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 73).

101 W tych okolicznościach choć prawdą jest, że środek ustawodawczy przewidujący zatrzymywanie adresów IP wszystkich osób fizycznych będących właścicielami urządzeń końcowych, za pomocą których można uzyskać dostęp do Internetu, dotyczy osób, które na pierwszy rzut oka nie wykazują związku, w rozumieniu orzecznictwa przytoczonego w pkt 70 niniejszego wyroku, z realizowanymi celami i że internauci mają, zgodnie z tym, co zostało stwierdzone w pkt 54 niniejszego wyroku, prawo oczekiwać, na mocy art. 7 i 8 karty, że ich tożsamość nie będzie co do zasady ujawniana, środek ustawodawczy przewidujący uogólnione i niezróżnicowane zatrzymywanie jedynie adresów IP przypisanych do źródła połączenia nie wydaje się co do zasady sprzeczny z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, pod warunkiem że możliwość ta zostanie uzależniona od drobiazgowego spełnienia warunków materialnych i proceduralnych, które winny regulować wykorzystywanie tych danych (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 155).

102 Z uwagi na poważny charakter ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty, jaką pociąga za sobą to zatrzymywanie, jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniom dla bezpieczeństwa publicznego mogą, podobnie jak ochrona bezpieczeństwa narodowego, uzasadniać tę ingerencję. Ponadto okres zatrzymywania nie może przekraczać okresu ściśle niezbędnego w świetle zamierzonego celu. Wreszcie środek tego rodzaju powinien przewidywać ścisłe warunki i gwarancje dotyczące wykorzystywania tych danych, w szczególności do śledzenia komunikacji i działalności w Internecie prowadzonej przez osoby, których dane dotyczą (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 156).

103 W ten sposób, wbrew temu, co podkreślił sąd odsyłający, między pkt 155 a pkt 168 wyroku 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) nie ma sprzeczności. Jak bowiem wskazał w istocie rzecznik generalny w pkt 81 i 82 opinii, z owego pkt 155 w związku z pkt 156 i pkt 168 tego wyroku jasno wynika, że jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniom bezpieczeństwa publicznego mogą, podobnie jak ochrona bezpieczeństwa narodowego, uzasadniać uogólnione zatrzymywanie adresów IP przypisanych do źródła połączenia, niezależnie od tego, czy osoby, których dane dotyczą, mogą mieć co najmniej pośredni związek z realizowanymi celami.

104 W trzeciej kolejności, jeśli chodzi o środki ustawodawcze przewidujące ukierunkowane zatrzymywanie i szybkie zatrzymywanie danych o ruchu i danych dotyczących lokalizacji, niektóre względy przedstawione przez państwa członkowskie w odniesieniu do takich środków świadczą o węższym zrozumieniu zakresu tych środków niż zakres przyjęty w orzecznictwie przypomnianym w pkt 75 niniejszego wyroku. Choć bowiem zgodnie z tym, co zostało przypomniane w pkt 57 niniejszego wyroku, te polegające na zatrzymywaniu środki powinny mieć charakter odstępstwa w systemie ustanowionym w dyrektywie 2002/58, to dyrektywa ta jednak, interpretowana w świetle praw podstawowych ustanowionych w art. 7, 8 i 11 oraz art. 52 ust. 1 karty, nie uzależnia możliwości wydania nakazu przewidującego ukierunkowane zatrzymywanie od warunku, by miejsca mogące być sceną poważnych przestępstw oraz osoby podejrzane o udział w takim przestępstwie były z góry znane. Podobnie dyrektywa ta nie ustanawia wymogu, by nakaz przewidujący szybkie zatrzymywanie był ograniczony do podejrzanych zidentyfikowanych przed wydaniem takiego nakazu (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 75).

105 Po pierwsze, jeśli chodzi o ukierunkowane zatrzymywanie, Trybunał orzekł, że art. 15 ust. 1 dyrektywy 2002/58 nie stoi na przeszkodzie uregulowaniu krajowemu opartemu na obiektywnych elementach, umożliwiającemu objęcie – z jednej strony – osób, których dotyczące dane o ruchu i dane dotyczące lokalizacji mogą ujawnić związek, przynajmniej pośredni, z poważnymi przestępstwami, przyczynić się do zwalczania poważnej przestępczości lub zapobiegać poważnemu ryzyku dla bezpieczeństwa publicznego bądź ryzyku dla bezpieczeństwa narodowego (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 76 i przytoczone tam orzecznictwo).

106 Trybunał wyjaśnił w tym względzie, że chociaż te obiektywne elementy mogą się różnić w zależności od środków podjętych w celu zapobiegania poważnym przestępstwom, ich dochodzenia, wykrywania i ścigania, takie środki mogą obejmować w szczególności te osoby, które zostały wcześniej zidentyfikowane w ramach właściwych procedur krajowych oraz na podstawie obiektywnych i niedyskryminacyjnych przesłanek jako stwarzające zagrożenie dla bezpieczeństwa publicznego lub bezpieczeństwa narodowego danego państwa członkowskiego (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 77).

107 Państwa członkowskie mają zatem w szczególności możliwość przyjmowania środków polegających na zatrzymywaniu danych odnoszących się do osób, które – tytułem takiej identyfikacji – są objęte dochodzeniem lub innymi aktualnymi środkami nadzoru lub wpisem w krajowym rejestrze karnym wspominającym o wcześniejszym skazaniu za poważne przestępstwa, mogącym oznaczać wysokie ryzyko recydywy. Gdy zaś taka identyfikacja opiera się na określonych przez prawo krajowe obiektywnych i niedyskryminacyjnych przesłankach, ukierunkowane zatrzymywanie danych obejmujące zidentyfikowane w ten sposób osoby jest uzasadnione (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 78).

108 Z drugiej strony środek polegający na ukierunkowanym zatrzymywaniu danych o ruchu i danych dotyczących lokalizacji może – zgodnie z wyborem ustawodawcy krajowego i w ścisłym poszanowaniu zasady proporcjonalności – być również oparty na kryterium geograficznym, jeżeli właściwe organy krajowe uznają, na podstawie obiektywnych i niedyskryminacyjnych przesłanek, że na jednym lub większej liczbie obszarów geograficznych istnieje wysokie ryzyko przygotowania lub popełnienia poważnych przestępstw. Obszarami tymi mogą być w szczególności miejsca charakteryzujące się dużą liczbą poważnych przestępstw, miejsca szczególnie narażone na popełnianie poważnych przestępstw, takie jak miejsca lub infrastruktura, w których regularnie przebywa bardzo wiele osób, lub też miejsca strategiczne, takie jak porty lotnicze, dworce, porty morskie lub strefy poboru opłat za przejazd (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 79 i przytoczone tam orzecznictwo).

109 Należy podkreślić, że zgodnie z tym orzecznictwem właściwe organy krajowe mogą przyjąć w odniesieniu do stref, o których mowa w poprzednim punkcie, środek polegający na ukierunkowanym zatrzymywaniu danych oparty na kryterium geograficznym, takim jak między innymi średni wskaźnik przestępczości w danej strefie geograficznej, przy czym nie muszą one koniecznie dysponować konkretnymi wskazówkami dotyczącymi przygotowywania lub popełniania w danych strefach poważnych przestępstw. Jako że ukierunkowane zatrzymywanie danych oparte na takim kryterium może objąć – w zależności od poważnych przestępstw, do których się ono odnosi, oraz sytuacji właściwej dla poszczególnych państw członkowskich – zarówno miejsca charakteryzujące się dużą liczbą poważnych przestępstw, jak i miejsca szczególnie narażone na popełnianie takich przestępstw, co do zasady nie może ono spowodować

dyskryminacji, gdyż kryterium oparte na średnim wskaźniku poważnej przestępczości nie ma samo w sobie żadnego związku z potencjalnie dyskryminacyjnymi przesłankami (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 80).

110 Ponadto środek polegający na ukierunkowanym zatrzymywaniu danych odnoszący się do miejsc lub infrastruktury, w których regularnie przebywa bardzo wiele osób, lub też do miejsc strategicznych, takich jak porty lotnicze, dworce, porty morskie lub strefy poboru opłat za przejazd, pozwala właściwym organom na gromadzenie danych o ruchu, a w szczególności danych dotyczących lokalizacji wszystkich osób, które w danym momencie korzystają ze środka łączności elektronicznej w jednym z tych miejsc. A zatem taki środek polegający na ukierunkowanym zatrzymywaniu danych może pozwolić wspomnianym organom na uzyskanie – poprzez dostęp do zatrzymanych w ten sposób danych – informacji na temat obecności tych osób w miejscach lub strefach geograficznych objętych tym środkiem oraz na temat tras pokonywanych między tymi miejscami lub strefami lub w ich obrębie oraz na wyciągnięcie, do celów zwalczania poważnej przestępczości, wniosków co do obecności i działalności owych osób w tych miejscach lub tych strefach geograficznych w danym momencie w okresie zatrzymywania danych (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 81).

111 Należy jeszcze zauważyć, że strefy geograficzne objęte takim ukierunkowanym zatrzymywaniem danych mogą – a w stosownym wypadku muszą – zostać zmodyfikowane, w zależności od zmiany warunków, które uzasadniały ich wybór, pozwalając tym samym reagować na zmiany w walce z poważną przestępczością. Trybunał orzekł już bowiem, że czas obowiązywania środków polegających na ukierunkowanym zatrzymywaniu danych, opisanych w pkt 105–110 niniejszego wyroku, nie może przekraczać okresu, który jest ściśle niezbędny w świetle zamierzonego celu oraz okoliczności je uzasadniających, bez uszczerbku dla ewentualnego jego przedłużenia ze względu na utrzymywanie się konieczności takiego zatrzymywania (wyroki 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 151; a także z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 82).

112 Jeśli chodzi o możliwość przewidzenia kryteriów odróżniających innych niż kryterium osobowe lub geograficzne w celu wprowadzenia w życie ukierunkowanego zatrzymywania danych o ruchu i danych dotyczących lokalizacji, nie można wykluczyć, że pod uwagę mogą zostać wzięte inne obiektywne i niedyskryminacyjne kryteria, aby zapewnić, by zakres ukierunkowanego zatrzymywania danych był ograniczony do tego, co jest ściśle niezbędne, oraz ustalić przynajmniej pośredni związek między poważnymi przestępstwami a osobami, których dane są zatrzymywane. Niemniej jednak ze względu na to, że art. 15 ust. 1 dyrektywy 2002/58 odnosi się do środków ustawodawczych państw członkowskich, to do tych państw, a nie do Trybunału należy ustalenie takich kryteriów, przy czym nie może być mowy o ponownym wprowadzeniu za pomocą tego środka uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych dotyczących lokalizacji (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 83).

113 W każdym wypadku, jak zauważył rzecznik generalny w pkt 50 opinii, ewentualne istnienie trudności w dokładnym określeniu przesłanek i warunków, na jakich można dokonać ukierunkowanego zatrzymywania danych, nie może uzasadniać wprowadzenia przez państwa członkowskie, w drodze przyjęcia wyjątku za regułę, uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych dotyczących lokalizacji (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 84).

114 Po drugie, w odniesieniu do szybkiego zatrzymywania danych o ruchu i danych dotyczących lokalizacji przetwarzanych i przechowywanych przez dostawców usług łączności elektronicznej na podstawie art. 5, 6 i 9 dyrektywy 2002/58 lub środków ustawodawczych przyjętych na podstawie art. 15 ust. 1 tej dyrektywy, należy przypomnieć, że takie dane powinny co do zasady zostać, w zależności od przypadku, usunięte lub zanonimizowane po upływie ustawowych terminów, w których zgodnie z krajowymi przepisami transponującymi ową dyrektywę powinno nastąpić ich przetwarzanie i przechowywanie. Jednak Trybunał rozstrzygnął, że podczas tego przetwarzania i tego przechowywania danych mogą występować sytuacje, w których występuje konieczność zatrzymywania rzeczonych danych po upływie tych terminów w celu wyjaśnienia poważnych przestępstw lub naruszeń bezpieczeństwa narodowego, i to zarówno w sytuacji, gdy te przestępstwa lub te naruszenia już zostały wykryte, jak i w sytuacji, w której, po przeprowadzeniu obiektywnego badania wszystkich istotnych okoliczności, można racjonalnie podejrzewać ich istnienie (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 85).

115 W takiej sytuacji, z uwagi na konieczność pogodzenia rozpatrywanych praw i uzasadnionych interesów, o której mowa w pkt 65–68 niniejszego wyroku, państwa członkowskie mogą przewidzieć w ustawodawstwie przyjętym na podstawie art. 15 ust. 1 dyrektywy 2002/58 możliwość nakazania dostawcom usług łączności elektronicznej, w drodze decyzji właściwego organu poddanej skutecznej kontroli sądowej, szybkiego zatrzymywania przez określony czas danych o ruchu i danych dotyczących lokalizacji, którymi oni dysponują (wyroki 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 163; a także z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 86).

116 Ponieważ cel takiego szybkiego zatrzymywania nie odpowiada już celom, dla których dane zostały pierwotnie zgromadzone i zatrzymane, a wszelkie przetwarzanie danych powinno na mocy art. 8 ust. 2 karty odpowiadać określonym celom, państwa członkowskie powinny określić w swoim ustawodawstwie cel, dla którego może nastąpić szybkie zatrzymywanie danych. Ze względu na poważny charakter ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty, jaką może stanowić takie zatrzymywanie, jedynie walka z poważną przestępczością i, a fortiori, ochrona bezpieczeństwa narodowego mogą uzasadniać tę ingerencję, pod warunkiem że ten środek oraz dostęp do zatrzymanych w ten sposób danych przestrzegają granic tego, co ściśle niezbędne, takich jak te wskazane w pkt 164–167 wyroku 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) (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 87).

117 Trybunał wyjaśnił, że tego rodzaju środek polegający na zatrzymywaniu danych nie powinien być ograniczony do danych osób zidentyfikowanych uprzednio jako stanowiące zagrożenie dla bezpieczeństwa publicznego lub bezpieczeństwa narodowego danego państwa członkowskiego lub osób konkretnie podejrzewanych o popełnienie poważnego przestępstwa lub naruszenie bezpieczeństwa narodowego. Zdaniem Trybunału taki środek, przy poszanowaniu ram ustanowionych w art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, może bowiem z uwagi na rozważania zawarte w pkt 70 niniejszego wyroku – zgodnie z wyborem ustawodawcy krajowego i przy poszanowaniu granic tego, co ściśle niezbędne – zostać rozszerzony na dane o ruchu i dane dotyczących lokalizacji dotyczące osób innych niż te, które są podejrzewane o planowanie lub popełnienie poważnego przestępstwa lub naruszenie bezpieczeństwa narodowego, o ile dane te mogą w oparciu o obiektywne i niedyskryminacyjne kryteria przyczynić się do wyjaśnienia takiego przestępstwa lub takiego naruszenia bezpieczeństwa narodowego, takie jak dane ofiary tego przestępstwa lub naruszenia, jej otoczenia

społecznego lub zawodowego (wyroki: 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 165; a także z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 88).

118 A zatem środek ustawodawczy może zezwalać na skorzystanie ze skierowanego do dostawców usług łączności elektronicznej nakazu dokonania szybkiego zatrzymania danych o ruchu i danych dotyczących lokalizacji, w szczególności osób, z którymi – przed wystąpieniem poważnego zagrożenia dla bezpieczeństwa publicznego lub popełnienia poważnego przestępstwa – ofiara była w kontakcie przy użyciu swoich środków łączności elektronicznej (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 89).

119 Takie szybkie zatrzymywanie danych może – zgodnie z orzecznictwem Trybunału przypomnianym w pkt 117 niniejszego wyroku oraz w takich warunkach, o jakich mowa w tym punkcie – także zostać rozszerzone na określone strefy geograficzne, takie jak miejsca popełnienia i przygotowania danego przestępstwa lub naruszenia bezpieczeństwa narodowego. Należy doprecyzować, że przedmiotem takiego środka mogą być również dane o ruchu i dane lokalizacji związane z miejscem, w którym osoba będąca potencjalnie ofiarą poważnego przestępstwa zaginęła, pod warunkiem że ten środek oraz dostęp do zatrzymanych w ten sposób danych nie przekraczają granic tego, co ściśle niezbędne do celów walki z poważną przestępczością lub ochrony bezpieczeństwa narodowego, takich jak granice wskazane w pkt 164–167 wyroku 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) (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 90).

120 Ponadto należy uściślić, że art. 15 ust. 1 dyrektywy 2002/58 nie stoi na przeszkodzie temu, by właściwe organy krajowe zarządziły środek polegający na szybkim zatrzymywaniu danych już na pierwszym etapie dochodzenia dotyczącego poważnego zagrożenia dla bezpieczeństwa publicznego lub ewentualnego poważnego przestępstwa, czyli w chwili, w której zgodnie z właściwymi przepisami prawa krajowego organy te mogą wszcząć takie dochodzenie (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 91).

121 W odniesieniu do różnorodności środków polegających na zatrzymywaniu danych o ruchu i danych dotyczących lokalizacji, o których mowa w pkt 75 niniejszego wyroku, należy uściślić, że te różnego rodzaju środki mogą – zgodnie z wyborem ustawodawcy krajowego i przy poszanowaniu granic tego, co ściśle niezbędne – znaleźć zastosowanie wspólnie. W tych okolicznościach art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, w wykładni nadanej mu w orzecznictwie wynikającym z wyroku 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) nie stoi na przeszkodzie połączeniu tych środków (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 92).

122 W czwartej i ostatniej kolejności należy podkreślić, że proporcjonalność środków przyjętych na podstawie art. 15 ust. 1 dyrektywy 2002/58 wymaga – zgodnie z utrwalonym orzecznictwem Trybunału, które zostało podsumowane w wyroku 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) – spełnienia nie tylko wymogów zdatności i konieczności, ale także wymogu odnoszącego się do proporcjonalnego charakteru tych środków w stosunku do zamierzonego celu (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 93).

123 W związku z tym należy przypomnieć, że w pkt 51 wyroku z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in. (C-293/12 i C-594/12, EU:C:2014:238) Trybunał orzekł, iż walka z poważną przestępczością ma wprawdzie pierwszorzędne znaczenie dla zagwarantowania bezpieczeństwa publicznego, zaś jej skuteczność może w znacznym stopniu zależeć od wykorzystania nowoczesnych technik dochodzeniowo-śledczych, jednak tego rodzaju cel interesu ogólnego, mimo że ma on fundamentalne znaczenie, nie może sam w sobie uzasadniać stwierdzenia, że środek polegający na uogólnionym i niezróżnicowanym zatrzymywaniu danych o ruchu i danych dotyczących lokalizacji, taki jak ten ustanowiony w dyrektywie 2006/24, miałby być konieczny (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 94).

124 Podążając za tym samym rozumowaniem, Trybunał w pkt 145 wyroku z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791) wyjaśnił, że nawet pozytywne obowiązki państw członkowskich, które mogą wynikać, w zależności od przypadku, z art. 3, 4 i 7 karty i które, jak zauważono w pkt 64 niniejszego wyroku, dotyczą ustanowienia przepisów umożliwiających skuteczne zwalczanie przestępstw, nie mogą uzasadniać tak poważnych ingerencji jak te wynikające z przepisów przewidujących zatrzymywanie danych o ruchu i danych dotyczących lokalizacji w prawa podstawowe ustanowione w art. 7 i 8 karty prawie całej ludności, gdy dane rozpatrywanych osób nie wykazują związku, choćby pośredniego, z zamierzonym celem (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 95).

125 Ponadto na podstawie wyroków ETPC z dnia 25 maja 2021 r. w sprawie Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu (CE:ECHR:2021:0525JUD 005817013) i w sprawie Centrum för Rättvisa przeciwko Szwecji (CE:ECHR:2021:0525JUD 003525208), przywołanych przez niektóre rządy podczas rozprawy celem poparcia twierdzenia, zgodnie z którym EKPC nie stoi na przeszkodzie przepisom krajowym przewidującym w istocie uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych dotyczących lokalizacji, nie można podważyć wynikającej z powyższych rozważań wykładni art. 15 ust. 1 dyrektywy 2002/58. Wyroki te dotyczyły bowiem masowego przechwytywania danych dotyczących połączeń międzynarodowych. Podobnie jak podniosła Komisja podczas rozprawy, Europejski Trybunał Praw Człowieka nie wypowiedział się w tych wyrokach w przedmiocie zgodności z EKPC uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i dotyczących lokalizacji na terytorium krajowym ani nawet o przechwytywaniu na szeroką skalę tych danych w celu zapobiegania poważnym przestępstwom, ich wykrywania i ścigania. W każdym razie należy przypomnieć, że art. 52 ust. 3 karty ma na celu zapewnienie niezbędnej spójności między prawami zawartymi w karcie a odpowiadającymi im prawami zagwarantowanymi w EKPC, bez naruszania autonomii prawa Unii i Trybunału Sprawiedliwości Unii Europejskiej, efektem czego odpowiednie wynikające z EKPC prawa należy uwzględniać, w celu dokonania wykładni postanowień zawartych w karcie, jedynie jako minimalny próg ochrony (wyrok z dnia 17 grudnia 2020 r., Centraal Israëlitisch Consistorie van België i in., C-336/19, EU:C:2020:1031, pkt 56).

W przedmiocie dostępu do danych zatrzymywanych w uogólniony i niezróżnicowany sposób

126 Na rozprawie rząd duński utrzymywał, że właściwe organy krajowe, do celów walki z poważną przestępczością, powinny móc mieć dostęp do danych o ruchu i danych dotyczących lokalizacji, które zostały zatrzymane w sposób uogólniony i niezróżnicowany, zgodnie z orzecznictwem wynikającym z wyroku 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 135–139), aby stawić czoła poważnemu zagrożeniu dla bezpieczeństwa narodowego, które okazuje się być rzeczywiste i aktualne czy też przewidywalne.

127 Należy od razu zauważyć, że zezwolenia na dostęp, do celów walki z poważną przestępczością, do danych o ruchu i danych dotyczących lokalizacji, które zostały zatrzymane w sposób uogólniony i niezróżnicowany, spowodowałoby uzależnienie tego dostępu od okoliczności niezwiązanych z tym celem, w zależności od istnienia lub nieistnienia w danym państwie członkowskim poważnego zagrożenia dla bezpieczeństwa narodowego, takiego jak to wspomniane w poprzednim punkcie, podczas gdy w świetle jedynego celu w postaci zwalczania poważnej przestępczości, który powinien uzasadniać zatrzymywanie tych danych i dostęp do nich, nic nie uzasadnia różnicy w traktowaniu w szczególności wśród państw członkowskich (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 97).

128 Jak już zostało to orzeczone przez Trybunał, dostęp do danych o ruchu i do danych dotyczących lokalizacji zatrzymywanych przez dostawców usług łączności elektronicznej 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 rzecz ma się jedynie wówczas, 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).

129 Argumentacja rządu duńskiego odnosi się zaś do sytuacji, w której cel planowanego wniosku o udzielenie dostępu, to jest zwalczanie poważnej przestępczości, ma w hierarchii celów interesu ogólnego mniejsze znaczenie niż cel, który uzasadniał zatrzymywanie danych, czyli ochrona bezpieczeństwa narodowego. Zezwolenie w takiej sytuacji na dostęp do zatrzymanych danych pozostawałoby w sprzeczności z tą hierarchią celów interesu ogólnego, przypomnianą w poprzednim punkcie, jak również w pkt 68, 71, 72 i 73 niniejszego wyroku (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 99).

130 Ponadto i przede wszystkim należy stwierdzić, że zgodnie z orzecznictwem przypomnianym w pkt 74 niniejszego wyroku dane o ruchu i dane dotyczących lokalizacji nie mogą być przedmiotem uogólnionego i niezróżnicowanego zatrzymywania danych do celów walki z poważną przestępczością, a tym samym dostęp do tych danych nie może być uzasadniony ze względu na te cele. Jeżeli zaś te dane zostały wyjątkowo zatrzymane w sposób uogólniony i niezróżnicowany do celów ochrony bezpieczeństwa narodowego przed zagrożeniem, które okazuje się rzeczywiste i aktualne lub przewidywalne, w warunkach wskazanych w pkt 71 niniejszego wyroku, organy krajowe właściwe w zakresie dochodzeń w sprawach karnych nie mogą mieć dostępu do owych danych w ramach ścigania karnego, pod rygorem pozbawienia wszelkiej skuteczności (effet utile) zakazu takiego zatrzymywania do celów walki z poważną przestępczością, przypomnianego w pkt 74 (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 100).

131 W świetle całokształtu powyższych rozważań na pytanie prejudycjalne należy odpowiedzieć, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty należy interpretować w ten sposób, iż sprzeczne z nim są krajowe 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. Natomiast wspomniany art. 15 ust. 1 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty należy interpretować w taki sposób, że nie są z nim sprzeczne krajowe przepisy ustawodawcze:

– umożliwiające, w celu ochrony bezpieczeństwa narodowego, posłużenie się skierowanym do dostawców usług łączności elektronicznej nakazem 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, przy czym decyzja o wydaniu takiego nakazu może być przedmiotem skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja wywiera wiążący skutek, mającej na celu weryfikację występowania jednej z takich sytuacji oraz poszanowania warunków i gwarancji, które powinny zostać przewidziane, zaś wspomniany nakaz można wydać jedynie na określony czas, ograniczony do tego, co ściśle niezbędne, jednak z możliwością przedłużenia w przypadku utrzymywania się tego zagrożenia;

– przewidujące, 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, na okres ograniczony do tego, co ściśle niezbędne, ale odnawialny;

– przewidujące, w celu ochrony bezpieczeństwa narodowego, zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, uogólnione i niezróżnicowane zatrzymywanie adresów IP przydzielonych źródłu połączenia, w okresie ograniczonym do tego, co ściśle niezbędne;

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

– umożliwiające, w celu zwalczania poważnej przestępczości oraz, a fortiori, ochrony bezpieczeństwa narodowego, posłużenie się nakazem skierowanym do dostawców usług łączności elektronicznej, w drodze decyzji właściwego organu poddanej skutecznej kontroli sądowej, szybkiego zatrzymywania 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.

W przedmiocie kosztów

132 Dla stron w postępowaniach głównych 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 postępowaniach głównych, nie podlegają zwrotowi.

Z powyższych względów Trybunał (wielka 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

sprzeczne z nim są krajowe środki ustawodawczym przewidujące, do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych dotyczących lokalizacji;

nie są z nim sprzeczne są krajowe środki ustawodawcze:

– **umożliwiające, w celu ochrony bezpieczeństwa narodowego, posłużenie się skierowanym do dostawców usług łączności elektronicznej nakazem 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, przy czym decyzja o wydaniu takiego nakazu może być przedmiotem skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja wywiera wiążący skutek, mającej na celu weryfikację występowania jednej z takich sytuacji oraz poszanowania warunków i gwarancji, które powinny zostać przewidziane, zaś wspomniany nakaz można wydać jedynie na określony czas ograniczony do tego, co ściśle niezbędne, jednak z możliwością przedłużenia w przypadku utrzymywania się tego zagrożenia;**

– **przewidujące, 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, na okres ograniczony do tego, co ściśle niezbędne, ale odnawialny;**

– **przewidujące, w celu ochrony bezpieczeństwa narodowego, zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego uogólnione i niezróżnicowane zatrzymywanie adresów IP przydzielonych źródłu połączenia, w okresie ograniczonym do tego, co ściśle niezbędne;**

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

– **umożliwiające, w celu zwalczania poważnej przestępczości oraz, a fortiori, ochrony bezpieczeństwa narodowego, posłużenie się nakazem skierowanym do dostawców usług łączności elektronicznej, w drodze decyzji właściwego organu poddanej skutecznej**

kontroli sądowej, szybkiego zatrzymywania 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.

Podpisy