Zbiór Orzeczeń

WYROK TRYBUNAŁU (wielka izba)

z dnia 2 października 2018 r.*

Odesłanie prejudycjalne – Łączność elektroniczna – Przetwarzanie danych osobowych – Dyrektywa 2002/58/WE – Artykuły 1 i 3 – Zakres stosowania – Poufność łączności elektronicznej – Ochrona – Artykuł 5 i art. 15 ust. 1 – Karta praw podstawowych Unii Europejskiej – Artykuły 7 i 8 – Dane przetwarzane w związku ze świadczeniem usług łączności elektronicznej – Dostęp organów krajowych do danych do celów dochodzenia – Próg wagi naruszenia mogący uzasadniać dostęp do danych

W sprawie C-207/16

mającej za przedmiot wniosek o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożony przez Audiencia Provincial de Tarragona (sąd okręgowy w Tarragonie, Hiszpania) postanowieniem z dnia 6 kwietnia 2016 r., które wpłynęło do Trybunału w dniu 14 kwietnia 2016 r., w postępowaniu wszczętym przez

Ministerio Fiscal,

TRYBUNAŁ (wielka izba),

w składzie: K. Lenaerts, prezes, A. Tizzano, wiceprezes, R. Silva de Lapuerta, T. von Danwitz (sprawozdawca), J.L. da Cruz Vilaça, C.G. Fernlund i C. Vajda, prezesi izb, E. Juhász, A. Borg Barthet, C. Toader, M. Safjan, D. Šváby, M. Berger, E. Jarašiūnas, i E. Regan, sędziowie,

rzecznik generalny: H. Saugmandsgaard Øe,

sekretarz: L. Carrasco Marco, administrator,

uwzględniając pisemny etap postępowania i po przeprowadzeniu rozprawy w dniu 29 stycznia 2018 r.,

rozważywszy uwagi przedstawione:

– w imieniu Ministerio Fiscal przez E. Tejadę de la Fuente,

– w imieniu rządu hiszpańskiego przez M. Sampola Pucurulla, działającego w charakterze pełnomocnika,

– w imieniu rządu czeskiego przez M. Smolka, J. Vláčila i A. Brabcovą, działających w charakterze pełnomocników,

– w imieniu rządu duńskiego przez J. Nymanna-Lindegrena i M. Wolff, działających w charakterze pełnomocników,

* Język postępowania: hiszpański.

– w imieniu rządu estońskiego przez N. Grünberg, działającą w charakterze pełnomocnika,

– w imieniu Irlandii przez M. Browne, L. Williams, E. Creedon i A. Joyce'a, działających w charakterze pełnomocników, wspieranych przez E. Gibson, BL,

– w imieniu rządu francuskiego przez D. Colasa, E. de Moustier i E. Armoet, działających w charakterze pełnomocników,

– w imieniu rządu łotewskiego przez I. Kucinę i J. Davidovičę, działające w charakterze pełnomocników,

– w imieniu rządu węgierskiego przez M. Fehéra i G. Koósa, działających w charakterze pełnomocników,

– w imieniu rządu austriackiego przez C. Pesendorfer, działającą w charakterze pełnomocnika,

– w imieniu rządu polskiego przez B. Majczynę, D. Lutostańską i J. Sawicką, działających w charakterze pełnomocników,

– w imieniu rządu Zjednoczonego Królestwa przez S. Brandona i C. Brodie, działających w charakterze pełnomocników, wspieranych przez C. Knighta, barrister, i G. Facennę, QC,

– w imieniu Komisji Europejskiej przez I. Martínez del Peral, P. Costę de Oliveirę, R. Troostersa i D. Nardiego, działających w charakterze pełnomocników,

po zapoznaniu się z opinią rzecznika generalnego na posiedzeniu w dniu 3 maja 2018 r.,

wydaje następujący

Wyrok

1 Przedmiotem wniosku o wydanie orzeczenia w trybie prejudycjalnym jest w istocie wykładnia art. 15 ust. 1 dyrektywy Parlamentu Europejskiego i Rady 2002/58/WE z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywy o prywatności i łączności elektronicznej) (Dz.U. 2002, L 201, s. 37 – wyd. spec. w jęz. polskim, rozdz. 13, t. 29, s. 514), 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. 7, 8 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą").

2 Wniosek ten został złożony w ramach skargi wniesionej przez Ministerio Fiscal (prokuraturę, Hiszpania) na decyzję Juzgado de Instrucción nº 3 de Tarragona (sądu śledczego nr 3 w Tarragonie, zwanego dalej „sądem śledczym") w przedmiocie odmowy przyznania policji dostępu do danych osobowych przechowywanych przez dostawców usług łączności elektronicznej.

Ramy prawne

Prawo Unii

Dyrektywa 95/46

3 Zgodnie z art. 2 lit. b) dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. 1995, L 281, s. 31 – wyd. spec. w jęz. polskim, rozdz. 13, t. 15, s. 355), do celów tej dyrektywy pojęcie „przetwarzania danych osobowych" oznacza „każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie".

4 Artykuł 3 tej dyrektywy, zatytułowany „Zakres obowiązywania", stanowi:

„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 Traktatu o Unii Europejskiej, 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

5 Motywy 2, 11, 15 i 21 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 [k]arty.

[…]

(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 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 [przysługujące państwom członkowskim] możliwości […] 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, dla której wykładnię stanowi

orzecznictwo Europejskiego Trybunału Praw Człowieka. Środki tego rodzaju muszą być właściwe, współmierne do zamierzonego celu i niezbędne w społeczeństwie demokratycznym oraz powinny podlegać stosownym zabezpieczeniom zgodnie z europejską Konwencją o ochronie praw człowieka i podstawowych wolności.

[…]

(15) Komunikat może obejmować wszelkiego rodzaju nazwy, liczby lub adresy dostarczone przez nadawcę komunikatu lub użytkownika połączenia w celu przeprowadzenia łączności. Dane o ruchu mogą obejmować wszelkiego rodzaju przekształcanie tej informacji w sieci, przez którą nadawany jest komunikat, do celów przeprowadzenia operacji przesłania danych. […]

[…]

(21) W celu ochrony przed niedozwolonym dostępem do komunikatów należy podjąć odpowiednie środki, aby zapewnić ochronę poufności łączności, włączając zarówno treść, jak i dane związane z tego rodzaju komunikatem, przy pomocy publicznych sieci łączności i publicznie dostępnych usług łączności elektronicznej. Ustawodawstwo krajowe w niektórych państwach członkowskich zabrania jedynie zamierzonego niedozwolonego dostępu do komunikatów.”.

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

„1. Niniejsza dyrektywa harmonizuje przepisy państw członkowskich wymagane dla zapewnienia równoważnego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do prywatności, 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 ustanawiającego Wspólnotę Europejską, takiej jak działalność określona w tytułach V i VI Traktatu o Unii Europejskiej, ani w żadnym wypadku do działalności dotyczącej bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając dobrobyt gospodarczy państwa, gdy działalność odnosi się do spraw bezpieczeństwa państwa) i działalności państwa w dziedzinie prawa karnego”.

7 Artykuł 2 dyrektywy 2002/58, zatytułowany „Definicje”, stanowi:

„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 (dyrektywy ramowej) [(Dz.U. 2002, L 108, s. 33 – wyd. spec. w jęz. polskim, rozdz. 13, t. 29, s. 349)].

Stosuje się również następujące definicje:

[…]

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. […]

[…]

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. […]".

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 [lub w którym można dochodzić jego zapłaty].

[…]".

11 Artykuł 15 tej dyrektywy, 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 (i.e. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania [ścigania] przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy [95/46]. 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 Traktatu o Unii Europejskiej”.

Prawo hiszpańskie

Ustawa 25/2007

12 Artykuł 1 Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a la redes públicas de comunicaciones (ustawy 25/2007 w sprawie zatrzymywania danych dotyczących łączności elektronicznej i publicznych sieci łączności) z dnia 18 października 2007 r. (BOE nr 251 z dnia 19 października 2007 r., s. 42517) stanowi:

„1. Niniejsza ustawa ma na celu regulację ciążącego na operatorach obowiązku zatrzymywania danych generowanych lub przetwarzanych w związku ze świadczeniem usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz obowiązku przekazywania tych danych upoważnionym przedstawicielom na każdy wniosek na podstawie odpowiedniej zgody sądu, w celu zapobiegania, wykrywania i ścigania poważnych przestępstw, o których mowa w kodeksie karnym lub w specjalnych ustawach.

2. Niniejsza ustawa ma zastosowanie do danych o ruchu i lokalizacji, dotyczących zarówno osób fizycznych, jak i prawnych oraz do powiązanych z nimi danych niezbędnych do identyfikacji abonenta lub zarejestrowanego użytkownika.

[…]”.

Kodeks karny

13 Artykuł 13 ust. 1 Ley Orgánica 10/1995 del Código Penal (kodeksu karnego) z dnia 23 listopada 1995 r. (BOE nr 281 z dnia 24 listopada 1995 r., s. 33987) brzmi następująco:

„Stanowią poważne przestępstwa te, które są zagrożone w ustawie surową karą”.

14 Artykuł 33 wspomnianego kodeksu przewiduje:

„1. Ze względu na ich charakter i okres trwania kary dzielą się na surowe, mniej surowe oraz łagodne.

2. Karami surowymi są:

a) dożywotnie pozbawienie wolności, które może podlegać zmianie;

b) pozbawienie wolności powyżej pięciu lat.

[…]”.

Kodeks postępowania karnego

15 Po czasie wystąpienia okoliczności faktycznych, których dotyczy postępowanie główne, Ley de Enjuiciamiento Criminal (kodeks postępowania karnego) został zmieniony przez Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (ustawę organiczną 13/2015 zmieniającą kodeks postępowania karnego w celu wzmocnienia gwarancji procesowych i uregulowania środków technologicznego dochodzenia) z dnia 5 października 2015 r. (BOE nr 239 z dnia 6 października 2015 r., s. 90192).

16 Ustawa ta weszła w życie w dniu 6 grudnia 2015 r. Wprowadza ona do kodeksu postępowania karnego dziedzinę dostępu do danych dotyczących komunikatów telefonicznych i telematycznych, zatrzymywanych przez dostawców usług łączności elektronicznej.

17 Artykuł 579 ust. 1 kodeksu postępowania karnego, w brzmieniu ustalonym ustawą organiczną 13/2015, stanowi:

„1. Sąd może zezwolić na przechwytywanie prywatnej korespondencji pocztowej i telegraficznej, w tym faksu, Burofaxu i międzynarodowych przekazów pocztowych, którą podejrzany wysyła lub otrzymuje, oraz jej otwarcie i badanie, jeżeli istnieją przesłanki pozwalające sądzić, że pozwoli to wykryć lub potwierdzić czyn lub okoliczność lub czynnik istotne dla sprawy, w przypadku gdy dochodzenie dotyczy następujących przestępstw:

1) przestępstw umyślnych zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej trzy lata;

2) przestępstw popełnionych w ramach grupy lub organizacji przestępczej;

3) przestępstwo charakterze terrorystycznym.

[…]”.

18 Artykuł 588 ter j wspomnianego kodeksu przewiduje:

„1. Dane elektroniczne zatrzymywane przez usługodawców lub osoby umożliwiające komunikowanie się zgodnie z ustawodawstwem o zatrzymywaniu danych o połączeniach elektronicznych albo z ich własnej inicjatywy z powodów handlowych, albo z innych, i które są związane z komunikowaniem się, będą mogły zostać przekazane w celu ich uwzględnienia w postępowaniu tylko za zgodą sądu.

2. W sytuacji gdy znajomość tych danych okaże się niezbędna dla dochodzenia, należy zwrócić się do właściwego sądu z wnioskiem o udzielenie zgody na dostęp do informacji znajdujących się w zautomatyzowanych archiwach usługodawców, w szczególności w celu krzyżowego lub inteligentnego poszukiwania danych, pod warunkiem że zostały określone charakter danych, które mają być poznane i powody uzasadniające ich przekazanie”.

Postępowanie główne i pytania prejudycjalne

19 P. Hernandez Sierra złożył na policji zawiadomienie o popełnieniu rozboju, do którego doszło w dniu 16 lutego 2015 r., w wyniku którego doznał obrażeń i dokonano zaboru jego portfela i telefonu komórkowego.

20 W dniu 27 lutego 2015 r. policja zwróciła się do sądu śledczego z wnioskiem o nakazanie różnym dostawcom usług łączności elektronicznej przekazania numerów telefonicznych działających, między dniem 16 lutego i dniem 27 lutego 2015 r., z numerem identyfikacyjnym telefonu komórkowego (zwanego dalej „numerem IMEI") skradzionego telefonu komórkowego, a także danych osobowych dotyczących tożsamości posiadaczy lub użytkowników numerów telefonicznych odpowiadających kartom SIM działających z tym numerem, takich jak imię, nazwisko oraz, w stosownych przypadkach, adres.

21 Postanowieniem z dnia 5 maja 2015 r. sąd śledczy oddalił ten wniosek. Po pierwsze, orzekł, że żądany środek nie był potrzebny w celu identyfikacji sprawców przestępstwa. Po drugie, odmówił uwzględnienia wniosku ze względu na to, że ustawa 25/2007 ogranicza przekazywanie danych zatrzymywanych przez dostawców usług łączności elektronicznej do poważnych przestępstw. Zgodnie z kodeksem karnym poważne przestępstwa zagrożone są karą pozbawienia wolności powyżej pięciu lat, natomiast okoliczności faktyczne w postępowaniu głównym nie wydają się stanowić takiego przestępstwa.

22 Prokuratura wniosła apelację od tego postanowienia do sądu odsyłającego, mając na uwadze, że przekazanie omawianych danych powinno było zostać umożliwione z uwagi na charakter okoliczności faktycznych i na mocy wyroku Tribunal Supremo (sądu najwyższego, Hiszpania) z dnia 26 lipca 2010 r. dotyczącego podobnej sprawy.

23 Sąd odsyłający wyjaśnia, że po tym, jak nastąpiło wydanie wspomnianego postanowienia, ustawodawca hiszpański zmienił kodeks postępowania karnego, przyjmując ustawę organiczną 13/2015. Ustawa ta, która jest istotna dla rozstrzygnięcia skargi w postępowaniu głównym, wprowadziła dwa nowe alternatywne kryteria w celu określenia, jak poważne jest dane przestępstwo. Chodzi, po pierwsze, o kryterium materialne określone przez zachowania odpowiadające kwalifikacji karnej, których charakter przestępczy jest szczególny i poważny i które mają szczególnie niekorzystny skutek dla indywidualnych i zbiorowych interesów prawnych. Po drugie, ustawodawca krajowy posłużył się formalnym kryterium prawnym opartym na karze przewidzianej za dane przestępstwo. Przewidziany w nim obecnie próg trzech lat pozbawienia wolności obejmuje jednak ogromną większość przestępstw. Ponadto sąd odsyłający uważa, że interes państwa w zwalczaniu bezprawnych czynów nie może uzasadniać nieproporcjonalnej ingerencji w prawa podstawowe ustanowione w karcie.

24 W tym względzie sąd ten uważa, że w postępowaniu głównym dyrektywy 95/46 i 2002/58 ustanawiają powiązanie z kartą. Uregulowanie krajowe rozpatrywane w postępowaniu głównym jest objęte zatem, zgodnie z art. 51 ust. 1 karty, jej zakresem stosowania, pomimo stwierdzenia nieważności dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE (Dz.U. 2006, L 105, s. 54) wyrokiem z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in. (C-293/12 i C-594/12, EU:C:2014:238).

25 W wyroku tym Trybunał uznał, że przechowywanie i udostępnianie danych o ruchu stanowią poważną ingerencję w prawa gwarantowane w art. 7 i 8 karty i określił kryteria oceny zgodności z zasadą proporcjonalności, w tym wagę naruszeń uzasadniającą przechowywanie tych danych i dostęp do nich do celów dochodzenia.

26 W tej sytuacji Audiencia Provincial de Tarragona (sąd okręgowy w Tarragonie) postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„1) Czy można określić wystarczającą wagę przestępstwa, jako kryterium uzasadniające ingerencję w prawa podstawowe uznane w art. 7 i 8 [karty], jedynie ze względu na karę grożącą za przestępstwo będące przedmiotem dochodzenia, czy też jest ponadto konieczne wskazanie w przestępczym zachowaniu szczególnie niekorzystnego skutku dla indywidualnych lub publicznych interesów prawnych?

2) W danym przypadku, gdyby określenie wagi przestępstwa jedynie w zależności od kary, która może zostać nałożona, było zgodne z podstawowymi zasadami Unii zastosowanymi przez Trybunał w wyroku [z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238] jako kryterium ścisłej kontroli dyrektywy [2002/58], jaki powinien być minimalny poziom tej kary? Czy dopuszczalne jest ustalenie tego minimalnego poziomu w sposób ogólny na trzy lata pozbawienia wolności?”.

Postępowanie przed Trybunałem

27 Na mocy postanowienia prezesa Trybunału z dnia 23 maja 2016 r. postępowanie przed Trybunałem zostało zawieszone do czasu wydania wyroku z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970, zwanego dalej „wyrokiem Tele2 Sverige i Watson i in.”). W następstwie wydania tego wyroku sąd odsyłający został zapytany, czy chce podtrzymać, czy też wycofać swój wniosek o wydanie orzeczenia w trybie prejudycjalnym. W odpowiedzi sąd odsyłający, w piśmie z dnia 30 stycznia 2017 r., które wpłynęło do Trybunału w dniu 14 lutego 2017 r., wskazał, że uważa, iż wyrok ten nie pozwala na ocenienie z wystarczającą pewnością rozpatrywanego w postępowaniu głównym uregulowania krajowego z punktu widzenia prawa Unii. W konsekwencji postępowanie przed Trybunałem podjęto w dniu 16 lutego 2017 r.

W przedmiocie pytań prejudycjalnych

28 Rząd hiszpański podnosi, po pierwsze, brak właściwości Trybunału do udzielenia odpowiedzi na wniosek o wydanie orzeczenia w trybie prejudycjalnym, a po drugie, niedopuszczalność takiego wniosku.

W przedmiocie właściwości Trybunału

29 W uwagach na piśmie przedstawionych Trybunałowi rząd hiszpański przedstawił stanowisko, podzielone na rozprawie przez rząd Zjednoczonego Królestwa, w myśl którego Trybunał nie jest właściwy do udzielenia odpowiedzi na wniosek o wydanie orzeczenia w trybie prejudycjalnym ze względu na to, że sprawa, której dotyczy postępowanie główne, jest zgodnie z art. 3 ust. 2 tiret pierwsze dyrektywy 95/46 i art. 1 ust. 3 dyrektywy 2002/58 wyłączona z zakresu stosowania tych dwóch dyrektyw. Sprawa ta nie jest zatem objęta zakresem stosowania prawa Unii, wobec czego karta, zgodnie z jej art. 51 ust. 1, nie znajduje zastosowania.

30 Zdaniem rządu hiszpańskiego Trybunał stwierdził wprawdzie w wyroku Tele2 Sverige i Watson i in., że środek prawny, regulujący dostęp organów krajowych do danych zatrzymywanych przez dostawców usług łączności elektronicznej wchodzi w zakres stosowania dyrektywy 2002/58, jednak w niniejszym przypadku chodzi o żądanie udzielenia dostępu organom publicznym, na mocy decyzji sądowej wydanej w ramach dochodzenia w postępowaniu karnym, do danych osobowych zatrzymywanych przez dostawców usług łączności elektronicznej. Rząd hiszpański wnioskuje z tego, że przedmiotowy

wniosek wpisuje się w ramy wykonywania przez właściwe organy krajowe, ius puniendi, wobec czego stanowi on działalność państwa w obszarach prawa karnego objętą wyjątkiem przewidzianym w art. 3 ust. 2 tiret pierwsze dyrektywy 95/46 oraz w art. 1 ust. 3 dyrektywy 2002/58.

31 W celu dokonania oceny tego wyjątku dotyczącego braku właściwości należy zauważyć, że zgodnie z art. 1 ust. 1 dyrektywa 2002/58 przewiduje harmonizację przepisów krajowych wymaganych do, między innymi, zapewnienia równego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do prywatności i poufności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej. Zgodnie z jej art. 1 ust. 2 wspomniana dyrektywa dookreśla i uzupełnia dyrektywę 95/46 zgodnie z celami przedstawionymi w ust. 1.

32 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 (wyrok Tele2 Sverige i Watson i in., pkt 69 i przytoczone tam orzecznictwo). Rodzaje działalności, które zostały w nim wymienione tytułem przykładu, stanowią w każdym wypadku działalność właściwą państwom i organom państwowym, odmienną od dziedzin działalności podmiotów indywidualnych (zob. analogicznie, w odniesieniu do art. 3 ust. 2 tiret pierwsze dyrektywy 95/46, wyrok z dnia 10 lipca 2018 r., Jehovan todistajat, C-25/17, EU:C:2018:551, pkt 38 i przytoczone tam orzecznictwo).

33 Artykuł 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"). W konsekwencji należy uznać, że dyrektywa ta odnosi się do działalności dostawców tych usług (wyrok Tele2 Sverige i Watson i in., pkt 70).

34 W odniesieniu do art. 15 ust. 1 dyrektywy 2002/58 Trybunał orzekł już, że środki ustawodawcze, o których mowa w tym postanowieniu, są objęte zakresem stosowania tej dyrektywy, nawet jeśli odnoszą się do działalności właściwej państwom lub organom państwowym i niezwiązanej z dziedzinami, w których prowadzą działalność jednostki, nawet jeżeli cele, którym środki te mają służyć, są zasadniczo zbieżne z celami działalności, o których mowa w art. 1 ust. 3 dyrektywy 2002/58. Artykuł 15 ust. 1 owej dyrektywy stosuje się bowiem 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 środki ustawodawcze, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, regulują, do celów, o których mowa w tym przepisie, działalność dostawców usług łączności elektronicznej (zob. podobnie wyrok Tele2 Sverige i Watson i in., pkt 72–74).

35 Trybunał stwierdził, iż wspomniany art. 15 ust. 1 w związku z art. 3 dyrektywy 2002/58 należy interpretować w ten sposób, że 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 dotyczący dostępu organów krajowych do danych zatrzymywanych przez owych dostawców (zob. podobnie wyrok Tele2 Sverige i Watson i in., pkt 75, 76).

36 Zagwarantowana w art. 5 ust. 1 dyrektywy 2002/58 ochrona poufności łączności elektronicznej i związanych z nimi danych dotyczących ruchu znajduje bowiem zastosowanie do środków stosowanych przez podmioty inne niż użytkownicy, niezależnie od tego, czy są to podmioty prywatne, czy też państwowe. Jak potwierdza motyw 21 tej dyrektywy, ma ona na celu uniemożliwienie każdego

niedozwolonego „dostępu” do komunikatów, włączając w to „dane związane z tego rodzaju komunikatem”, w celu ochrony poufności łączności elektronicznej (wyrok Tele2 Sverige i Watson i in., pkt 77).

37 Należy dodać, że środki ustawodawcze nakładające na dostawców usług łączności elektronicznej obowiązek zatrzymywania danych osobowych lub udzielenia właściwym organom krajowym dostępu do tych danych, wymagają przetwarzania wspomnianych danych przez tych dostawców (zob. podobnie wyrok Tele2 Sverige i Watson i in., pkt 75, 78). Środki takie, w zakresie, w jakim regulują działalność wspomnianych dostawców, nie mogą zatem być traktowane jako działalność właściwa państwom, o której mowa w art. 1 ust. 3 dyrektywy 2002/58.

38 W niniejszym przypadku, jak wynika z postanowienia odsyłającego, podstawą wniosku rozpatrywanego w postępowaniu głównym, w którym policja ubiega się o zezwolenie na uzyskanie dostępu do danych osobowych zatrzymywanych przez dostawców usług łączności elektronicznej, jest ustawa 25/2007 w związku z kodeksem postępowania karnego, w brzmieniu mającym zastosowanie do okoliczności faktycznych w postępowaniu głównym, która reguluje dostęp organów publicznych do takich danych. Uregulowanie to umożliwia policji, w przypadku uzyskania zgody, o którą wnosi się na jego podstawie, wymaganie od dostawców usług łączności elektronicznej, aby jej udostępnili dane osobowe i aby tym samym dokonali, w świetle definicji zawartej w art. 2 lit. b) dyrektywy 95/46 mającej zastosowanie w kontekście dyrektywy 2002/58 na podstawie jej art. 2 akapit pierwszy, „przetwarzania” takich danych w rozumieniu tych dwóch dyrektyw. Wspomniane uregulowanie normuje zatem działalność dostawców usług łączności elektronicznej i w konsekwencji wchodzi w zakres stosowania dyrektywy 2002/58.

39 W tej sytuacji podniesiona przez rząd hiszpański okoliczność, że wniosek o udzielenie dostępu został złożony w ramach postępowania karnego, nie może pozbawić dyrektywy 2002/58 zastosowania w sprawie, której dotyczy postępowanie główne, na mocy art. 1 ust. 3 tej dyrektywy.

40 W tym względzie nie ma również znaczenia to, że wniosek o udzielenie dostępu rozpatrywany w postępowaniu głównym zmierza – jak wynika z pisemnej odpowiedzi rządu hiszpańskiego na pytanie zadane przez Trybunał, i jak zostało to potwierdzone na rozprawie zarówno przez rząd francuski, jak i przez prokuraturę – do umożliwienia dostępu wyłącznie do numerów telefonu odpowiadających kartom SIM działającym z numerem IMEI skradzionego telefonu komórkowego i do danych dotyczących tożsamości cywilnej posiadaczy tych kart, takich jak nazwisko, imię oraz, w stosownych przypadkach, adres, z wykluczeniem danych odnoszących się do komunikatów przekazanych za pośrednictwem wspomnianych kart SIM i danych dotyczących lokalizacji skradzionego telefonu komórkowego.

41 Jak bowiem wskazał rzecznik generalny w pkt 54 opinii, dyrektywa 2002/58 reguluje, zgodnie z jej art. 1 ust. 1 i art. 3, wszelkie przetwarzanie danych osobowych w związku ze świadczeniem usług łączności elektronicznej. Ponadto, zgodnie z art. 2 akapit drugi lit. b) tej dyrektywy pojęcie „danych o ruchu” obejmuje „wszelkie dane przetwarzane do celów przekazywania komunikatu w sieci łączności elektronicznej lub naliczania opłat za te usługi”.

42 W tym ostatnim względzie, co się tyczy w szczególności danych dotyczących tożsamości cywilnej posiadaczy kart SIM, to z motywu 15 dyrektywy 2002/58 wynika, że dane o ruchu mogą, między innymi, obejmować nazwę i adres nadawcy komunikatu lub użytkownika połączenia w celu przeprowadzenia łączności. Dane dotyczące tożsamości cywilnej posiadaczy kart SIM mogą ponadto okazać się konieczne w celu naliczania opłat za świadczone usługi łączności elektronicznej i wobec tego należą do danych o ruchu w rozumieniu art. 2 akapit drugi lit. b) tej dyrektywy. Dane te są objęte zakresem stosowania dyrektywy 2002/58.

43 Wobec powyższego Trybunał jest właściwy w zakresie udzielenia odpowiedzi na pytanie przedstawione przez sąd odsyłający.

W przedmiocie dopuszczalności

44 Rząd hiszpański podnosi, że wniosek o wydanie orzeczenia w trybie prejudycjalnym jest niedopuszczalny, ponieważ nie określa jasno przepisów prawa Unii, co do których zwrócono się do Trybunału o wydanie orzeczenia. Co więcej, według rządu hiszpańskiego rozpatrywany w postępowaniu głównym wniosek policji dotyczy nie przechwytywania komunikatów przekazanych przy użyciu kart SIM działających z numerem IMEI skradzionego telefonu komórkowego, lecz powiązania tych kart z ich posiadaczami, wobec czego poufność łączności nie zostaje naruszona. Artykuł 7 karty, o którym mowa w pytaniach prejudycjalnych, nie ma zatem znaczenia w kontekście niniejszej sprawy.

45 Zgodnie z utrwalonym orzecznictwem Trybunału jedynie do sądu krajowego, przed którym zawisł spór i na którym spoczywa odpowiedzialność za mające zapaść rozstrzygnięcie, należy ustalenie, czy, w celu wydania rozstrzygnięcia i przy uwzględnieniu specyfiki danej sprawy, zachodzi potrzeba uzyskania orzeczenia w trybie prejudycjalnym, jak i zasadności zadawanych Trybunałowi pytań. W konsekwencji, jeśli postawione pytania dotyczą wykładni prawa Unii, Trybunał jest co do zasady zobowiązany do wydania orzeczenia. Odmowa wydania przez Trybunał orzeczenia w trybie prejudycjalnym, o które wnioskował sąd krajowy, jest możliwa tylko wtedy, gdy jest oczywiste, że wykładnia prawa Unii, o którą się zwrócono, nie ma żadnego związku ze stanem faktycznym lub przedmiotem sporu w postępowaniu głównym, gdy problem jest natury hipotetycznej bądź gdy Trybunał nie dysponuje informacjami w zakresie stanu faktycznego lub prawnego niezbędnymi do udzielenia użytecznej odpowiedzi na pytania, które zostały mu postawione (wyrok z dnia 10 lipca 2018 r., Jehovan todistajat, C-25/17, EU:C:2018:551, pkt 31 i przytoczone tam orzecznictwo).

46 W niniejszej sprawie postanowienie odsyłające zawiera elementy stanu faktycznego i prawnego wystarczające zarówno dla określenia przepisów prawa Unii, których dotyczą pytania prejudycjalne, jak i dla zrozumienia zakresu tych pytań. W szczególności z postanowienia odsyłającego wynika, że pytania prejudycjalne zmierzają do umożliwienia sądowi odsyłającemu dokonania oceny, czy i w jakim stopniu uregulowanie krajowe, na którym jest oparty wniosek policji rozpatrywany w postępowaniu głównym, realizuje cel mogący uzasadniać naruszenie praw podstawowych ustanowionych w art. 7 i 8 karty. Tymczasem, zgodnie z wskazaniami sądu odsyłającego owo uregulowanie krajowe wchodzi w zakres stosowania dyrektywy 2002/58, wobec czego karta znajduje zastosowanie do sprawy, której dotyczy postępowanie główne. Pytania prejudycjalne mają zatem bezpośredni związek z przedmiotem postępowania głównego i wobec tego nie mogą być uznane za hipotetyczne.

47 W tych okolicznościach pytania prejudycjalne są dopuszczalne.

Co do istoty

48 Poprzez swoje dwa pytania, które należy rozpatrzyć łącznie, sąd odsyłający zmierza w istocie do ustalenia, czy art. 15 ust. 1 dyrektywy 2002/58 w świetle art. 7 i 8 karty należy interpretować w ten sposób, że dostęp organów publicznych do danych w celu identyfikacji posiadaczy kart SIM działających w skradzionym telefonie komórkowym, takich jak nazwisko, imię oraz, w stosownych przypadkach, adres tych posiadaczy, powoduje ingerencję w ich prawa podstawowe wynikające z owych artykułów karty, która jest na tyle poważna, aby dostęp ten należało ograniczyć – w zakresie zapobiegania, dochodzenia, wykrywania i ścigania przestępstw – do walki z poważną przestępczością, a jeśli tak, to według jakich kryteriów powinna być oceniana waga naruszenia.

49 W tym względzie z postanowienia odsyłającego wynika, że – jak zauważył w istocie rzecznik generalny w pkt 38 opinii – wniosek o wydanie orzeczenia w trybie prejudycjalnym zmierza nie do ustalenia, czy dane osobowe, których dotyczy postępowanie główne, były przechowywane przez dostawców usług łączności elektronicznej zgodnie z warunkami, o których mowa w art. 15 ust. 1 dyrektywy 2002/58 w świetle art. 7 i 8 karty. Wniosek ten dotyczy, jak wynika z pkt 46 niniejszego wyroku, wyłącznie

kwestii, czy i w jakim stopniu cel zamierzony przez uregulowanie, którego dotyczy postępowanie główne, może uzasadniać dostęp organów publicznych, takich jak policja, do takich danych, przy czym inne warunki dostępu wynikające z art. 15 ust. 1 nie są przedmiotem tego wniosku.

50 W szczególności sąd odsyłający zastanawia się, jakie elementy należy uwzględnić przy ocenie, czy naruszenia, w odniesieniu do których organy policyjne mogą uzyskać zgodę, do celów śledztwa, na dostęp do danych osobowych zatrzymywanych przez dostawców usług łączności elektronicznej, są wystarczająco poważne, aby uzasadnić spowodowaną przez taki dostęp ingerencję w prawa podstawowe zagwarantowane w art. 7 i 8 karty, w świetle ich wykładni dokonanej przez Trybunał w wyrokach z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in. (C-293/12 i C-594/12, EU:C:2014:238), oraz Tele2 Sverige i Watson i in.

51 Co się tyczy wystąpienia ingerencji w te prawa podstawowe, to należy przypomnieć, że – jak wskazał rzecznik generalny w pkt 76 i 77 swojej opinii – dostęp organów publicznych do takich danych stanowi ingerencję w podstawowe prawo do poszanowania życia prywatnego, zapewnione w art. 7 karty, nawet w braku okoliczności pozwalających na zakwalifikowanie tej ingerencji jako „poważnej”, i nie ma znaczenia, czy informacje związane z życiem prywatnym osób, których dotyczą, mają charakter wrażliwy czy nie, lub czy zainteresowane osoby poniosły jakiekolwiek negatywne konsekwencje z powodu tej ingerencji. Taki dostęp stanowi również ingerencję w prawo podstawowe do ochrony danych osobowych zagwarantowane w art. 8 karty, ponieważ stanowi przetwarzanie danych osobowych [zob. podobnie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 124, 126 i przytoczone tam orzecznictwo].

52 Jeśli chodzi o cele, które mogą uzasadniać uregulowanie krajowe takie jak rozpatrywane w postępowaniu głównym, normujące dostęp organów publicznych do danych zatrzymywanych przez dostawców usług łączności elektronicznej i tym samym stanowiące odstępstwo od zasady poufności łączności elektronicznej, to należy przypomnieć, że wyliczenie celów dokonane w art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 ma charakter wyczerpujący, wobec czego ów dostęp powinien odpowiadać rzeczywiście i ściśle jednemu z tych celów (zob. podobnie wyrok Tele2 Sverige i Watson i in., pkt 90, 115).

53 Jeśli zaś chodzi o cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu przestępstw kryminalnych, to należy zauważyć, że brzmienie art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 nie ogranicza tego celu do zwalczania poważnych przestępstw, lecz odnosi się ogólnie do „przestępstw kryminalnych”.

54 Prawdą jest, iż w tym względzie Trybunał orzekł, że w zakresie zapobiegania, dochodzenia, wykrywania i ścigania przestępstw kryminalnych jedynie walka z poważną przestępczością może usprawiedliwiać dostęp organów publicznych do danych osobowych zatrzymywanych przez dostawców usług łączności elektronicznej, których całokształt może dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, o których dane chodzi (zob. podobnie wyrok Tele2 Sverige i Watson i in., pkt 99).

55 Trybunał uzasadnił jednak tę wykładnię, powoławszy się na okoliczność, że cel realizowany przez uregulowanie normujące ten dostęp powinien być powiązany z wagą ingerencji w odnośne prawa podstawowe, jaką dostęp taki pociąga za sobą (zob. podobnie wyrok Tele2 Sverige i Watson i in., pkt 115).

56 Zgodnie z zasadą proporcjonalności poważna ingerencja może bowiem być uzasadniona w zakresie zapobiegania, dochodzenia, wykrywania i ścigania przestępstw karnych jedynie przez cel polegający na zwalczaniu przestępczości, którą można uznać za „poważną”.

57 Jeżeli natomiast ingerencja wynikająca z takiego dostępu nie jest poważna, to może być uzasadniona przez cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu ogółu „przestępstw kryminalnych”.

58 Należy zatem przede wszystkim określić, czy w niniejszym przypadku w świetle okoliczności rozpatrywanej sprawy ingerencja w prawa podstawowe ustanowione w art. 7 i 8 karty, jaką powodowałby dostęp policji do danych, których dotyczy postępowanie główne, powinna zostać uznana za „poważną”.

59 W tym względzie rozpatrywany w postępowaniu głównym wniosek, w którym policja żąda, dla potrzeb dochodzenia karnego, zgody organu sądowego na dostęp do danych osobowych zatrzymywanych przez dostawców usług łączności elektronicznej, ma na celu jedynie identyfikację posiadaczy kart SIM działających, w okresie dwunastu dni, z numerem IMEI skradzionego telefonu komórkowego. Jak zostało wskazane w pkt 40 niniejszego wyroku, wniosek ten dotyczy dostępu do numerów telefonu odpowiadających tym kartom SIM, a także do danych dotyczących tożsamości cywilnej posiadaczy owych kart, takich jak nazwisko, imię, oraz, w stosownych przypadkach, adres. Natomiast dane te nie dotyczą, jak potwierdziły na rozprawie zarówno rząd hiszpański, jak i prokuratura, komunikatów przekazanych przy użyciu skradzionego telefonu komórkowego ani jego lokalizacji.

60 Wydaje się zatem, że dane objęte wnioskiem o udzielenie dostępu rozpatrywanym w postępowaniu głównym pozwalają jedynie powiązać, w danym okresie, kartę lub karty SIM działające w skradzionym telefonie komórkowym z tożsamością cywilną posiadaczy owych kart SIM. Bez badania krzyżowego z danymi dotyczącymi komunikatów przekazanych przy użyciu wspomnianych kart SIM i z danymi dotyczącymi lokalizacji, dane te nie umożliwiają poznania ani daty, godziny, czasu trwania i odbiorców komunikatów przekazanych przy użyciu przedmiotowej karty lub przedmiotowych kart SIM, ani miejsc, w których łączność miała miejsce, lub częstotliwość komunikowania się z określonymi osobami w danym okresie. Rzeczone dane te nie pozwalają zatem na wyciągnięcie konkretnych wniosków dotyczących prywatnego życia osób, o których dane chodzi.

61 W tych okolicznościach dostęp wyłącznie do danych objętych wnioskiem rozpatrywanym w postępowaniu głównym nie może zostać uznany za „poważną” ingerencję w prawa podstawowe osób, o których dane chodzi.

62 Jak wynika z pkt 53–57 niniejszego wyroku, ingerencja, którą spowodowałby dostęp do takich danych, może zatem być uzasadniona przez cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu ogółu „przestępstw kryminalnych”, do którego odwołuje się art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58, bez konieczności zakwalifikowania tych przestępstw jako „poważnych”.

63 Mając na uwadze powyższe rozważania, na przedstawione pytania prejudycjalne należy odpowiedzieć, iż art. 15 ust. 1 dyrektywy 2002/58, w związku z art. 7 i 8 karty, należy interpretować w ten sposób, że dostęp organów publicznych do danych w celu identyfikacji posiadaczy kart SIM działających w skradzionym telefonie komórkowym, takich jak nazwisko, imię oraz, w stosownych przypadkach, adres tych posiadaczy, powoduje ingerencję w prawa podstawowe tych posiadaczy, ustanowione w owych artykułach karty, która nie jest na tyle poważna, aby dostęp ten należało ograniczyć – w zakresie zapobiegania, dochodzenia, wykrywania i ścigania przestępstw kryminalnych – do walki z poważną przestępczością.

W przedmiocie kosztów

64 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:

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 i 8 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że dostęp organów publicznych do danych w celu identyfikacji posiadaczy kart SIM działających w skradzionym telefonie komórkowym, takich jak nazwisko, imię oraz, w stosownych przypadkach, adres tych posiadaczy, powoduje ingerencję w prawa podstawowe tych posiadaczy, ustanowione w owych artykułach karty, która nie jest na tyle poważna, aby dostęp ten należało ograniczyć – w zakresie zapobiegania, dochodzenia, wykrywania i ścigania przestępstw kryminalnych – do walki z poważną przestępczością.

Podpisy