Zbiór Orzeczeń

WYROK TRYBUNAŁU (wielka izba)

z dnia 6 października 2020 r.*

Odesłanie prejudycjalne – Przetwarzanie danych osobowych w sektorze łączności elektronicznej – Dostawcy usług łączności elektronicznej – Uogólniona i niezróżnicowana transmisja danych o ruchu i danych o lokalizacji – Ochrona bezpieczeństwa narodowego – Dyrektywa 2002/58/WE – Zakres stosowania – Artykuł 1 ust. 3 i art. 3 – Poufność łączności elektronicznej – Ochrona – Artykuł 5 i art. 15 ust. 1 – Karta praw podstawowych Unii Europejskiej – Artykuły 7, 8 i 11 oraz art. 52 ust. 1 – Artykuł 4 ust. 2 TUE

W sprawie C-623/17

mającej za przedmiot wniosek o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożony przez Investigatory Powers Tribunal (sąd ds. uprawnień operacyjnych, Zjednoczone Królestwo) postanowieniem z dnia 18 października 2017 r., które wpłynęło do Trybunału w dniu 31 października 2017 r., w postępowaniu:

Privacy International

przeciwko

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service,

TRYBUNAŁ (wielka izba),

w składzie: K. Lenaerts, prezes, R. Silva de Lapuerta, wiceprezes, J.C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P.G. Xuereb i L.S. Rossi, prezesi izb, J. Malenovský, L. Bay Larsen, T. von Danwitz (sprawozdawca), C. Toader, K. Jürimäe, C. Lycourgos i N. Piçarra, sędziowie,

rzecznik generalny: M. Campos Sánchez-Bordona,

sekretarz: C. Strömholm, administratorka,

uwzględniając pisemny etap postępowania i po przeprowadzeniu rozprawy w dniach 9 i 10 września 2019 r.,

* Język postępowania: angielski.

rozważywszy uwagi, które przedstawili:

– w imieniu Privacy International – B. Jaffey i T. de la Mare, QC, D. Cashman, solicitor, oraz H. Roy, avocat,

– w imieniu rządu Zjednoczonego Królestwa – Z. Lavery, D. Guðmundsdóttir oraz S. Brandon, w charakterze pełnomocników, wspierani przez G. Facennę i D. Bearda, QC, oraz C. Knighta i R. Palmera, barristers,

– w imieniu rządu belgijskiego – P. Cottin i J.-C. Halleux, w charakterze pełnomocników, wspierani przez J. Vanpraeta, advocaat, i E. de Lophema, avocat,

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

– w imieniu rządu niemieckiego – początkowo M. Hellmann, R. Kanitz, D. Klebs i T. Henze, a następnie J. Möller, M. Hellmann, R. Kanitz i D. Klebs, w charakterze pełnomocników,

– w imieniu rządu estońskiego – A. Kalbus, w charakterze pełnomocnika,

– w imieniu rządu irlandzkiego – M. Browne, G. Hodge oraz A. Joyce, w charakterze pełnomocników, wspierani przez D. Fennelly'ego, barrister,

– w imieniu rządu hiszpańskiego – początkowo L. Aguilera Ruiz i M.J. García-Valdecasas Dorrego, a następnie L. Aguilera Ruiz, w charakterze pełnomocników,

– w imieniu rządu francuskiego – początkowo E. de Moustier, E. Armoët, A.L. Desjonquères, F. Alabrune, D. Colas i D. Dubois, a następnie E. de Moustier, E. Armoët, A.L. Desjonquères, F. Alabrune i D. Dubois, w charakterze pełnomocników,

– w imieniu rządu cypryjskiego – E. Symeonidou i E. Neofytou, w charakterze pełnomocników,

– w imieniu rządu łotewskiego – początkowo V. Soņeca i I. Kucina, a następnie V. Soņeca, w charakterze pełnomocników,

– w imieniu rządu węgierskiego – początkowo G. Koós, M.Z. Fehér, G. Tornyai oraz Z. Wagner, a następnie G. Koós i M.Z. Fehér, w charakterze pełnomocników,

– w imieniu rządu niderlandzkiego – C.S. Schillemans i M.K. Bulterman, w charakterze pełnomocników,

– w imieniu rządu polskiego – B. Majczyna, J. Sawicka i M. Pawlicka, w charakterze pełnomocników,

– w imieniu rządu portugalskiego – L. Inez Fernandes, M. Figueiredo oraz F. Aragão Homem, w charakterze pełnomocników,

– w imieniu rządu szwedzkiego – początkowo A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren i A. Alriksson, następnie H. Shev, C. Meyer-Seitz, L. Zettergren i A. Alriksson, w charakterze pełnomocników,

– w imieniu rządu norweskiego – T.B. Leming, M. Emberland i J. Vangsnes, w charakterze pełnomocników,

– w imieniu Komisji Europejskiej – początkowo H. Kranenborg, M. Wasmeier, D. Nardi oraz P. Costa de Oliveira, a następnie H. Kranenborg, M. Wasmeier oraz D. Nardi, w charakterze pełnomocników,

– w imieniu Europejskiego Inspektora Ochrony Danych – T. Zerdick i A. Buchta, w charakterze pełnomocników,

po zapoznaniu się z opinią rzecznika generalnego na posiedzeniu w dniu 15 stycznia 2020 r.,

wydaje następujący

Wyrok

1 Wniosek o wydanie orzeczenia w trybie prejudycjalnym dotyczy wykładni art. 1 ust. 3 i 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 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r. (Dz.U. 2009, L 337, s. 11) (zwanej dalej „dyrektywą 2002/58”), w związku z art. 4 ust. 2 TUE, a także art. 7 i 8 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą”).

2 Wniosek ten przedstawiono w ramach sporu pomiędzy Privacy International a Secretary of State for Foreign and Commonwealth Affairs (sekretarzem stanu spraw zagranicznych i Commonwealth, Zjednoczone Królestwo), Secretary of State for the Home Departement (sekretarzem stanu spraw wewnętrznych, Zjednoczone Królestwo), Government Communications Headquarters (sztabem łączności rządowej Zjednoczonego Królestwa, zwanym dalej „GCHQ”), Security Service (służbą kontrwywiadu, Zjednoczone Królestwo, zwaną dalej „MI5”) i Secret Intelligence Service (służbą wywiadu, Zjednoczone Królestwo, zwaną dalej „MI6”), w przedmiocie zgodności z prawem ustawodawstwa umożliwiającego uzyskanie i wykorzystywanie przez służby wywiadu i bezpieczeństwa masowych danych telekomunikacyjnych (*bulk communications data*).

Ramy prawne

Prawo Unii

Dyrektywa 95/46

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 uchylona 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/WE (Dz.U. 2016, L 119, s. 1; sprostowanie Dz.U 2018, L 127, s. 2). Artykuł 3 wspomnianej dyrektywy, zatytułowany „Zakres obowiązywania”, miał następujące brzmienie:

„1. Niniejsza dyrektywa stosuje się do przetwarzania danych osobowych w całości lub w części w sposób zautomatyzowany oraz innego przetwarzania danych osobowych, stanowiących część zbioru danych lub mających stanowić część zbioru danych.

2. 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 [TUE], a w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarczą 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

4 Motywy 2, 6, 7, 11, 22, 26 i 30 dyrektywy 2002/58 mają następujące brzmienie:

„(2) Niniejsza dyrektywa dąży do poszanowania fundamentalnych praw i jest zgodna z zasadami uznanymi w szczególności przez [kartę]. W szczególności niniejsza dyrektywa zmierza 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 [Unii]. Dyrektywa nie zmienia zatem istniejącej równowagi między prawem do prywatności osoby fizycznej a możliwością państw członkowskich do 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 w dniu 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 oraz powinny podlegać stosownym zabezpieczeniom zgodnie z europejską Konwencją o ochronie praw człowieka i podstawowych wolności.

[…]

(22) Zakaz przechowywania komunikatów oraz związanych z nimi danych dotyczących ruchu w sieci przez osoby inne niż użytkownicy lub bez ich zgody nie ma na celu zakazu automatycznego, pośredniego i przejściowego przechowywania takiej informacji, wówczas gdy odbywa się to wyłącznie do celu przeprowadzenia transmisji w sieci łączności elektronicznej oraz pod warunkiem, że informacja nie jest przechowywana przez okres dłuższy niż jest to konieczne w celu wykonania transmisji i zarządzania ruchem oraz że w okresie przechowywania zagwarantowana zostaje poufność. W przypadku gdy jest to niezbędne dla zwiększenia wydajności transmisji jakiejkolwiek dostępnej publicznie informacji do innych odbiorców usług na ich żądanie, niniejsza dyrektywa nie powinna uniemożliwiać dalszego przechowywania takiej informacji, pod warunkiem że informacja jest w każdym przypadku dostępna publicznie bez ograniczeń oraz że dane o poszczególnych abonentach lub użytkownikach zamawiających taką informację zostaną usunięte.

[…]

(26) Dane dotyczące abonentów przetwarzane w ramach sieci łączności elektronicznej w celu ustanowienia połączenia i przenoszenia informacji zawierają informacje dotyczące prywatnego życia osób fizycznych i dotyczą prawa do poszanowania tajemnicy korespondencji lub dotyczą uzasadnionych interesów osób prawnych. Takie dane mogą być przechowywane tylko przez określony czas i wyłącznie w zakresie umożliwiającym świadczenie usług związanych z naliczaniem opłat i rozliczeń międzyoperatorskich. Wszelkie dalsze przetwarzanie tego rodzaju danych […] może być dozwolone tylko w przypadkach, gdy abonent wyraził na to zgodę na podstawie udzielonej mu przez dostawcę usług dokładnej i pełnej informacji o rodzajach zamierzonego dalszego przetwarzania oraz prawie abonenta do nieudzielenia zgody na przetwarzanie lub jej odwołania. Dane dotyczące ruchu wykorzystywane w marketingu usług komunikacyjnych […] powinny również zostać usunięte lub uczynione anonimowymi […].

[…]

(30) Systemy dostarczania sieci i usług łączności elektronicznej powinny być zaprojektowane w taki sposób, aby ograniczać ilość niezbędnych danych osobowych do ścisłego minimum […]”.

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

„1. Niniejsza dyrektywa przewiduje harmonizację przepisów krajowych wymaganych do zapewnienia równoważnego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do prywatności i poufności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej oraz w celu zapewnienia swobodnego przepływu [w Unii Europejskiej] 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 [TFUE], takiej jak działalność określona w tytułach V i VI Traktatu o Unii Europejskiej, ani, w żadnym wypadku, do działalności dotyczącej bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając dobrobyt gospodarczy państwa, gdy działalność odnosi się do spraw bezpieczeństwa państwa) i działalności państwa w dziedzinie prawa karnego”.

6 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;

[…]”.

7 W art. 3 wspomnianej dyrektywy, zatytułowanym „Usługi”, przewidziano:

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

8 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”.

9 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”.

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

„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 […]”.

11 Artykuł 15 omawianej dyrektywy, zatytułowany „Stosowanie niektórych przepisów dyrektywy [95/46]”, w ust. 1 stanowi:

„Państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4 i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (i.e. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania 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 [Unii], w tym zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej”.

Rozporządzenie 2016/679

12 Artykuł 2 rozporządzenia 2016/679 stanowi:

„1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

2. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:

a) w ramach działalności nieobjętej zakresem prawa Unii;

b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;

[…]

d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

[…]”.

13 W art. 4 tego rozporządzenia przewidziano:

„Na użytek niniejszego rozporządzenia:

[…]

2) »przetwarzanie« oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

[…]”.

14 Zgodnie z art. 23 ust. 1 tego rozporządzenia:

„Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:

a) bezpieczeństwu narodowemu;

b) obronie;

c) bezpieczeństwu publicznemu;

d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;

e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu;

f) ochronie niezależności sądów i postępowania sądowego;

g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu;

h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a)–e) oraz g);

i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób;

j) egzekucji roszczeń cywilnoprawnych".

15 Zgodnie z art. 94 ust. 2 rozporządzenia 2016/679:

„Odesłania do uchylonej dyrektywy należy traktować jako odesłania do niniejszego rozporządzenia. Odesłania do Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, ustanowionej w art. 29 dyrektywy [95/46], należy traktować jako odesłania do Europejskiej Rady Ochrony Danych, ustanowionej niniejszym rozporządzeniem".

Prawo Zjednoczonego Królestwa

16 Artykuł 94 Telecommunications Act 1984 (ustawy o telekomunikacji), w brzmieniu mającym zastosowanie do okoliczności w postępowaniu głównym (zwanej dalej „ustawą z 1984"), zatytułowany „Polecenia wydawane w interesie bezpieczeństwa narodowego itp.", stanowi:

„(1) Sekretarz stanu może, po konsultacji z osobą, do której stosuje się niniejszy artykuł, wydawać tej osobie ogólne polecenia, jakie sekretarz stanu uzna za konieczne w interesie bezpieczeństwa narodowego lub stosunków z rządem kraju lub terytorium znajdującego się poza Zjednoczonym Królestwem.

(2) Jeśli sekretarz stanu uzna za to konieczne w interesie bezpieczeństwa narodowego lub stosunków z rządem kraju lub terytorium znajdującego się poza Zjednoczonym Królestwem, może on po konsultacji z osobą, do której stosuje się niniejszy artykuł, wydawać tej osobie polecenia (w zależności od danego przypadku) podjęcia lub niepodejmowania konkretnego działania określonego w tych poleceniach.

(2A) Sekretarz stanu może wydawać polecenia na podstawie ust. 1 lub 2, jeśli uważa, że zachowanie wymagane w tych poleceniach jest proporcjonalne do celu, jaki ma zostać osiągnięty za pomocą tego zachowania.

(3) Osoba, do której stosuje się niniejszy artykuł, ma obowiązek wprowadzić w życie wszelkie polecenia wydane jej przez sekretarza stanu na podstawie niniejszego artykułu, niezależnie od wszelkich innych obowiązków ciążących na niej na podstawie części 1 lub części 2 rozdziału 1 Communications Act

2003 [ustawy z 2003 r. o łączności], oraz w przypadku poleceń wydawanych dostawcy publicznej sieci łączności elektronicznej, nawet jeśli wspomniane polecenia mają do niego zastosowanie w innym charakterze niż w charakterze dostawcy dostępu do takiej sieci.

(4) Sekretarz stanu przekazuje każdej izbie Parlamentu kopię wszelkich poleceń wydanych na podstawie niniejszego artykułu, chyba że uważa, iż ujawnienie omawianych poleceń byłoby sprzeczne z interesem bezpieczeństwa narodowego lub stosunków z rządem kraju lub terytorium znajdującego się poza Zjednoczonym Królestwem lub z interesami handlowymi jakiejś osoby.

(5) Osoba nie może ujawniać ani nie może zostać zobowiązana do ujawnienia, na podstawie żadnej ustawy, jakichkolwiek informacji dotyczących środków podjętych zgodnie z niniejszym artykułem, jeśli sekretarz stanu poinformował ją, że jest zdania, iż ujawnienie tych informacji byłoby sprzeczne z interesem bezpieczeństwa narodowego lub stosunków z rządem kraju lub terytorium znajdującego się poza Zjednoczonym Królestwem lub z interesami handlowymi innej osoby.

[…]

(8) Niniejszy artykuł stosuje się do [Office of communications, urzędu komunikacji (OFCOM)] i do dostawców publicznych sieci łączności elektronicznej".

17 Artykuł 21 ust. 4 i 6 Regulation of Investigatory Powers Act 2000 (ustawy regulującej uprawnienia operacyjne z 2000 r., zwanej dalej „RIPA") stanowi:

„(4) Do celów niniejszego rozdziału »dane dotyczące łączności« oznaczają:

(a) dane o ruchu zawarte w komunikacie lub powiązane z nim (przez nadawcę lub w inny sposób) dla celów dowolnej usługi pocztowej lub systemu telekomunikacyjnego, za pomocą którego komunikat ten jest lub może być transmitowany;

(b) wszelkie informacje, które nie obejmują treści komunikatu [z wyłączeniem informacji, o których mowa w lit. a)], dotyczące korzystania przez dowolną osobę:
(i) z dowolnej usługi pocztowej lub telekomunikacyjnej; lub
(ii) w zakresie związanym ze świadczeniem na rzecz dowolnej osoby lub korzystaniem przez nią z dowolnej usługi telekomunikacyjnej w ramach części systemu telekomunikacyjnego;

(c) wszelkie informacje nienależące do zakresu uregulowanego w lit. a) i b), które znajdują się w posiadaniu lub zostały uzyskane przez osobę świadczącą usługi pocztowe lub usługi telekomunikacyjne, w zakresie dotyczącym osób, na rzecz których owe usługi są świadczone.

[…]

(6) [P]ojęcie »danych o ruchu« użyte w odniesieniu do dowolnego komunikatu oznacza:

(a) wszelkie dane identyfikujące lub mogące identyfikować dowolną osobę, urządzenie lub miejsce, do którego lub z którego jest lub może być transmitowany komunikat,

(b) wszelkie dane identyfikujące lub selekcjonujące bądź mogące identyfikować lub selekcjonować urządzenie, z wykorzystaniem którego jest lub może być transmitowany komunikat,

(c) wszelkie dane zawierające sygnały służące działaniu urządzenia wykorzystywanego w systemach łączności dla celów transmisji dowolnego komunikatu; oraz

(d) wszelkie dane identyfikujące dane zawarte lub dołączone do danego komunikatu lub inne dane zawarte lub dołączone do danego komunikatu.

[…]”.

18 W art. 65–69 RIPA ustanowiono przepisy dotyczące funkcjonowania i właściwości Investigatory Powers Tribunal (sądu ds. uprawnień operacyjnych, Zjednoczone Królestwo). Zgodnie z art. 65 tej ustawy można składać skargi do tego sądu, jeśli istnieje powód, aby uważać, że dane uzyskano w sposób niewłaściwy.

Spór w postępowaniu głównym i pytania prejudycjalne

19 Na początku 2015 r. ujawniono publicznie istnienie praktyk uzyskiwania i wykorzystywania masowych danych telekomunikacyjnych przez różne służby wywiadu i bezpieczeństwa Zjednoczonego Królestwa, mianowicie GCHQ, MI5 i MI6, w szczególności w sprawozdaniu Intelligence and Security Committee of Parliament (komisji parlamentarnej do spraw wywiadu i bezpieczeństwa, Zjednoczone Królestwo). W dniu 5 czerwca 2015 r. Privacy International, organizacja pozarządowa, wniosła do Investigatory Powers Tribunal (sądu ds. uprawnień operacyjnych) skargę przeciwko sekretarzowi stanu spraw zagranicznych i Commonwealth, sekretarzowi stanu spraw wewnętrznych oraz wspomnianym służbom wywiadu i bezpieczeństwa, w której zakwestionowano zgodność tych praktyk z prawem.

20 Sąd odsyłający zbadał zgodność z prawem wspomnianych praktyk w świetle przede wszystkim prawa wewnętrznego i postanowień europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, podpisanej w Rzymie w dniu 4 listopada 1950 r. (zwanej dalej „EKPC”), a następnie w świetle prawa Unii. W wyroku z dnia 17 października 2016 r. sąd ów orzekł, że pozwani w postępowaniu głównym przyznali, iż wspomniane służby wywiadu i bezpieczeństwa uzyskiwały i wykorzystywały w ramach ich działań zestawy danych dotyczących osób prywatnych, należących do różnych kategorii (*bulk personal data*), takich jak dane biograficzne lub dotyczące podróży, informacje o charakterze finansowym lub handlowym, dane związane z łącznością i mogące zawierać dane szczególnie chronione, objęte tajemnicą zawodową lub materiały dziennikarskie. Dane te, uzyskane na różne sposoby, niekiedy niejawnie, były analizowane w drodze badania krzyżowego oraz za pomocą zautomatyzowanego przetwarzania, mogły zostać ujawnione innym osobom i organom oraz przekazane zagranicznym partnerom. W tych ramach służby wywiadu i bezpieczeństwa wykorzystywały również masowe dane telekomunikacyjne, uzyskane od dostawców publicznych sieci łączności elektronicznej na mocy w szczególności poleceń sekretarza stanu wydanych na podstawie art. 94 ustawy z 1984 r. GCHQ i MI5 prowadziły takie działania, odpowiednio, od 2001 r. i od 2005 r.

21 Sąd odsyłający uznał, że te środki umożliwiające uzyskiwanie i wykorzystywanie danych były zgodne z prawem wewnętrznym, a od 2015 r., z zastrzeżeniem kwestii dotąd niezbadanych, dotyczących proporcjonalności omawianych środków i przekazywania danych stronom trzecim, z art. 8 EKPC. W tym ostatnim względzie wyjaśnił on, że zostały mu przedstawione dowody dotyczące stosowanych zabezpieczeń, w szczególności w odniesieniu do procedur dostępu i ujawniania poza służbami wywiadu i bezpieczeństwa, metod zatrzymywania danych i istnienia niezależnego nadzoru.

22 Co się tyczy zgodności z prawem rozpatrywanych w postępowaniu głównym środków umożliwiających uzyskiwanie i wykorzystywanie z punktu widzenia prawa Unii sąd odsyłający zbadał w wyroku z dnia 8 września 2017 r., czy środki te były objęte zakresem stosowania tego prawa, a jeśli tak, to czy były one zgodne z tym prawem. Sąd ów stwierdził, w odniesieniu do masowych danych telekomunikacyjnych, że dostawcy publicznych sieci łączności elektronicznej byli zobowiązani na podstawie art. 94 ustawy z 1984 r., w przypadku odpowiednich poleceń wydanych przez sekretarza stanu, do dostarczenia służbom wywiadu i bezpieczeństwa danych zgromadzonych w ramach ich działalności gospodarczej podlegającej prawu Unii. Nie dotyczyło to natomiast uzyskiwania innych danych, które służby te uzyskały bez wykorzystania takich nadzwyczajnych uprawnień. Na podstawie tego stwierdzenia sąd ów uznał za niezbędne zwrócenie się do Trybunału w celu ustalenia, czy system taki jak wynikający z owego art. 94 podlega prawu Unii, a jeśli tak, to czy – i w jaki sposób – wymogi

ustanowione w orzecznictwie wynikającym z wyroku z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, zwanego dalej „wyrokiem Tele2", EU:C:2016:970, mają zastosowanie do tego systemu.

23 W tym względzie w swoim wniosku o wydanie orzeczenia w trybie prejudycjalnym sąd odsyłający wskazuje, że zgodnie z omawianym art. 94 sekretarz stanu może wydawać dostawcom publicznych sieci łączności elektronicznej polecenia ogólne lub szczególne, jakie uważa za konieczne w interesie bezpieczeństwa narodowego lub stosunków z zagranicznym rządem. Odsyłając do definicji zawartej w art. 21 ust. 4 i 6 RIPA, sąd ten wyjaśnia, że rozpatrywane dane obejmują dane o ruchu oraz informacje o używanych usługach, w rozumieniu tego ostatniego przepisu, z wyłączeniem jedynie treści komunikatów. Te dane i informacje pozwalają w szczególności na ustalenie „kto, kiedy, gdzie i jak" w odniesieniu do danego komunikatu. Omawiane dane są transmitowane służbom wywiadu i bezpieczeństwa i zatrzymywane przez te służby do celów ich działalności.

24 Zdaniem wspomnianego sądu system rozpatrywany w postępowaniu głównym różni się od systemu wynikającego z Data Retention and Investigatory Powers Act 2014 (ustawy z 2014 r. o zatrzymywaniu danych i uprawnieniach dochodzeniowych), rozpatrywanego w sprawie, w której zapadł wyrok z dnia 21 grudnia 2016 r., Tele2 (C-203/15 i C-698/15, EU:C:2016:970), ponieważ ten ostatni system przewidywał zatrzymywanie danych przez dostawców usług łączności elektronicznej i ich udostępnianie nie tylko służbom wywiadu i bezpieczeństwa w interesie bezpieczeństwa narodowego, ale także innym organom publicznym, jeśli tego potrzebowały. Wyrok ten dotyczył ponadto dochodzenia w sprawie karnej, a nie bezpieczeństwa narodowego.

25 Sąd odsyłający dodaje, że bazy danych utworzone przez służby wywiadu i bezpieczeństwa podlegają masowemu i zautomatyzowanemu przetwarzaniu, niespecyficznemu, zmierzającemu do wykrycia istnienia ewentualnych nieznanych zagrożeń. W tym względzie sąd ów wskazuje, że utworzony w ten sposób zestaw metadanych powinien być tak pełny, jak to tylko możliwe, aby móc stanowić „stóg siana", w którym znajdzie się ukryta „igła". Co się tyczy użyteczności gromadzenia masowych danych przez wspomniane służby i technik przeglądania tych danych, omawiany sąd odnosi się w szczególności do wniosków sprawozdania sporządzonego w dniu 19 sierpnia 2016 r. przez Davida Andersona, QC, ówczesnego United Kingdom Independent Reviewer of Terrorism Legislation (niezależnego kontrolera Zjednoczonego Królestwa do spraw ustawodawstwa dotyczącego terroryzmu), który przy sporządzaniu tego sprawozdania oparł się na badaniu przeprowadzonym przez zespół specjalistów w dziedzinie informacji i na świadectwie agentów służb wywiadu i bezpieczeństwa.

26 Sąd odsyłający wyjaśnia również, że według Privacy International system rozpatrywany w postępowaniu głównym jest niezgodny z prawem z punktu widzenia prawa Unii, podczas, gdy strony pozwane w postępowaniu głównym są zdania, że obowiązek transmisji danych przewidziany w tym systemie, dostęp do tych danych oraz ich wykorzystanie nie podlegają kompetencjom Unii, zgodnie w szczególności z art. 4 ust. 2 TUE, który przewiduje, że bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego.

27 W tym względzie sad odsyłający uważa, na podstawie wyroku z dnia 30 maja 2006 r., Parlament/Rada i Komisja (C-317/04 i C-318/04, EU:C:2006:346, pkt 56–59), dotyczącego przekazywania danych PNR (Passenger Name Record) do celów ochrony bezpieczeństwa publicznego, że działalność spółek handlowych w ramach przetwarzania i przekazywania danych do celów ochrony bezpieczeństwa narodowego nie wydaje się objęta zakresem stosowania prawa Unii. Należy zbadać nie to, czy rozpatrywana działalność stanowi przetwarzanie danych, ale jedynie to, czy w istocie i rzeczywiście celem takiej działalności jest wykonywanie podstawowej funkcji państwa w rozumieniu art. 4 ust. 2 TUE, w ramach ustanowionych przez organy publiczne, dotyczących bezpieczeństwa publicznego.

28 W przypadku gdyby środki rozpatrywane w postępowaniu głównym były jednak objęte prawem Unii, sąd odsyłający uważa, że wymogi zawarte w pkt 119–125 wyroku z dnia 21 grudnia 2016 r., Tele2 (C-203/15 i C-698/15, EU:C:2016:970) wydają się niewłaściwe w kontekście bezpieczeństwa narodowego i mogą naruszać zdolność służb wywiadu i bezpieczeństwa do zapanowania na niektórymi zagrożeniami dla bezpieczeństwa narodowego.

29 W tych okolicznościach Investigatory Powers Tribunal (sąd ds. uprawnień operacyjnych) postanowił zawiesić postępowanie i przedstawić Trybunałowi następujące pytania prejudycjalne:

„W przypadku gdy:

a) możliwości wykorzystywania przez [służby wywiadu i bezpieczeństwa (SIA)] [masowych danych telekomunikacyjnych], które zostały im przekazane, są konieczne do ochrony bezpieczeństwa narodowego Zjednoczonego Królestwa, w tym w obszarach zwalczania terroryzmu oraz przeciwdziałania szpiegostwu i rozprzestrzenianiu broni jądrowej;

b) służby wywiadu i bezpieczeństwa wykorzystują masowe dane telekomunikacyjne głównie w celu wykrywania wcześniej nieznanych zagrożeń dla bezpieczeństwa narodowego przez zastosowanie masowych technik nieukierunkowanych na konkretne osoby, opartych na gromadzeniu masowych danych telekomunikacyjnych w jednym miejscu. Służy to przede wszystkim szybkiej identyfikacji i rozpracowaniu celu, a także zapewnieniu podstaw do podjęcia działań w obliczu bezpośredniego zagrożenia;

c) dostawca sieci łączności elektronicznej nie ma potem obowiązku zatrzymania masowych danych telekomunikacyjnych (przez okres dłuższy niż przewidują to jego zwykłe wymogi biznesowe), a dane te zatrzymuje wyłącznie państwo (służby wywiadu i bezpieczeństwa);

d) sąd krajowy ustalił (z wyjątkiem pewnych zastrzeżonych kwestii), że gwarancje towarzyszące wykorzystywaniu masowych danych telekomunikacyjnych przez służby wywiadu i bezpieczeństwa są zgodne z wymogami Konwencji o ochronie praw człowieka i podstawowych wolności; oraz

e) sąd krajowy stwierdził, że narzucenie wymogów określonych w pkt 119–125 wyroku [z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15 (EU:C:2016:970)], o ile mają zastosowanie, zniweczyłoby środki podjęte w celu ochrony bezpieczeństwa narodowego przez służby wywiadu i bezpieczeństwa i tym samym zagroziłoby bezpieczeństwu narodowemu Zjednoczonego Królestwa;

1) uwzględniając art. 4 TUE i art. 1 ust. 3 dyrektywy [2002/58] – czy wymóg w poleceniu sekretarza stanu dla dostawcy sieci łączności elektronicznej, zgodnie z którym dostawca ten musi przekazać masowe dane telekomunikacyjne służbom wywiadu i bezpieczeństwa państwa członkowskiego, wchodzi w zakres prawa Unii oraz dyrektywy [2002/58]?

2) jeżeli odpowiedź na pytanie pierwsze jest twierdząca – czy do takiego polecenia sekretarza stanu zastosowanie mają którekolwiek z wymogów [mających zastosowanie do zatrzymywanych danych telekomunikacyjnych określonych w pkt 119–125 wyroku z dnia 21 grudnia 2016 r., Tele2 (C-203/15 i C-698/15, EU:C:2016:970)] lub inne wymogi poza wymogami nałożonymi przez Konwencję o ochronie praw człowieka i podstawowych wolności? Jeśli tak, w jaki sposób i w jakim zakresie zastosowanie mają takie wymogi, biorąc pod uwagę konieczność zastosowania przez służby wywiadu i bezpieczeństwa technik masowego uzyskiwania i automatycznego przetwarzania w celu ochrony bezpieczeństwa narodowego oraz zakres, w jakim możliwości takie, o ile są zgodne z Konwencją o ochronie praw człowieka i podstawowych wolności, mogą być w istotny sposób osłabione przez nałożenie takich wymagań?”.

W przedmiocie pytań prejudycjalnych

W przedmiocie pytania pierwszego

30 Poprzez pytanie pierwsze sąd odsyłający zmierza w istocie do ustalenia, czy art. 1 ust. 3 dyrektywy 2002/58 w związku z art. 4 ust. 2 TUE należy interpretować w ten sposób, że zakresem stosowania tej dyrektywy objęte jest uregulowanie krajowe umożliwiające organowi państwa zobowiązanie dostawców usług łączności elektronicznej do transmitowania służbom wywiadu i bezpieczeństwa danych o ruchu i danych o lokalizacji dla celów ochrony bezpieczeństwa narodowego.

31 W tym względzie Privacy International podnosi w istocie, że z uwagi na wnioski płynące z orzecznictwa Trybunału co do zakresu stosowania dyrektywy 2002/58 zarówno uzyskiwanie danych przez służby wywiadu i bezpieczeństwa od tych dostawców na podstawie art. 94 ustawy z 1984 r., jak i ich wykorzystanie przez wspomniane służby objęte jest zakresem stosowania tej dyrektywy, bez względu na to, czy omawiane dane uzyskuje się w drodze transmisji z opóźnieniem, czy w czasie rzeczywistym. W szczególności okoliczność, że cel ochrony bezpieczeństwa narodowego wymieniono wyraźnie w art. 15 ust. 1 omawianej dyrektywy, nie powoduje niemożności stosowania tej dyrektywy do takich sytuacji, zaś art. 4 ust. 2 TUE nie ma wpływu na tę ocenę.

32 Z kolei rządy Zjednoczonego Królestwa, czeski i estoński, Irlandia oraz rządy francuski, cypryjski, węgierski, polski i szwedzki podnoszą w istocie, że dyrektywa 2002/58 nie ma zastosowania do uregulowania krajowego rozpatrywanego w postępowaniu głównym, ponieważ jego celem jest ochrona bezpieczeństwa narodowego. Działalność służb wywiadu i bezpieczeństwa jest objęta podstawową funkcją państw członkowskich, zmierzającą do utrzymania porządku publicznego, a także ochrony bezpieczeństwa wewnętrznego i integralności terytorialnej, a co za tym idzie – należy do wyłącznej kompetencji tych państw, jak wskazuje w szczególności art. 4 ust. 2 zdanie trzecie TUE.

33 Według tych rządów dyrektywy 2002/58 nie można więc interpretować w ten sposób, że środki krajowe zmierzające do ochrony bezpieczeństwa narodowego są objęte zakresem jej stosowania. W art. 1 ust. 3 tej dyrektywy wyznaczono ten zakres stosowania i wyłączono z niego, podobnie jak przewidziano już w art. 3 ust. 2 tiret pierwsze dyrektywy 95/46, działalność dotyczącą bezpieczeństwa publicznego, obronności i bezpieczeństwa państwa. Przepisy te odzwierciedlają podział kompetencji przewidziany w art. 4 ust. 2 TUE i zostałyby one pozbawione skuteczności (effet utile), gdyby środki należące do dziedziny bezpieczeństwa narodowego musiały spełniać wymogi dyrektywy 2002/58. Co więcej, orzecznictwo Trybunału wynikające z wyroku z dnia 30 maja 2006 r., Parlament/Rada i Komisja (C-317/04 i C-318/04, EU:C:2006:346), dotyczące art. 3 ust. 2 tiret pierwsze dyrektywy 95/46, przekłada się na art. 1 ust. 3 dyrektywy 2002/58.

34 W tym względzie należy wskazać, że w art. 1 ust. 1 dyrektywy 2002/58 przewidziano w szczególności harmonizację przepisów krajowych wymaganych dla 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.

35 Artykuł 1 ust. 3 dyrektywy 2002/58 wyłącza z zakresu jej stosowania „działalność" państwa w obszarach, które zostały tam wymienione, a w szczególności działalność państwa w dziedzinie prawa karnego oraz działalność dotyczącą bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa, włączając w to dobrobyt gospodarczy państwa, gdy działalność odnosi się do spraw bezpieczeństwa państwa. Rodzaje działalności wymienione w ten sposób tytułem przykładu stanowią w każdym wypadku działalność właściwą państwom i organom państwa, odmienną od dziedzin działalności podmiotów indywidualnych (wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 32 i przytoczone tam orzecznictwo).

36 Ponadto art. 3 dyrektywy 2002/58 stanowi, że ma ona zastosowanie do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii, włącznie z publicznymi sieciami łączności służącymi do zbierania danych i obsługi urządzeń identyfikacyjnych (zwanymi dalej „usługami łączności elektronicznej"). Co za tym idzie, należy uznać, że wspomniana dyrektywa odnosi się do działalności dostawców tych usług (wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 33 i przytoczone tam orzecznictwo).

37 W tych ramach art. 15 ust. 1 dyrektywy 2002/58 pozwala państwom członkowskim uchwalić, z poszanowaniem przewidzianych w nim warunków, „środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4 i art. 9 [tej] dyrektywy" (wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 71).

38 Tymczasem art. 15 ust. 1 dyrektywy 2002/58 stosuje się przy założeniu, że środki krajowe, które są w nim wymienione, wchodzą w zakres stosowania tej dyrektywy, ponieważ ta ostatnia upoważnia wyraźnie państwa członkowskie do ich przyjmowania wyłącznie z poszanowaniem ustanowionych w niej warunków. Ponadto takie środki regulują, do celów, o których mowa w tym przepisie, działalność dostawców usług łączności elektronicznej (wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 34 i przytoczone tam orzecznictwo).

39 To w szczególności w obliczu tych rozważań Trybunał orzekł, że art. 15 ust. 1 w związku z art. 3 dyrektywy 2002/58 należy interpretować w ten sposób, iż do zakresu stosowania tej dyrektywy należy nie tylko środek ustawodawczy, który nakłada na dostawców usług łączności elektronicznej obowiązek zatrzymywania danych o ruchu i danych o lokalizacji, lecz również środek ustawodawczy zobowiązujący ich do udzielenia właściwym organom krajowym dostępu do tych danych. Takie środki ustawodawcze wymagają bowiem przetwarzania wspomnianych danych przez omawianych dostawców i w zakresie, w jakim regulują działalność wspomnianych dostawców, nie mogą być traktowane jako działalność właściwa państwom, o której mowa w art. 1 ust. 3 omawianej dyrektywy (zob. podobnie wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 35, 37 i przytoczone tam orzecznictwo).

40 Co się tyczy środka ustawodawczego takiego jak art. 94 ustawy z 1984 r., na podstawie którego właściwy organ może wydać dostawcom usług łączności elektronicznej polecenie ujawnienia poprzez transmitowanie masowych danych służbom wywiadu i bezpieczeństwa, należy wskazać, że zgodnie z definicją zawartą w art. 4 pkt 2 rozporządzenia 2016/679, która ma zastosowanie zgodnie z art. 2 dyrektywy 2002/58, w związku z art. 94 ust. 2 wspomnianego rozporządzenia pojęcie „przetwarzani[a] [danych osobowych]" oznacza „operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie […], przechowywanie […], przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie […]".

41 Wynika z tego, że ujawnienie danych osobowych poprzez transmisję, podobnie jak zatrzymywanie danych lub każdy inny rodzaj udostępniania, stanowi przetwarzanie w rozumieniu art. 3 dyrektywy 2002/58, a co za tym idzie – mieści się w zakresie stosowania tej dyrektywy (zob. podobnie wyrok z dnia 29 stycznia 2008 r., Promusicae, C-275/06, EU:C:2008:54, pkt 45).

42 Ponadto, przy uwzględnieniu rozważań zawartych w pkt 38 niniejszego wyroku i systematykę dyrektywy 2002/58, wykładnia tej dyrektywy, zgodnie z którą środki ustawodawcze, o których mowa w art. 15 ust. 1 tej dyrektywy, są wyłączone z zakresu stosowania wspomnianej dyrektywy z tego powodu, że cele, do których środki te muszą prowadzić, pokrywają się zasadniczo z celami działalności, o których mowa w art. 1 ust. 3 tej dyrektywy, oznaczałaby pozbawienie rzeczonego art. 15 ust. 1 wszelkiej skuteczności (effet utile) (zob. podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 72, 73).

43 Pojęcia „działalności”, zawartego w art. 1 ust. 3 dyrektywy 2002/58, nie można zatem, jak wskazał w istocie rzecznik generalny w pkt 75 swojej opinii w sprawach połączonych La Quadrature du Net i in. (C-511/18 i C-512/18, EU:C:2020:6), do której odsyła on w pkt 24 swojej opinii w niniejszej sprawie, interpretować jako obejmującego środki ustawodawcze, o których mowa w art. 15 ust. 1 tej dyrektywy.

44 Postanowienia art. 4 ust. 2 TUE, do których odniosły się rządy wymienione w pkt 32 niniejszego wyroku, nie mogą podważyć tego wniosku. Zgodnie bowiem z utrwalonym orzecznictwem Trybunału mimo iż to do państw członkowskich należy określenie ich podstawowych interesów bezpieczeństwa i podjęcie środków zmierzających do zagwarantowania bezpieczeństwa zewnętrznego i wewnętrznego, sam tylko fakt, że środek krajowy został podjęty w celu ochrony bezpieczeństwa narodowego, nie może powodować niemożności stosowania prawa Unii i zwolnienia państw członkowskich z konieczności przestrzegania tego prawa [zob. podobnie wyroki: z dnia 4 czerwca 2013 r., ZZ, C-300/11, EU:C:2013:363, pkt 38 i przytoczone tam orzecznictwo; z dnia 20 marca 2018 r., Komisja/Austria (Drukarnia państwowa), C-187/16, EU:C:2018:194, pkt 75, 76; a także z dnia 2 kwietnia 2020 r., Komisja/Polska, Węgry i Republika Czeska (Tymczasowy mechanizm relokacji osób ubiegających się o udzielenie ochrony międzynarodowej), C-715/17, C-718/17 i C-719/17, EU:C:2020:257, pkt 143, 170].

45 Prawdą jest, że w wyroku z dnia 30 maja 2006 r., Parlament/Rada i Komisja (C-317/04 i C-318/04, EU:C:2006:346, pkt 56–59) Trybunał orzekł, iż przekazywanie danych osobowych przez linie lotnicze organom publicznym państwa trzeciego w celu zapobiegania terroryzmowi i innym poważnym przestępstwom oraz zwalczania ich nie było zgodnie z art. 3 ust. 2 tiret pierwsze dyrektywy 95/46 objęte zakresem stosowania tej dyrektywy, ponieważ takie przekazywanie następuje w ramach ustanowionych przez organy publiczne, mających na celu ochronę bezpieczeństwa publicznego.

46 Niemniej jednak, z uwagi na rozważania zawarte w pkt 36, 38 i 39 niniejszego wyroku, orzecznictwo to nie znajduje odpowiedniego zastosowania do wykładni art. 1 ust. 3 dyrektywy 2002/58. Jak w istocie wskazał rzecznik generalny w pkt 70–72 opinii w sprawach połączonych La Quadrature du Net i in. (C-511/18 i C-512/18, EU:C:2020:6), art. 3 ust. 2 tiret pierwsze dyrektywy 95/46, do którego odnosi się wspomniane orzecznictwo, wyłączył z zakresu stosowania tej dyrektywy w sposób ogólny „działalność na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa”, bez rozróżnienia w zależności od rozpatrywanego podmiotu przetwarzającego dane. Natomiast w ramach wykładni art. 1 ust. 3 dyrektywy 2002/58 takie rozróżnienie okazuje się niezbędne. Jak bowiem wynika z pkt 37–39 i 42 niniejszego wyroku, zakresem stosowania omawianej dyrektywy objęte jest wszelkie przetwarzanie danych osobowych przez dostawców usług łączności elektronicznej, w tym przetwarzanie wynikające z obowiązków nałożonych na nich przez organy publiczne, podczas gdy to ostatnie przetwarzanie może ewentualnie być objęte zakresem stosowania odstępstwa przewidzianego w art. 3 ust. 2 tiret pierwsze dyrektywy 95/46, biorąc pod uwagę bardziej ogólne sformułowanie tego przepisu, odnoszące się do wszelkiego przetwarzania, bez względu na podmiot przetwarzający, na rzecz bezpieczeństwa publicznego, obronności lub bezpieczeństwa państwa.

47 Co więcej, należy wskazać, że dyrektywa 95/46, rozpatrywana w sprawie, w której zapadł wyrok z dnia 30 maja 2006 r., Parlament/Rada i Komisja (C-317/04 i C-318/04, EU:C:2006:346), została na mocy art. 94 ust. 1 rozporządzenia 2016/679 uchylona i zastąpiona przez to rozporządzenie ze skutkiem od dnia 25 maja 2018 r. Tymczasem jakkolwiek w art. 2 ust. 2 lit. d) omawianego rozporządzenia sprecyzowano, że nie ma ono zastosowania do przetwarzania „przez właściwe organy” do celów w szczególności wykrywania i ścigania czynów zabronionych, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, to jednak z art. 23 ust. 1 lit. d) i h) tego rozporządzenia wynika, że przetwarzanie danych osobowych w tych samych celach przez osoby prywatne jest objęte zakresem stosowania tego rozporządzenia. Wynika z tego, że powyższa wykładnia art. 1 ust. 3, art. 3 i art. 15 ust. 1 dyrektywy 2002/58 jest spójna z wyznaczeniem zakresu stosowania rozporządzenia 2016/679, które ta dyrektywa uzupełnia i doprecyzowuje.

48 Natomiast kiedy państwa członkowskie wprowadzają bezpośrednio środki stanowiące odstępstwo od poufności łączności elektronicznej, bez nakładania obowiązków przetwarzania na dostawców usług łączności elektronicznej, ochrona danych osobowych jest objęta nie dyrektywą 2002/58, ale jedynie prawem krajowym, z zastrzeżeniem stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz.U. 2016, L 119, s. 89), a więc rozpatrywane środki muszą respektować w szczególności prawo krajowe rangi konstytucyjnej i wymogi EKPC.

49 Biorąc pod uwagę powyższe rozważania, na pytanie pierwsze należy udzielić odpowiedzi, że art. 1 ust. 3, art. 3 i art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 4 ust. 2 TUE należy interpretować w ten sposób, iż zakresem stosowania tej dyrektywy objęte jest uregulowanie krajowe umożliwiające organowi państwa zobowiązanie dostawców usług łączności elektronicznej do transmitowania służbom wywiadu i bezpieczeństwa danych o ruchu i danych o lokalizacji do celów ochrony bezpieczeństwa narodowego.

W przedmiocie pytania drugiego

50 Poprzez pytanie drugie sąd odsyłający zmierza w istocie do ustalenia w szczególności, czy art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 4 ust. 2 TUE, a także art. 7, 8 i 11 oraz art. 52 ust. 1 karty, należy interpretować w ten sposób, że sprzeciwia się on przepisom krajowym umożliwiającym organowi państwa zobowiązanie dostawców usług łączności elektronicznej do uogólnionego i niezróżnicowanego transmitowania danych o ruchu i danych o lokalizacji służbom wywiadu i bezpieczeństwa w celu ochrony bezpieczeństwa narodowego.

51 Na wstępie należy przypomnieć, że zgodnie z informacjami zawartymi we wniosku o wydanie orzeczenia w trybie prejudycjalnym art. 94 ustawy z 1984 r. upoważnia sekretarza stanu do zobowiązania dostawców usług łączności elektronicznej w drodze poleceń transmitowania służbom wywiadu i bezpieczeństwa masowych danych komunikacyjnych, w tym danych o ruchu i danych o lokalizacji, a także informacji o używanych usługach w rozumieniu art. 21 ust. 4 i 6 RIPA, jeśli uzna on to za konieczne w interesie bezpieczeństwa narodowego lub stosunków z zagranicznym rządem. Ten ostatni przepis obejmuje między innymi dane niezbędne do zidentyfikowania źródła komunikatu i jego przeznaczenia, określenia daty, godziny, czasu trwania i rodzaju połączenia, zidentyfikowania użytego narzędzia oraz zlokalizowania urządzeń końcowych i połączeń, danych obejmujących w szczególności nazwisko i adres użytkownika, numer telefonu dzwoniącego i numer wybierany, adresy IP źródła i odbiorcy komunikatu oraz adresy odwiedzanych stron internetowych.

52 Takie ujawnienie poprzez transmisję danych dotyczy wszystkich użytkowników środków łączności elektronicznej, bez wskazania, czy to transmisja ta ma nastąpić w czasie rzeczywistym czy z opóźnieniem. Po transmisji dane te są zgodnie z informacjami zawartymi we wniosku o wydanie orzeczenia w trybie prejudycjalnym zatrzymywane przez służby wywiadu i bezpieczeństwa i pozostają do ich dyspozycji dla celów ich działalności, podobnie jak inne bazy danych utrzymywane przez te służby. W szczególności uzyskane w ten sposób dane, poddane przetwarzaniu i masowym zautomatyzowanym analizom, mogą być porównywane krzyżowo z danymi pochodzącymi z innych baz danych, zawierających różne kategorie masowych danych osobowych lub być udostępniane poza tymi służbami i państwom trzecim. Wreszcie czynności te nie podlegają obowiązkowi uzyskania uprzedniej zgody sądu ani niezależnego organu administracji i nie powodują przekazania żadnej informacji osobom, których dane dotyczą.

53 Dyrektywa 2002/58 ma na celu, jak wynika w szczególności z jej motywów 6 i 7, ochronę użytkowników usług łączności elektronicznej przed zagrożeniami dla ich danych osobowych i ich życia prywatnego wynikającymi z nowych technologii, a w szczególności ze zwiększonej zdolności do automatycznego zatrzymywania i przetwarzania danych. W szczególności, omawiana dyrektywa zmierza, jak wynika z jej motywu 2, do zapewnienia pełnego poszanowania praw określonych w art. 7 i 8 karty. W tym względzie z uzasadnienia wniosku 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, 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".

54 W tym względzie w art. 5 ust. 1 dyrektywy 2002/58 przewidziano, że „[p]aństwa 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 tym samym przepisie podkreślono także, że „[w] szczególności [państwa członkowskie] 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" oraz wyjaśniono, że „[ten] ustęp nie zabrania technicznego przechowywania, które jest niezbędne do przekazania komunikatu bez uszczerbku dla zasady poufności".

55 Tak więc w owym art. 5 ust. 1 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 tej komunikacji i tych danych bez ich zgody. Z uwagi na ogólne sformułowanie tego przepisu obejmuje on siłą rzeczy każdą czynność pozwalającą osobom trzecim na zapoznanie się z komunikacją i związanymi z nią danymi w celach innych niż transmisja komunikatu.

56 Zakaz przechwytywania komunikacji i związanych z nią danych zawarty w art. 5 ust. 1 dyrektywy 2002/58 obejmuje więc każdą formę udostępniania przez dostawców usług łączności elektronicznych danych o ruchu i danych o lokalizacji organom publicznym, takim jak służby wywiadu i bezpieczeństwa, a także zatrzymywanie omawianych danych przez te służby, bez względu na sposób ich dalszego wykorzystania.

57 Tak więc poprzez przyjęcie tej dyrektywy prawodawca Unii skonkretyzował prawa ustanowione w art. 7 i 8 karty 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 utrwalane bez ich zgody (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, pkt 109).

58 Jednakże art. 15 ust. 1 dyrektywy 2002/58 pozwala państwom członkowskim na wprowadzenie wyjątków od ustanowionej w art. 5 ust. 1 tej dyrektywy zasady gwarantowania poufności danych osobowych, a także od korespondujących z nią obowiązków wymienionych w szczególności w art. 6 i 9 omawianej dyrektywy, kiedy takie ograniczenie jest niezbędne, właściwe i proporcjonalne w społeczeństwie demokratycznym do ochrony bezpieczeństwa narodowego, obronności i bezpieczeństwa publicznego lub do zapobiegania, dochodzenia, wykrywania i ścigania przestępstw kryminalnych lub niedozwolonego używania systemu łączności elektronicznej. W tym celu państwa członkowskie mogą między innymi przyjmować środki ustawodawcze przewidujące zatrzymywanie danych przez określony czas, jeśli jest to uzasadnione jednym z tych względów.

59 Jednakże ta możliwość wprowadzenia odstępstwa od praw i obowiązków przewidzianych w art. 5, 6 i 9 dyrektywy 2002/58 nie może uzasadniać tego, że odstępstwo od mającego zasadnicze znaczenie obowiązku zapewnienia poufności łączności elektronicznej i danych z nią związanych,

a w szczególności zakazu przechowywania tych danych, wyraźnie przewidzianego w art. 5 tej dyrektywy, stanie się regułą (zob. podobnie wyroki: z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 89, 104; a także z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, pkt 111).

60 Ponadto z art. 15 ust. 1 zdanie trzecie dyrektywy 2002/58 wynika, że państwa członkowskie są upoważnione do przyjmowania środków ustawodawczych zmierzających do ograniczenia zakresu praw i obowiązków, o których mowa w art. 5, 6 i 9 tej dyrektywy, jedynie z poszanowaniem zasad ogólnych prawa Unii, do których należy zasada proporcjonalności, i praw podstawowych gwarantowanych w karcie. W tym względzie Trybunał orzekł już, że nałożony na dostawców usług łączności elektronicznej przez uregulowanie krajowe obowiązek zatrzymywania danych o ruchu w celu ewentualnego udostępniania ich właściwym organom krajowym rodzi pytania dotyczące zgodności nie tylko z art. 7 i 8 karty, dotyczącymi, odpowiednio, ochrony życia prywatnego oraz ochrony danych osobowych, lecz również z art. 11 karty, dotyczącym wolności wypowiedzi (zob. podobnie wyroki: z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 25, 70; a także z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 91, 92 i przytoczone tam orzecznictwo).

61 Te same pytania powstają również w odniesieniu do innych rodzajów przetwarzania danych, takich jak ich transmitowanie osobom innym niż użytkownicy lub dostęp do tych danych z zamiarem ich wykorzystania [zob. analogicznie opinia 1/15 (Umowa PNR UE–Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 122, 123 i przytoczone tam orzecznictwo].

62 Tak więc przy wykładni art. 15 ust. 1 dyrektywy 2002/58 należy uwzględnić wagę zarówno prawa do poszanowania życia prywatnego, gwarantowanego w art. 7 karty, jak i prawa do ochrony danych osobowych, gwarantowanego w art. 8 karty, w postaci wynikającej z orzecznictwa Trybunału, a także prawa do wolności wypowiedzi, ponieważ to prawo podstawowe, zagwarantowane w art. 11 karty, stanowi jeden z istotnych fundamentów pluralistycznego i demokratycznego społeczeństwa, stanowiąc część wartości, na jakich zgodnie z art. 2 TUE opiera się Unia (zob. podobnie wyroki: z dnia 6 marca 2001 r., Connolly/Komisja, C-274/99 P, EU:C:2001:127, pkt 39; z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 93 i przytoczone tam orzecznictwo).

63 Niemniej jednak 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 (zob. podobnie wyrok z dnia 16 lipca 2020 r., Facebook Ireland i Schrems, C-311/18, EU:C:2020:559, pkt 172 i przytoczone tam orzecznictwo).

64 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 i z poszanowaniem zasady proporcjonalności są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

65 Należy dodać, że wymóg, zgodnie z którym wszelkie ograniczenia korzystania z praw podstawowych muszą być przewidziane ustawą, oznacza, że podstawa prawna, która pozwala na ingerencję w te prawa, musi sama określać zakres ograniczenia wykonywania danego prawa (wyrok z dnia 16 lipca 2020 r., Facebook Ireland i Schrems, C-311/18, EU:C:2020:559, pkt 175 i przytoczone tam orzecznictwo).

66 Co się tyczy poszanowania zasady proporcjonalności, w art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 przewidziano, że państwa członkowskie mogą uchwalić środek stanowiący odstępstwo od zasady poufności komunikacji i związanych z nią danych o ruchu, gdy taki środek jest „niezbędny, właściwy i proporcjonalny w ramach społeczeństwa demokratycznego” z punktu widzenia celów wymienionych w tym przepisie. W motywie 11 tej dyrektywy wyjaśniono, że środek tego rodzaju musi być „współmierny” do zamierzonego celu.

67 W tym względzie należy przypomnieć, że ochrona prawa podstawowego do poszanowania życia prywatnego wymaga zgodnie z utrwalonym orzecznictwem Trybunału, aby odstępstwa od ochrony danych osobowych i jej ograniczenia mieściły się w ramach tego, co ściśle konieczne. 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 i interesami a rozpatrywanymi prawami [zob. podobnie wyroki: z dnia 16 grudnia 2008 r., Satakunnan Markkinapörssi i Satamedia, C-73/07, EU:C:2008:727, pkt 56; z dnia 9 listopada 2010 r., Volker und Markus Schecke i Eifert, C-92/09 i C-93/09, EU:C:2010:662, pkt 76, 77, 86; a także z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 52; opinia 1/15 (Umowa PNR UE–Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 140].

68 Aby spełniać wymóg proporcjonalności, uregulowanie 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 ryzykiem nadużyć. To uregulowanie 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 jeszcze 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, jaką są dane szczególnie chronione [zob. podobnie wyroki: z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 54, 55; a także z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 117; opinia 1/15 (Umowa PNR UE–Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 141].

69 Co się tyczy kwestii, czy uregulowanie krajowe takie jak rozpatrywane w postępowaniu głównym spełnia wymogi zawarte w art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, należy wskazać, że transmitowanie danych o ruchu i danych o lokalizacji osobom innym niż użytkownicy, takim jak służby wywiadu i bezpieczeństwa, stanowi odstępstwo od zasady poufności. Kiedy dzieje się to, jak w niniejszej sprawie, w sposób uogólniony i niezróżnicowany, odstąpienie od mającego zasadnicze znaczenie obowiązku zagwarantowania poufności danych staje się regułą, podczas gdy system wprowadzony dyrektywą 2002/58 wymaga, aby takie odstępstwo pozostało wyjątkiem.

70 Ponadto, zgodnie z utrwalonym orzecznictwem Trybunału, transmisja danych o ruchu i danych o lokalizacji osobie trzeciej stanowi ingerencję w prawa podstawowe ustanowione w art. 7 i 8 karty, bez względu na sposób późniejszego wykorzystania tych danych. W tym względzie nie ma znaczenia, 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 [zob. podobnie opinia 1/15 (Umowa PNR UE–Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 124. 126 i przytoczone tam orzecznictwo; a także wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, pkt 115, 116].

71 Ingerencję w prawo ustanowione w art. 7 karty, jaką stanowi transmitowanie danych o ruchu i danych o lokalizacji służbom wywiadu i bezpieczeństwa, należy uważać za szczególnie poważną, biorąc pod uwagę między innymi okoliczność, że z danych tych mogą wynikać informacje szczególnie chronione, a zwłaszcza możliwość sporządzenia na ich podstawie profilu osób, których dane dotyczą, zaś taka informacja jest w tym samym stopniu szczególnie chroniona jak sama treść komunikacji. Ponadto może ona wywoływać u osób, których dane dotyczą, wrażenie, że ich prywatne życie podlega ciągłej obserwacji (zob. analogicznie wyroki: z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 27, 37; a także z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 99, 100).

72 Należy również wskazać, że transmitowanie organom publicznym danych o ruchu i danych o lokalizacji w celach związanych z bezpieczeństwem może samo w sobie naruszać prawo do poszanowania komunikacji, ustanowione w art. 7 karty, i wpływać zniechęcająco na wykonywanie przez użytkowników środków łączności elektronicznej ich wolności wypowiedzi, zagwarantowanej w art. 11 karty. Taki zniechęcający wpływ może zostać wywarty w szczególności na osoby, których komunikacja podlega zgodnie z prawem krajowym tajemnicy zawodowej, oraz na sygnalistów, których działalność chroni dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (UE) (Dz.U. 2019, L 305, s. 17). Ponadto skutki te są tym dotkliwsze, że zatrzymywane dane są bardzo liczne i zróżnicowane (zob. podobnie wyroki: z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 28; z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 101; a także z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, pkt 118).

73 Wreszcie, z uwagi na okoliczność, że znaczna ilość danych o ruchu i danych o lokalizacji może być zatrzymywana w sposób ciągły przy użyciu środka uogólnionego 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.

74 Co się tyczy celów, które mogłyby uzasadnić takie ingerencje, a bardziej konkretnie rozpatrywanego w postępowaniu głównym celu ochrony bezpieczeństwa narodowego, należy wskazać na wstępie, że art. 4 ust. 2 TUE stanowi, iż bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego. Odpowiedzialność ta obejmuje pierwszorzędny interes w ochronie podstawowych funkcji państwa i podstawowych interesów społeczeństwa, a także zapobieganie i ściganie działalności mogącej poważnie zdestabilizować podstawowe struktury konstytucyjne, polityczne lub społeczne kraju, w szczególności bezpośrednio zagrozić społeczeństwu, ludności lub państwu jako takiemu, takiej jak w szczególności działalność terrorystyczna (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, pkt 135).

75 Znaczenie celu ochrony bezpieczeństwa narodowego w związku z art. 4 ust. 2 TUE wykracza poza inne cele, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, w szczególności cele zwalczania przestępstw, choćby poważnych, a także ochrony bezpieczeństwa publicznego. Zagrożenia takie jak te, o których mowa w poprzednim punkcie, różnią się bowiem ze względu na swój charakter i szczególną wagę od ogólnych zagrożeń powstania napięć i problemów, choćby poważnych, dla bezpieczeństwa publicznego. Z zastrzeżeniem poszanowania innych wymogów przewidzianych w art. 52 ust. 1 karty cel ochrony bezpieczeństwa narodowego może więc uzasadnić środki związane z dalej idącą ingerencją w prawa podstawowe niż w przypadku tych innych celów (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, pkt 136).

76 Niemniej jednak aby spełnić wymóg proporcjonalności przypomniany w pkt 67 niniejszego wyroku, zgodnie z którym odstępstwa od ochrony danych osobowych i jej ograniczenia muszą następować w granicach tego, co ściśle konieczne, uregulowanie krajowe związane z ingerencją w prawa podstawowe ustanowione w art. 7 i 8 karty musi szanować wymogi wynikające z orzecznictwa przytoczonego w pkt 65, 67 i 68 niniejszego wyroku.

77 W szczególności, co się tyczy dostępu organu do danych osobowych, uregulowanie nie może ograniczać się do wymagania, aby dostęp organów do danych odpowiadał celowi, do którego zmierza to uregulowanie, ale musi również przewidywać warunki materialne i proceduralne regulujące to wykorzystanie [zob. analogicznie opinia 1/15 (Umowa PNR UE–Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 192 i przytoczone tam orzecznictwo].

78 I tak skoro uogólniony dostęp do wszystkich zatrzymanych danych, niezależnie od jakiegokolwiek związku, nawet pośredniego, z realizowanym celem nie może być uważany za ograniczony do tego, co absolutnie niezbędne, przepisy krajowe regulujące dostęp do danych o ruchu i danych o lokalizacji winny opierać się na obiektywnych kryteriach umożliwiających określenie okoliczności i warunków

udzielenia dostępu właściwym organom krajowym do rozpatrywanych danych (zob. podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 119 i przytoczone tam orzecznictwo).

79 Wymogi te mają zastosowanie tym bardziej do środków ustawodawczych takich jak środek rozpatrywany w postępowaniu głównym, na podstawie którego właściwe organy krajowe mogą zobowiązać dostawców usług łączności elektronicznej do ujawnienia danych o ruchu i danych o lokalizacji poprzez transmitowanie ich służbom wywiadu i bezpieczeństwa w sposób uogólniony i niezróżnicowany. Taka transmisja skutkuje bowiem udostępnieniem tych danych organom publicznym [zob. analogicznie opinia 1/15 (Umowa PNR UE–Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 212].

80 W sytuacji gdy transmisja danych o ruchu i danych o lokalizacji następuje w sposób uogólniony i niezróżnicowany, dotyczy ona ogólnie wszystkich osób używających usług łączności elektronicznej. Dotyczy ona zatem nawet osób, w przypadku których nic nie wskazuje na to, że należy uważać, iż ich zachowanie mogłoby mieć związek, choćby pośredni lub odległy, z celem ochrony bezpieczeństwa narodowego, a w szczególności w przypadku których nie ustalono związku między danymi, których transmisja została przewidziana, a zagrożeniem dla bezpieczeństwa narodowego (zob. podobnie wyroki: z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 57, 58; a także z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 105). Biorąc pod uwagę okoliczność, że transmisja takich danych organom publicznym, zgodnie z tym, co stwierdzono w pkt 79 niniejszego wyroku, oznacza dostęp, należy uznać, że uregulowanie umożliwiające uogólnioną i niezróżnicowaną transmisję danych organom publicznym oznacza uogólniony dostęp.

81 Wynika z tego, że uregulowanie krajowe nakładające na dostawców usług łączności elektronicznej obowiązek ujawnienia danych o ruchu i danych o lokalizacji poprzez ich uogólnioną i niezróżnicowaną transmisję służbom wywiadu i bezpieczeństwa wykracza poza granice tego, co ściśle konieczne, i nie może być uważane za uzasadnione w społeczeństwie demokratycznym, jak tego wymaga art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 4 ust. 2 TUE, a także art. 7, 8 i 11 oraz 52 ust. 1 karty.

82 Biorąc pod uwagę całość powyższych rozważań, na pytanie drugie należy udzielić odpowiedzi, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 4 ust. 2 TUE, a także art. 7, 8 i 11 oraz 52 ust. 1 karty, należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu umożliwiającemu organowi państwa nałożenie na dostawców usług łączności elektronicznej obowiązku uogólnionego i niezróżnicowanego transmitowania służbom wywiadu i bezpieczeństwa danych o ruchu i danych o lokalizacji do celów ochrony bezpieczeństwa narodowego.

W przedmiocie kosztów

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

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

1) **Artykuł 1 ust. 3, art. 3 i 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 (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. 4 ust. 2 TUE należy interpretować w ten sposób, że zakresem stosowania tej dyrektywy objęte jest uregulowanie krajowe umożliwiające organowi**

państwa zobowiązanie dostawców usług łączności elektronicznej do transmitowania służbom wywiadu i bezpieczeństwa danych o ruchu i danych o lokalizacji do celów ochrony bezpieczeństwa narodowego.

2) **Artykuł 15 ust. 1 dyrektywy 2002/58, zmienionej dyrektywą 2009/136, w związku z art. 4 ust. 2 TUE, a także art. 7, 8 i 11 oraz 52 ust. 1 Karty praw podstawowych Unii Europejskiej, należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu umożliwiającemu organowi państwa nałożenie na dostawców usług łączności elektronicznej obowiązku uogólnionego i niezróżnicowanego transmitowania służbom wywiadu i bezpieczeństwa danych o ruchu i danych o lokalizacji do celów ochrony bezpieczeństwa narodowego.**

Podpisy