Zbiór Orzeczeń

WYROK TRYBUNAŁU (wielka izba)

21 grudnia 2016 r.*

[Sprostowane postanowieniem z dnia 16 marca 2017 r.]

Odesłanie prejudycjalne — Łączność elektroniczna — Przetwarzanie danych osobowych — Poufność łączności elektronicznej — Ochrona — Dyrektywa 2002/58/WE — Artykuły 5, 6 i 9 oraz art. 15 ust. 1 — Karta praw podstawowych Unii Europejskiej — Artykuły 7, 8 i 11 oraz art. 52 ust. 1 — Przepisy krajowe — Dostawcy usług łączności elektronicznej — Obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji — Organy władz krajowych — Dostęp do danych — Brak uprzedniej kontroli sądowej lub niezależnego organu administracyjnego — Zgodność z prawem Unii

W sprawach połączonych C-203/15 i C-698/15,

mających za przedmiot wnioski o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożone przez Kammarrätten i Stockholm (sąd administracyjny Sztokholmu, Szwecja) i Court of Appeal (England & Wales) (Civil Division) (wydział cywilny sądu apelacyjnego dla Anglii i Walii, Zjednoczone Królestwo), postanowieniami, odpowiednio, z dnia 29 kwietnia 2015 r. i z dnia 9 grudnia 2015 r., które wpłynęły do Trybunału w dniu 4 maja 2015 r. i w dniu 28 grudnia 2015 r., w postępowaniach:

Tele2 Sverige AB (C-203/15)

przeciwko

Post- och telestyrelsen,

oraz

Secretary of State for the Home Department (C-698/15)

przeciwko

Tomowi Watsonowi,

Peterowi Brice'owi,

Geoffreyowi Lewisowi,

przy udziale:

Open Rights Group,

* * Język postępowania: szwedzki i angielski.

Privacy International,

The Law Society of England and Wales,

TRYBUNAŁ (wielka izba),

w składzie: K. Lenaerts, prezes, A. Tizzano, wiceprezes, R. Silva de Lapuerta, T. von Danwitz (sprawozdawca), J.L. da Cruz Vilaça, E. Juhász i M. Vilaras, prezesi izb, A. Borg Barthet, J. Malenovský, E. Levits, J.C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen i C. Lycourgos, sędziowie,

rzecznik generalny: H. Saugmandsgaard Øe,

sekretarz: C. Strömholm, administrator,

uwzględniając postanowienie prezesa Trybunału z dnia 1 lutego 2016 r. o rozpoznaniu sprawy C-698/15 w przewidzianym w art. 105 § 1 regulaminu postępowania przed Trybunałem postępowaniu w trybie przyśpieszonym,

uwzględniając procedurę pisemną i po przeprowadzeniu rozprawy w dniu 12 kwietnia 2016 r.,

rozważywszy uwagi przedstawione:

— w imieniu Tele2 Sverige AB przez M. Johanssona i N. Thorgerzona, advokater, oraz przez E. Lagerlöfa i S. Backmana,

— w imieniu T. Watsona przez J. Welcha i E. Norton, solicitors, I. Steele'a, advocate, B. Jaffeya, barrister, oraz D. Rose, QC,

— w imieniu P. Brice'a i G. Lewisa przez A. Suterwalla i R. de Mella, barristers, R. Drabble'a, QC, oraz S. Luke'a, solicitor,

— w imieniu Open Rights Group i Privacy International przez D. Careya, solicitor, oraz przez R. Mehtę i J. Simor, barristers,

— w imieniu The Law Society of England and Wales przez T. Hickmana, barrister, oraz przez N. Turner,

— w imieniu rządu szwedzkiego przez A. Falk, C. Meyer-Seitz, U. Persson, N. Otte Widgren oraz L. Swedenborga, działających w charakterze pełnomocników,

— w imieniu rządu Zjednoczonego Królestwa przez S. Brandona, L. Christiego oraz V. Kaye, działających w charakterze pełnomocników, wspieranych przez D. Bearda, G. Facennę, J. Eadiego, QC, oraz przez S. Ford, barrister,

— w imieniu rządu belgijskiego przez J.C. Halleux, S. Vanrie oraz C. Pochet, działających w charakterze pełnomocników,

— w imieniu rządu czeskiego przez M. Smolka oraz J. Vláčila, działających w charakterze pełnomocników,

— w imieniu rządu duńskiego przez C. Thorninga i M. Wolff, działających w charakterze pełnomocników,

— w imieniu rządu niemieckiego, przez T. Henzego, M. Hellmanna oraz J. Kemper, działających w charakterze pełnomocników, wspieranych przez M. Kottmanna oraz U. Karpensteina, Rechtsanwälte,

— w imieniu rządu estońskiego przez K. Kraavi-Käerdi, działającą w charakterze pełnomocnika,

— w imieniu Irlandii przez E. Creedon, L. Williams oraz A. Joyce'a, działających w charakterze pełnomocników, wspieranych przez D. Fennelly'ego, BL,

— w imieniu rządu hiszpańskiego przez A. Rubia Gonzáleza, działającego w charakterze pełnomocnika,

— w imieniu rządu francuskiego przez G. de Bergues'a, D. Colasa, F.X. Bréchota oraz C. David, działających w charakterze pełnomocników,

— w imieniu rządu cypryjskiego,przez K. Kleanthous, działającą w charakterze pełnomocnika,

— w imieniu rządu węgierskiego przez M. Fehéra oraz G. Koósa, działających w charakterze pełnomocników,

— w imieniu rządu niderlandzkiego przez M. Bulterman, M. Gijzen oraz J. Langera, działających w charakterze pełnomocników,

— w imieniu rządu polskiego przez B. Majczynę, działającego w charakterze pełnomocnika,

— w imieniu rządu fińskiego przez J. Heliskoskiego, działającego w charakterze pełnomocnika,

— w imieniu Komisji Europejskiej przez H. Krämera, K. Simonssona, H. Kranenborga, D. Nardiego, P. Costę de Oliveirę oraz J. Vondung, działających w charakterze pełnomocników,

po zapoznaniu się z opinią rzecznika generalnego na posiedzeniu w dniu 19 lipca 2016 r.,

wydaje następujący

Wyrok

1 Wnioski o wydanie orzeczenia w trybie prejudycjalnym dotyczą wykładni art. 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. 2002, L 201, s. 37), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. (Dz.U. 2009, L 337, s. 11) (zwanej dalej „dyrektywą 2002/58") w związku z art. 7, 8 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą").

2 Wnioski te zostały przedstawione w ramach dwóch sporów, jakie zaistniały, po pierwsze, pomiędzy Tele2 Sverige AB a Post- och telestyrelsen (szwedzkim organem nadzoru usług pocztowych i telekomunikacji, zwanym dalej „PTS") w przedmiocie skierowanego przez tego ostatniego do Tele2 Sverige żądania zatrzymywania danych o ruchu i danych o lokalizacji jego abonentów i zarejestrowanych użytkowników (sprawa C-203/15), a po drugie, pomiędzy Tomem Watsonem, Peterem Brice'em i Geoffreyem Lewisem a Secretary of State for the Home Department (ministrem spraw wewnętrznych, Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej) w przedmiocie

zgodności z prawem Unii art. 1 Data Retention and Investigatory Powers Act 2014 (ustawy z 2014 r. o zatrzymywaniu danych i uprawnieniach dochodzeniowych, zwanej dalej „DRIPA”) (sprawa C-698/15).

Ramy prawne

Prawo Unii Europejskiej

Dyrektywa 2002/58

3 Motywy 2, 6, 7, 11, 21, 22, 26 i 30 dyrektywy 2002/58 stanowią:

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

[…]

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

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

[…]

(11) Niniejsza dyrektywa, podobnie jak dyrektywa 95/46/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)], nie odnosi się do kwestii ochrony podstawowych praw i wolności związanych z działalnością, która nie jest regulowana prawem wspólnotowym. Dyrektywa nie zmienia zatem istniejącej równowagi między prawem do prywatności osoby fizycznej a [przysługującą państwom członkowskim] możliwością podejmowania środków, określonych w art. 15 ust. 1 niniejszej dyrektywy, niezbędnych do ochrony bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając gospodarczy dobrobyt państwa, gdy działania dotyczą zagadnień bezpieczeństwa państwa) i wykonywania prawa karnego. Wskutek tego, niniejsza dyrektywa nie wpływa na [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 ramach społeczeństwa demokratycznego oraz powinny podlegać stosownym zabezpieczeniom zgodnie z europejską Konwencją o ochronie praw człowieka i podstawowych wolności.

[…]

(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 rodzaj 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.

(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 […].

[…]

(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 […].

[…]

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

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

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

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

3. Niniejsza dyrektywa nie ma zastosowania do działalności, która wykracza poza zakres Traktatu 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”.

5 Zgodnie z art. 2 dyrektywy 2002/58, 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. L 108, s. 33].

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;

[…]”.

6 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”.

7 Artykuł 4 tej dyrektywy, zatytułowany „Bezpieczeństwo”, ma następujące brzmienie:

„1. Dostawca publicznie dostępnych usług łączności elektronicznej musi podjąć właściwe środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa oferowanych przez siebie usług, jeśli to konieczne wraz z dostawcą publicznej sieci komunikacyjnej, w odniesieniu do bezpieczeństwa sieci. Uwzględniając najnowocześniejsze osiągnięcia techniczne oraz koszty ich wprowadzenia, środki te zapewniają poziom bezpieczeństwa odpowiedni do stopnia ryzyka.

1a. Bez uszczerbku dla dyrektywy 95/46/WE środki, o których mowa w ust. 1, muszą co najmniej:

— zapewniać, aby do danych osobowych mógł mieć dostęp wyłącznie uprawniony personel w dozwolonych prawem celach,

— chronić przechowywane lub przekazywane dane osobowe przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą lub zmianą oraz nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, oraz

— zapewnić wdrożenie polityki bezpieczeństwa w odniesieniu do przetwarzania danych osobowych.

[…]”.

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 [lub w którym można dochodzić jego zapłaty].

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 możliwość odwołania swojej zgody na przetwarzanie danych o ruchu w każdej chwili.

[…]

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”, przewiduje w ust. 1:

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

11 Artykuł 15 tej dyrektywy, zatytułowany „Stosowanie niektórych przepisów dyrektywy [95/46]”, stanowi:

„1. Państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4 i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (tj. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy [95/46]. W tym celu państwa członkowskie mogą między innymi uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej.

[…]

1b. Dostawcy ustanawiają wewnętrzne procedury odpowiedzi na wnioski o dostęp do danych osobowych użytkownika w oparciu o krajowe przepisy przyjęte zgodnie z art. 1. Na żądanie przedstawiają oni właściwemu organowi krajowemu informacje o tych procedurach, liczbie otrzymanych wniosków, ich uzasadnieniu prawnym oraz udzielonej przez nich odpowiedzi.

2. Przepisy rozdziału III, dotyczącego środków zaskarżenia, odpowiedzialności i sankcji dyrektywy 95/46/WE, stosuje się w odniesieniu do przepisów krajowych przyjętych zgodnie z niniejszą dyrektywą i w odniesieniu do indywidualnych uprawnień wynikających z niniejszej dyrektywy.

[…]”.

Dyrektywa 95/46

12 Artykuł 22 dyrektywy 95/46, znajdujący się w jej rozdziale III, brzmi jak następuje:

„Bez uszczerbku dla wszystkich odwoławczych środków administracyjnych, które mogą być wprowadzone przez organ nadzorczy określony w art. 28, przed wszczęciem postępowania sądowego państwa członkowskie zapewnią każdej osobie prawo do korzystania ze środków prawnych w związku z naruszeniem praw zagwarantowanych jej przez przepisy krajowe dotyczące przetwarzania danych”.

Dyrektywa 2006/24/WE

13 Artykuł 1 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), zatytułowany „Przedmiot i zakres stosowania", stanowi w ust. 2:

„Niniejsza dyrektywa stosuje się 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. Nie odnosi się ona natomiast do treści komunikatów elektronicznych, w tym informacji uzyskiwanych przy użyciu sieci łączności elektronicznej".

14 Zgodnie z art. 3 tej dyrektywy, zatytułowanym „Obowiązek zatrzymywania danych":

„1. Na zasadzie odstępstwa od art. 5, 6 i 9 dyrektywy [2002/58] państwa członkowskie przyjmują środki w celu zagwarantowania, że [by] dane określone w art. 5 niniejszej dyrektywy są [były] zatrzymywane zgodnie z jej przepisami w stopniu, w jakim są generowane lub przetwarzane na ich terenie przez dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznej sieci łączności w trakcie świadczenia odnośnych usług łączności.

2. Obowiązek zatrzymywania danych, określony w ust. 1, obejmuje również zatrzymanie danych określonych w art. 5 w przypadku nieudanych prób połączenia, podczas których dane te są generowane, przetwarzane i przechowywane (w przypadku danych telefonicznych) lub zapisywane w momencie logowania (w przypadku danych internetowych) przez dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznej sieci łączności w trakcie świadczenia przedmiotowych usług łączności. Niniejsza dyrektywa nie wymaga zatrzymania danych w przypadku nieuzyskania połączenia telefonicznego".

Prawo szwedzkie

15 Jak wynika z postanowienia odsyłającego w sprawie C-203/15, ustawodawca szwedzki w celu transpozycji dyrektywy 2006/24 do prawa krajowego zmienił lagen (2003:389) om elektronisk kommunikation [ustawę (2003:389) o łączności elektronicznej] (zwaną dalej „LEK") i förordningen (2003:396) om elektronisk kommunikation [rozporządzenie (2003:396) o łączności elektronicznej]. Oba te akty, w brzmieniu mającym zastosowanie do sporu zawisłego w postępowaniu głównym, zawierają przepisy dotyczące zatrzymywania danych dotyczących łączności elektronicznej przez właściwe organy krajowe i ich dostępu do tych danych.

16 Dostęp do danych reguluje ponadto lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet [ustawa (2012:278) o przekazywaniu danych dotyczących łączności elektronicznej w ramach działań dochodzeniowo-śledczych prowadzonych przez organy ścigania, zwana dalej „ustawą nr 2012:278"], a także rättegångsbalken (kodeks postępowania sądowego, zwany dalej „RB").

W przedmiocie obowiązku zatrzymywania danych dotyczących łączności elektronicznej

17 Zgodnie z informacjami przedstawionymi przez sąd odsyłający w sprawie C-203/15 przepisy § 16a rozdziału 6 LEK w związku z § 1 rozdziału 2 owej ustawy nakładają na dostawców usług łączności elektronicznej obowiązek zatrzymywania danych, których zatrzymywanie jest przewidziane przez dyrektywę 2006/24. Chodzi tu o dane na temat abonamentu, jak i inne dane dotyczące konkretnego połączenia telekomunikacyjnego, które są niezbędne do śledzenia i identyfikacji źródła łączności, docelowego miejsca łączności, daty, godziny i czasu trwania połączenia, jego rodzaju, tak aby móc

zidentyfikować wykorzystane do komunikacji urządzenie telekomunikacyjne i zlokalizować urządzenie komunikacji mobilnej w momencie rozpoczęcia i zakończenia połączenia. Obowiązek zatrzymywania danych obejmuje dane generowane lub przetwarzane przez usługi telefonii stacjonarnej i komórkowej, przesyłania wiadomości, dostępu do Internetu oraz zapewniania możliwości dostępu do Internetu (sposób połączenia). Obowiązek ten obejmuje również dane dotyczące nieudanych prób połączeń. Nie odnosi się on natomiast do ich treści.

18 Paragrafy 38–43 rozporządzenia (2003:396) o łączności elektronicznej określają bardziej szczegółowo, jakie dane muszą być zatrzymywane. W odniesieniu do usług telefonii stacjonarnej dane, które mają być zatrzymywane, muszą zawierać numer wywołujący i numer wywołany, wraz z datą i możliwym do odtworzenia czasem, kiedy połączenie rozpoczęło się i zakończyło. Wobec usług telefonii komórkowej obowiązują dodatkowe wymogi zatrzymywania danych; i tak na przykład muszą być zatrzymywane również dane dotyczące lokalizacji na początku i na końcu połączenia. Co się tyczy usług telefonii zawierających pakiety IP, dane, które mają być zachowywane muszą zawierać, oprócz wyżej wymienionych, adresy IP osoby wywołującej i wywołanej. Dane, które mają być zachowywane w odniesieniu do usług przesyłania wiadomości, obejmują numer, adres IP lub inny adres wiadomości nadawcy i odbiorcy. W zakresie dostępu do Internetu, należy zachować adres IP użytkownika oraz datę i identyfikowalny czas zalogowania do usługi zapewniającej dostęp do Internetu i wylogowania z niej.

W przedmiocie okresu przechowywania zatrzymanych danych

19 Zgodnie z § 16d rozdziału 6 LEK dane, o których mowa w § 16a tego rozdziału, muszą być przechowywane przez dostawców usług łączności elektronicznej przez okres sześciu miesięcy, licząc od dnia zakończenia połączenia. Dane te muszą być następnie natychmiast usunięte, chyba że § 16d akapit drugi tego rozdziału LEK stanowi inaczej.

W przedmiocie dostępu do zatrzymywanych danych

20 Udzielanie dostępu do zatrzymywanych danych organom krajowym odbywa się zgodnie z przepisami ustawy 2012:278, przepisami LEK oraz RB.

– Ustawa 2012:278

21 W ramach swoich działań operacyjnych policja krajowa, Säkerhetspolisen (policja bezpieczeństwa, Szwecja) i Tullverket (urząd celny, Szwecja) mogą na podstawie § 1 ustawy 2012:278, na warunkach określonych w tej ustawie, w trakcie swoich dochodzeń bez wiedzy dostawcy sieci łączności elektronicznej lub usług łączności elektronicznej, zgodnie z LEK, zbierać dane dotyczące wiadomości, które zostały przekazane w sieci łączności elektronicznej, urządzeń służących do komunikacji elektronicznej, które były obecne w określonym obszarze geograficznym, a także obszaru geograficznego, w którym pewne urządzenia służące do komunikacji elektronicznej są lub były obecne.

22 Zgodnie z §§ 2 i 3 ustawy 2012:278 dane te mogą być co do zasady gromadzone, jeżeli okoliczności sprawy wskazują na to, że środek ten ma szczególne znaczenie dla zapobiegania lub wykrywania działalności przestępczej, która obejmuje przestępstwa zagrożone karą co najmniej dwóch lat pozbawienia wolności lub przestępstwa wymienione w § 3 tej ustawy, obejmującym przestępstwa zagrożone karą co najmniej do dwóch lat pozbawienia wolności. W tym przypadku zasadność zastosowania środka musi przeważać nad naruszeniami pewnych dóbr lub innymi szkodami spowodowanymi jego zastosowaniem wobec osób nim objętych lub jakimkolwiek stojącym z tym w sprzeczności interesem. Zgodnie z § 5 tej ustawy czas stosowania środka nie może przekraczać jednego miesiąca.

23 Decyzja o gromadzeniu danych jest podejmowana przez dyrektora właściwego organu lub pracownika, któremu dyrektor właściwego organu deleguje uprawnienia decyzyjne. Nie podlega ona uprzedniej kontroli przez organ sądowy ani niezależny organ administracyjny.

24 Zgodnie z § 6 ustawy 2012:278, Säkerhets- och integritetsskyddsnämnden (komisja ds. bezpieczeństwa i ochrony integralności, Szwecja) musi być informowana o każdej decyzji w sprawie zezwolenia na gromadzenie danych. Zgodnie z § 1 lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet [ustawy (2007:980) o nadzorze nad niektórymi działaniami związanymi ze zwalczaniem przestępczości] organ ten powinien sprawować nadzór nad stosowaniem prawa przez organy ścigania.

– LEK

25 Zgodnie z § 22 akapit pierwszy pkt 2 rozdziału 6 LEK dostawca usług łączności elektronicznej powinien na żądanie przekazać dane dotyczące abonamentu prokuraturze, policji krajowej, policji bezpieczeństwa lub innemu dowolnemu organowi odpowiedzialnemu za zwalczanie przestępczości, jeżeli dane te odnoszą się do domniemanego naruszenia prawa. Zgodnie z informacjami przedstawionymi przez sąd odsyłający w sprawie C-203/15 nie ma wymogu, że musi chodzić o poważne przestępstwo.

– RB

26 RB reguluje przekazywanie zatrzymywanych danych organom krajowym w ramach przygotowawczego etapu postępowania karnego. Zgodnie z § 19 rozdziału 27 RB „niejawne obserwowanie łączności elektronicznej" może co do zasady być przeprowadzone w ramach postępowania przygotowawczego, w szczególności w sprawie przestępstw zagrożonych karą co najmniej sześciu miesięcy pozbawienia wolności. Przez „niejawne obserwowanie łączności elektronicznej" należy zgodnie z § 19 rozdziału 27 RB rozumieć uzyskanie bez wiedzy osoby trzeciej danych dotyczących wiadomości, które zostały przekazane w sieci łączności elektronicznej, urządzeń służących do komunikacji elektronicznej, które są lub były obecne w określonym obszarze geograficznym, a także obszaru geograficznego, w którym pewne urządzenia komunikacji są lub były obecne.

27 Zgodnie z informacjami przedstawionymi przez sąd odsyłający w sprawie C-203/15 dane dotyczące treści wiadomości nie mogą być gromadzone w oparciu o § 19 rozdziału 27 RB. Niejawne obserwowanie łączności elektronicznej może, zgodnie z § 20 rozdziału 27 RB, być co do zasady przeprowadzone tylko wtedy, gdy istnieją uzasadnione podstawy, by podejrzewać, że ktoś popełnił przestępstwo, a środek ten ma szczególne znaczenie dla dochodzenia, przy czym powinno ono ponadto dotyczyć przestępstwa zagrożonego karą co najmniej dwóch lat pozbawienia wolności lub jego usiłowania lub przygotowania bądź też zmowy mającej na celu popełnienie takiego naruszenia. Zgodnie z § 21 rozdziału 27 RB prokurator, z wyjątkiem przypadków o pilnym charakterze, musi zwrócić się do właściwego sądu o zezwolenie na niejawne obserwowanie łączności elektronicznej.

W przedmiocie bezpieczeństwa i ochrony zatrzymanych danych

28 Paragraf 3a rozdziału 6 LEK stanowi, że dostawcy usług łączności elektronicznej podlegający obowiązkowi zatrzymywania danych muszą zastosować szczególne środki techniczne i organizacyjne niezbędne do zapewnienia ochrony danych zatrzymywanych w trakcie przetwarzania. Zgodnie z informacjami przedstawionymi przez sąd odsyłający w sprawie C-203/15 prawo szwedzkie nie normuje jednak zagadnienia miejsca przechowywania danych.

Prawo Zjednoczonego Królestwa

DRIPA

29 Artykuł 1 DRIPA, zatytułowany „Uprawnienia do zatrzymywania danych dotyczących określonych połączeń oraz mechanizmy ochronne”, stanowi:

„(1) [Minister spraw wewnętrznych] może w drodze decyzji (zwanej dalej „decyzją zobowiązującą do zatrzymywania danych”) zobowiązać publicznego operatora telekomunikacyjnego do zatrzymywania odpowiednich danych dotyczących połączeń, jeżeli uzna, że jest to konieczne i proporcjonalne w świetle jednego lub większej liczby celów określonych w sekcji 22 ust. 2 lit. a)–h) Regulation of Investigatory Powers Act 2000 (ustawy z 2000 r. o uprawnieniach dochodzeniowych) (cele uzasadniające dostęp do danych dotyczących łączności).

(2) Decyzja zobowiązująca do zatrzymywania danych może:

(a) dotyczyć konkretnego operatora albo określonego rodzaju operatorów;

(b) zobowiązywać do zatrzymywania wszystkich danych albo określonego rodzaju danych;

(c) określać okres lub okresy, dla których dane mają być zatrzymywane:

(d) zawierać inne wymogi lub ograniczenia dotyczące zatrzymywania danych;

(e) zawierać różne postanowienia dla poszczególnych celów;

(f) dotyczyć danych istniejących w chwili wydania decyzji lub jej wejścia w życie lub danych przyszłych.

(3) [Minister spraw wewnętrznych] może w drodze rozporządzenia ustanowić szczegółowe zasady dotyczące zatrzymywania odpowiednich danych dotyczących łączności.

(4) Zasady takie mogą w szczególności obejmować przepisy określające:

(a) wymogi, które muszą być spełnione przed wydaniem decyzji zobowiązującej do zatrzymywania danych;

(b) maksymalny okres przechowywania danych zatrzymanych na podstawie decyzji zobowiązującej do zatrzymywania danych;

(c) treść, sposób wydania, wejście w życie, tryb kontroli, zmiany lub cofnięcia decyzji zobowiązującej do zatrzymywania danych;

(d) wymogi w zakresie integralności, bezpieczeństwa i ochrony danych zatrzymanych na mocy niniejszego artykułu, dostępu do nich oraz ich ujawnienia lub niszczenia;

(e) tryb egzekwowania lub kontroli zgodności z określonymi wymogami i ograniczeniami;

(f) kodeks zatrzymywania danych regulujący określone wymogi i ograniczenia lub określone uprawnienia;

(g) sposób zwrotu przez [ministra spraw wewnętrznych] (z zastrzeżeniem warunków lub bez ich zastrzegania) kosztów poniesionych przez publicznych operatorów telekomunikacyjnych w celu wypełnienia wymogów lub przestrzegania ograniczeń;

(h) uchylenie [Data Retention (EC Directive) Regulations 2009 (rozporządzenia z 2009 r. w sprawie ochrony danych w rozumieniu dyrektywy WE] i objęcie zatrzymywania danych unormowaniami określonymi przez niniejszy artykuł.

(5) Maksymalny okres ustanowiony na podstawie ust. 4 lit. b) nie może przekraczać 12 miesięcy od dnia określonego w stosunku do danych objętych przepisami ustępu 3.

[…]".

30 Artykuł 2 DRIPA definiuje „odpowiednie dane dotyczące połączeń" jako „dane dotyczące połączeń, takie jak wymienione w załączniku do rozporządzenia z 2009 r. w sprawie ochrony danych w rozumieniu dyrektywy WE, w zakresie, w jakim dane takie są wytwarzane lub przetwarzane w Zjednoczonym Królestwie przez publicznych operatorów telekomunikacyjnych w ramach świadczenia odnośnych usług telekomunikacyjnych".

RIPA

31 Artykuł 21 ustawy z 2000 r. o uprawnieniach dochodzeniowych (zwanej dalej „RIPA"), znajdujący się w rozdziale II tej ustawy, zatytułowany „Pozyskiwanie i ujawnianie danych dotyczących łączności elektronicznej", stanowi w ust. 4:

„Do celów niniejszego rozdziału »dane komunikacyjne« oznaczają:

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

(b) wszelkie informacje, które nie obejmują treści połączenia (z wyłączeniem informacji, o których mowa w lit. a), dotyczące korzystania przez dowolną osobę:
(i) z usługi pocztowej lub usługi telekomunikacyjnej,
(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 lit. a) lub 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".

32 Zgodnie z informacjami zawartymi w postanowieniu odsyłającym w sprawie C-698/15 informacje te obejmują „dane o lokalizacji użytkownika", lecz nie obejmują informacji dotyczących treści komunikatu.

33 W odniesieniu do dostępu do zatrzymanych danych art. 22 RIPA stanowi:

„(1) Artykuł ten stosuje się również w przypadku, gdy osoba odpowiedzialna w rozumieniu niniejszego rozdziału stwierdza, że z przyczyn związanych z ust. 2 niniejszego artykułu konieczne jest uzyskanie danych dotyczących łączności.

(2) Uzyskanie danych dotyczących łączności jest konieczne z przyczyn związanych z niniejszym ustępem, jeśli są one niezbędne:

(a) ze względu na interes związany z bezpieczeństwem narodowym,

(b) w celu zapobiegania lub wykrywania przestępstw lub zapobiegania naruszeniom porządku publicznego,

(c) w interesie gospodarczym Zjednoczonego Królestwa,

(d) w interesie bezpieczeństwa publicznego,

(e) w celu ochrony zdrowia publicznego,

(f) w celu określania wymiaru lub poboru podatków, danin, opłat lub innych zobowiązań, składek lub obciążeń należnych jednostce administracji państwowej,

(g) w nagłych przypadkach w celu zapobieżenia śmierci, obrażeniom lub szkodzie na zdrowiu fizycznym lub psychicznym człowieka albo zmniejszeniu rozmiaru szkody na zdrowiu fizycznym lub psychicznym człowieka,

(h) w innych celach (nieobjętych lit. a–g) określonych w zarządzeniu wydanym przez [ministra spraw wewnętrznych].

(4) Z zastrzeżeniem ust. 5 osoba odpowiedzialna może, jeśli uzna, że operator telekomunikacyjny lub operator pocztowy jest w posiadaniu, może być w posiadaniu lub może być w stanie posiadać dane, wystąpić do niego z żądaniem, aby ów operator:

(a) uzyskał dane, jeżeli ich jeszcze nie posiada, oraz

(b) w każdym wypadku – ujawnił wszystkie dane znajdujące się w jego posiadaniu lub uzyskane później.

(5) Osoba odpowiedzialna może udzielić zgody na mocy ust. 3 lub wystąpić z żądaniem na podstawie ust. 4, o ile stwierdzi, że pozyskiwanie odpowiednich danych wynikające z działań na podstawie zezwolenia lub wymaganych na podstawie zezwolenia lub żądania jest proporcjonalne do zamierzonego celu pozyskiwania danych".

34 Zgodnie z art. 65 RIPA jeśli istnieje powód, aby sądzić, że dane zostały uzyskane w sposób niewłaściwy, skargi można składać do Investigatory Powers Tribunal (sądu ds. uprawnień dochodzeniowych, Zjednoczone Królestwo).

Data Retention Regulations 2014

35 Data Retention Regulations 2014 (rozporządzenie z 2014 r. o zatrzymywaniu danych), przyjęte na podstawie DRIPA, jest podzielone na trzy części, przy czym druga z nich obejmuje art. 2–14. Artykuł 4, zatytułowany „Żądania dotyczące zatrzymywania danych", stanowi:

„(1) W żądaniu dotyczącym zatrzymywania danych podaje się następujące informacje dotyczące:

(a) publicznego operatora telekomunikacyjnego, do którego żądanie jest skierowane (lub opis takich operatorów),

(b) danych dotyczących określonej łączności, które mają być zatrzymywane,

(c) okresu lub okresów, podczas których dane mają być zatrzymywane,

(d) wszelkie inne wymogi lub ograniczenia związane z zatrzymywaniem danych.

(2) Żądanie dotyczące zatrzymywania danych nie może dotyczyć wymogu zatrzymywania danych przez okres dłuższy niż 12 miesięcy począwszy od:

(a) w przypadku danych o ruchu lub danych odnoszących się do korzystania z usług – dnia nawiązania łączności w danym przypadku oraz

(b) w przypadku danych odnoszących się do abonentów – dnia, w którym osoba zakończyła korzystanie z usługi łączności, albo dnia, w którym dana została zmieniona (jeżeli nastąpił on wcześniej).

[…]”.

36 Zgodnie z art. 7 tego rozporządzenia, zatytułowanym „Integralność i bezpieczeństwo danych”:

„(1) Publiczny operator telekomunikacyjny, który zatrzymuje dane na podstawie art. 1 [DRIPA], ma obowiązek:

(a) zapewnić, by dane miały taką samą integralność i podlegały co najmniej takiemu samemu poziomowi bezpieczeństwa i ochrony jak dane w systemach, z których pochodzą,

(b) zapewnić, poprzez środki techniczne i organizacyjne, by do danych mógł mieć dostęp tylko personel upoważniony w tym zakresie, oraz

(c) chronić dane, poprzez odpowiednie środki techniczne i organizacyjne, przed bezprawnym zniszczeniem, utratą lub uszkodzeniem o charakterze przypadkowym oraz przed bezprawnym lub niezgodnym z prawem przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem.

(2) Publiczny operator telekomunikacyjny, który zatrzymuje dane dotyczące łączności w rozumieniu art. 1 [DRIPA], ma obowiązek zniszczyć dane, w sytuacji gdy zatrzymywanie danych przestanie być dopuszczalne na mocy tego artykułu, a nie będzie dozwolone przez prawo na innej podstawie.

(3) Wymóg zniszczenia danych, o którym mowa w ust. 2, polega na obowiązku usunięcia danych w taki sposób, aby uniemożliwić dostęp do nich.

(4) W tym względzie wystarczy, aby operator zastosował środki w celu usuwania danych w interwałach miesięcznych lub krótszych, zależnie od możliwości operatora w praktyce”.

37 Artykuł 8 rozporządzenia, zatytułowany „Ujawnianie zatrzymywanych danych”, stanowi:

„(1) Publiczny operator telekomunikacyjny ma obowiązek wdrożyć odpowiednie systemy bezpieczeństwa (środki techniczne i organizacyjne) do zarządzania dostępem do danych dotyczących łączności zatrzymywanych na mocy art. 1 [DRIPA] w celu uniknięcia przypadków ujawnień, które nie są objęte art. 1 ust. 6 lit. a) [DRIPA].

(2) Publiczny operator telekomunikacyjny, który zatrzymuje dane na podstawie art. 1 [DRIPA], ma obowiązek zatrzymywania danych w taki sposób, aby móc je niezwłocznie przekazać w odpowiedzi na żądania”.

38 Artykuł 9 tego rozporządzenia, zatytułowany „Kontrola sprawowana przez głównego inspektora ochrony danych”, stanowi:

„Główny inspektor ochrony danych kontroluje przestrzeganie wymogów i ograniczeń, o których mowa w tej części, dotyczących integralności, bezpieczeństwa i niszczenia danych zatrzymanych na podstawie art. 1 [DRIPA]”.

Kodeks pozyskiwania danych

39 Acquisition and Disclosure of Communications Data Code of Practice (kodeks dobrych praktyk w zakresie pozyskiwania i ujawniania danych dotyczących łączności, zwany dalej „kodeksem pozyskiwania danych”) zawiera w pkt 2.5–2.9 i 2.36–2.45 wskazówki na temat konieczności i proporcjonalności pozyskiwania danych dotyczących łączności. Według wyjaśnień sądu odsyłającego w sprawie C-698/15 zgodnie z pkt 3.72–3.77 tego kodeksu szczególną uwagę na tę konieczność i proporcjonalność należy zwrócić w przypadku, gdy dane dotyczące łączności odnoszą się do osoby wykonującej zawód wymagający obrotu informacjami chronionymi tajemnicą zawodową lub w inny sposób.

40 Zgodnie z pkt 3.78–3.84) rzeczonego kodeksu w szczególnym przypadku wniosku o dane dotyczące łączności składanego w celu ustalenia źródła informacji dziennikarza wymagane jest postanowienie sądowe. Zgodnie z pkt 3.85–3.87 tego kodeksu istnieje też wymóg zatwierdzenia przez sąd uzyskania dostępu do danych przez jednostkę samorządu terytorialnego. Nie ma natomiast wymogu uzyskania zezwolenia sądowego lub wydanego przez niezależny organ na uzyskanie dostępu do danych dotyczących łączności podlegających tajemnicy zawodowej prawników ani odnoszących się do lekarzy, członków Parlamentu i osób duchownych.

41 Punkt 7.1 kodeksu pozyskiwania danych stanowi, że z danymi dotyczącymi połączeń pozyskanymi lub otrzymanymi zgodnie z przepisami RIPA oraz z ich kopiami, fragmentami i podsumowaniami należy się obchodzić w sposób zapewniający ich bezpieczeństwo; muszą być one również przechowywane w bezpieczny sposób. Ponadto powinny być przestrzegane wymogi zawarte w Data Protection Act (ustawie o ochronie danych).

42 Zgodnie z pkt 7.18 tego kodeksu w sytuacji, gdy organ władzy publicznej Zjednoczonego Królestwa przewiduje możliwość przekazania danych dotyczących łączności organom zagranicznym, powinien on w szczególności zbadać, czy dane te będą chronione w odpowiedni sposób. Niemniej jednak, jak wynika z pkt 7.22 kodeksu, transfer danych do państw trzecich może mieć miejsce jedynie wtedy, gdy transfer ten jest konieczny z uwagi na ważny interes publiczny, nawet jeśli państwo trzecie nie zapewnia odpowiedniego stopnia ochrony. Zgodnie z informacjami przedstawionymi w tym względzie przez sąd odsyłający w sprawie C-698/15 minister spraw wewnętrznych może wydać poświadczenie bezpieczeństwa narodowego, ustanawiające w odniesieniu do określonych danych zwolnienie z wymogów przewidzianych przez ustawodawstwo.

43 Artykuł 8.1 wspomnianego kodeksu przypomina, że w RIPA ustanowiono urząd Interception of Communications Commissioner (głównego inspektora ds. przechwytywania komunikatów, Zjednoczone Królestwo), którego rola polega przede wszystkim na nadzorowaniu w sposób niezależny wykonywania i realizacji uprawnień i obowiązków zawartych w rozdziale II części I RIPA. Jak wynika z pkt 8.3 kodeksu, w przypadku podejrzenia bezprawnego wykorzystania uprawnień inspektor ów jest uprawniony do poinformowania o tym odnośnej osoby, o ile może „wykazać, że dana osoba została poszkodowana wskutek uchybienia umyślnego lub wynikającego z zaniedbania”.

Postępowania główne i pytania prejudycjalne

Sprawa C-203/15

44 W dniu 9 kwietnia 2014 r. Tele2 Sverige, dostawca usług łączności elektronicznej z siedzibą w Szwecji, powiadomiło PTS, że w następstwie stwierdzenia nieważności dyrektywy 2006/24 wyrokiem z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in. (C-293/12 i C-594/12, zwanym dalej „wyrokiem Digital Rights", EU:C:2014:238), zakończy z dniem 14 kwietnia 2014 r. zatrzymywanie danych dotyczących łączności elektronicznej, o których mowa w LEK, i przystąpi do usuwania przechowywanych do tego dnia danych.

45 W dniu 15 kwietnia 2014 r. Rikspolisstyrelsen (komenda główna policji krajowej, Szwecja) zwróciła się do PTS ze skargą na to, że Tele2 Sverige przestało przekazywać jej te dane.

46 W dniu 29 kwietnia 2014 r. justitieminister (minister sprawiedliwości, Szwecja) powołał specjalnego pełnomocnika do zbadania odnośnych przepisów szwedzkich w związku z wyrokiem Digital Rights. W sprawozdaniu z dnia 13 czerwca 2014 r., zatytułowanym „Datalagring, EU-rätt och svensk rätt, nº Ds 2014:23" (Zatrzymywanie danych, prawo Unii i prawo szwedzkie, zwanym dalej „sprawozdaniem z 2014 r."), specjalny pełnomocnik uznał, że przepisy krajowe dotyczące zatrzymywania danych, takie jak te przewidziane w §§ 16 a–f LEK, nie były sprzeczne ani z prawem Unii Europejskiej, ani z europejską Konwencją o ochronie praw człowieka i podstawowych wolności, podpisaną w Rzymie w dniu 4 listopada 1950 r. (zwaną dalej „EKPC"). Podkreślił on, że wyrok Digital Rights nie może być interpretowany w ten sposób, że Trybunał zakwestionował w nim zasadę uogólnionego i niezróżnicowanego zatrzymywania danych jako taką. Z punktu widzenia tego specjalnego pełnomocnika wyrok Digital Rights również nie powinien być rozumiany w ten sposób, że Trybunał określił w nim szereg kryteriów, z których wszystkie muszą być spełnione, aby dane uregulowanie mogło zostać uznane za proporcjonalne. W celu ustalenia, czy regulacje prawa szwedzkiego są zgodne z prawem Unii, należy dokonać oceny wszystkich okoliczności, takich jak zakres zatrzymywania danych w świetle przepisów dotyczących dostępu do danych, okres ich przechowywania, ochrona i bezpieczeństwo danych.

47 Na tej podstawie w dniu 19 czerwca 2014 r. PTS poinformowała Tele2 Sverige o tym, że uchybia ono zobowiązaniom przewidzianym w przepisach krajowych, ponieważ nie prowadzi zatrzymywania danych objętych LEK przez okres sześciu miesięcy do celów zwalczania przestępczości. Decyzją z dnia 27 czerwca 2014 r. PTS zobowiązała następnie operatora, aby najpóźniej do dnia 25 lipca 2014 r. przystąpił do zatrzymywania danych.

48 Uznawszy, że sprawozdanie z 2014 r. opiera się na błędnej interpretacji wyroku Digital Rights i że obowiązek zatrzymywania danych jest sprzeczny z prawami podstawowymi gwarantowanymi przez kartę, Tele2 Sverige wniosło przeciwko decyzji z dnia 27 czerwca 2014 r. skargę do Förvaltningsrätten i Stockholm (sądu administracyjnego Sztokholmu, Szwecja). Ponieważ sąd ten oddalił skargę wyrokiem z dnia 13 października 2014 r., Tele2 Sverige wniosło apelację od tego orzeczenia do sądu odsyłającego.

49 Zdaniem sądu odsyłającego zgodność przepisów prawa szwedzkiego z prawem Unii powinna być oceniana w świetle art. 15 ust. 1 dyrektywy 2002/58. Choć bowiem dyrektywa ta wprowadza zasadę, zgodnie z którą dane o ruchu i lokalizacji powinny zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu, to art. 15 ust. 1 tej dyrektywy wprowadza odstępstwo od tej zasady, ponieważ zezwala państwom członkowskim, w przypadku gdy jest to uzasadnione jednym ze wskazanych w niej powodów, na ograniczenie obowiązku usuwania lub anonimizacji danych albo wprowadzenie obowiązku zatrzymywania danych. Zatem prawo Unii w niektórych sytuacjach umożliwia ustanowienie obowiązku zatrzymywania danych dotyczących łączności elektronicznej.

50 Sąd odsyłający zastanawia się jednak, czy taki jak ten rozpatrywany w postępowaniu głównym obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych dotyczących łączności elektronicznej jest w świetle wyroku Digital Rights zgodny z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, art. 8 i art. 52 ust. 1 karty. Z uwagi na rozbieżne opinie zainteresowanych stron w tym względzie trzeba, aby Trybunał rozstrzygnął jednoznacznie kwestię tego, czy – jak twierdzi Tele2 Sverige – to uogólnione i niezróżnicowane zatrzymywanie danych dotyczących łączności elektronicznej nie jest samo w sobie sprzeczne z art. 7, art. 8 i art. 52 ust. 1 karty, czy też – jak wynika ze sprawozdania z 2014 r. – dopuszczalność prawna takiego zatrzymywania danych musi być oceniana w świetle przepisów dotyczących dostępu do danych, ich ochrony i bezpieczeństwa oraz okresu ich przechowywania.

51 W tych okolicznościach sąd odsyłający postanowił zawiesić postępowanie i wystąpić do Trybunału z następującymi pytaniami prejudycjalnymi:

„1. Czy ogólny obowiązek zatrzymywania danych o ruchu […], obejmujący wszystkie osoby, wszystkie środki łączności elektronicznej i wszystkie dane o ruchu […], bez rozróżnienia, ograniczenia, czy wyjątków do celów zwalczania przestępczości […], jest zgodny z art. 15 ust. 1 dyrektywy 2002/58/WE z uwzględnieniem art. 7, 8 i art. 52 ust. 1 karty?

2) W razie udzielenia odpowiedzi przeczącej na pytanie pierwsze czy przechowywanie może być jednak dozwolone, gdy:
   a) dostęp organów krajowych do zatrzymanych danych jest określony w sposób opisany w pkt 19–36 [postanowienia odsyłającego] oraz
   b) wymogi w zakresie ochrony i bezpieczeństwa danych są regulowane w sposób opisany w pkt 38–43 [postanowienia odsyłającego], a także
   c) wszystkie dane o ruchu telekomunikacyjnym mają być przechowywane przez sześć miesięcy licząc od dnia zakończenia połączenia, a następnie usuwane w sposób opisany w pkt 37 [postanowienia odsyłającego]?”.

Sprawa C-698/15

52 Tom Watson, P. Brice i G. Lewis wnieśli, każdy z osobna, do High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) [sądu najwyższego Anglii i Walii, wydziału Bench Queens' (izba wydziału), Zjednoczone Królestwo] skargę o sądową kontrolę legalności art. 1 DRIPA, powołując się między innymi na niezgodność tego przepisu z art. 7 i 8 karty oraz art. 8 EKPCz.

53 W wyroku z dnia 17 lipca 2015 r. sąd ten stwierdził, że w wyroku Digital Rights Trybunał Sprawiedliwości ustanowił „bezwzględne wymogi prawa Unii” mające zastosowanie do przepisów państw członkowskich w dziedzinie zatrzymywania danych dotyczących łączności elektronicznej i dostępu do takich danych. Zdaniem tego sądu, ze względu na to, iż Trybunał uznał w tym wyroku, że dyrektywa 2006/24 jest niezgodna z zasadą proporcjonalności, przepis krajowy o treści identycznej z tą dyrektywą również nie może być zgodny z tą zasadą. Wynika to z logiki leżącej u podstaw wyroku Digital Rights, według której prawo ustanawiające uogólniony system zatrzymywania danych dotyczących łączności narusza prawa zagwarantowane w art. 7 i 8 karty, o ile przepisy te nie są uzupełnione przez określony przez prawo krajowe system dostępu do danych, który przewiduje wystarczające gwarancje ochrony tych praw. Artykuł 1 DRIPA jest niezgodny z art. 7 i 8 karty, ponieważ nie ustanawia jasnych i precyzyjnych reguł dotyczących dostępu i wykorzystywania danych oraz nie uzależnia dostępu do tych danych od uprzedniej kontroli sądu lub niezależnego organu administracyjnego.

54 Minister spraw wewnętrznych wniósł apelację od tego wyroku do Court of Appeal (England & Wales) (Civil Division) (wydziału cywilnego sądu apelacyjnego dla Anglii i Walii, Zjednoczone Królestwo).

55 Sąd ten stwierdza, że art. 1 ust. 1 DRIPA upoważnia ministra spraw wewnętrznych do przyjęcia, bez jakiegokolwiek uprzedniego zezwolenia sądu lub niezależnego organu administracyjnego, powszechnego systemu nakładającego na publicznych operatorów telekomunikacyjnych obowiązek zatrzymywania wszystkich danych dotyczących wszystkich usług pocztowych lub telekomunikacyjnych, przez maksymalny okres dwunastu miesięcy, jeśli stwierdzi on, że taki wymóg jest konieczny i proporcjonalny dla realizacji celów określonych w ustawodawstwie Zjednoczonego Królestwa. Chociaż dane te nie obejmują treści połączenia, może to stanowić szczególnie silną ingerencję w prywatność użytkowników usług łączności.

56 W postanowieniu odsyłającym oraz w wyroku z dnia 20 listopada 2015 r., wydanym w postępowaniu odwoławczym, w którym sąd podjął decyzję o przedłożeniu Trybunałowi Sprawiedliwości niniejszego wniosku o wydanie orzeczenia w trybie prejudycjalnym, sąd odsyłający stwierdza, że przepisy krajowe dotyczące zatrzymywania danych są w sposób oczywisty objęte zakresem zastosowania art. 15 ust. 1 dyrektywy 2002/58, a zatem powinny odpowiadać wymogom wynikającym z karty. Jednakże zgodnie z art. 1 ust. 3 omawianej dyrektywy prawodawca Unii nie zharmonizował przepisów dotyczących dostępu do zatrzymanych danych.

57 Jeśli chodzi o znaczenie wyroku Digital Rights dla pytań powstałych w ramach zawisłego przed nim sporu, sąd odsyłający wskazuje, że w sprawie, która doprowadziła do wydania tego wyroku, do Trybunału wpłynął wniosek dotyczący ważności dyrektywy 2006/24, a nie przepisów krajowych. W szczególności ze względu na ścisły związek istniejący między zatrzymywaniem danych i dostępem do nich, konieczne byłoby, aby dyrektywie tej towarzyszył szereg gwarancji oraz aby w wyroku Digital Rights Trybunał przeanalizował, badając zgodność systemu zatrzymywania danych ustanowionego w tej dyrektywie, również reguły dotyczące dostępu do tych danych. Nie było więc zamiarem Trybunału ustanowienie w tym wyroku nadrzędnych wymogów mających zastosowanie do odnoszących się do dostępu do danych przepisów krajowych, które nie stanowią implementacji prawa Unii. Ponadto rozumowanie Trybunału było ściśle związane z celem tej dyrektywy. Ustawodawstwo krajowe powinno być jednak badane w świetle realizowanych przez nie celów oraz jego kontekstu.

58 Jeżeli chodzi o konieczność wystąpienia do Trybunału z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym, sąd odsyłający podkreśla fakt, iż w chwili wydania postanowienia odsyłającego sześć sądów innych państw członkowskich, w tym pięć w ostatniej instancji, uchyliło przepisy krajowe w oparciu o wyrok Digital Rights. Odpowiedź na przedłożone pytania nie jest zatem oczywista. Jest ona natomiast konieczna dla rozstrzygnięcia sprawy zawisłej przed tym sądem.

59 W powyższych okolicznościach sąd odsyłający postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„1) Czy wyrok Digital Rights (w tym w szczególności pkt 60–62 tego wyroku) ustanawia wiążące wymogi prawa Unii mające zastosowanie do prawa krajowego państwa członkowskiego normującego dostęp do danych zatrzymywanych zgodnie z ustawodawstwem krajowym w celu zapewnienia zgodności z art. 7 i 8 karty?

2) Czy wyrok Digital Rights rozszerza zakres stosowania art. 7 lub 8 karty w sposób wykraczający poza zakres art. 8 EKPC określony w orzecznictwie Europejskiego Trybunału Praw Człowieka?”.

W przedmiocie postępowania przed Trybunałem

60 Postanowieniem z dnia 1 lutego 2016 r., Davis i in. (C-698/15, EU:C:2016:70), prezes Trybunału postanowił uwzględnić złożony przez sąd odsyłający wniosek o objęcie sprawy C-698/15 trybem przyspieszonym przewidzianym w art. 105 § 1 regulaminu postępowania przed Trybunałem.

61 Postanowieniem prezesa Trybunału z dnia 10 marca 2016 r. sprawy C-203/15 i C-698/15 zostały połączone do celów procedury ustnej i wydania wyroku.

W przedmiocie pytań prejudycjalnych

W przedmiocie pytania pierwszego w sprawie C-203/15

62 W pierwszym pytaniu w sprawie C-203/15 Kammarrätten i Stockholm (sąd administracyjny w Sztokholmie) zmierza w istocie do ustalenia, czy art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i art. 52 ust. 1 karty należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu takiemu jak uregulowanie rozpatrywane w postępowaniu głównym, przewidującemu, do celów związanych ze zwalczaniem przestępczości, uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych o lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej.

63 Pytanie to wynika w szczególności z faktu, że dyrektywa 2006/24, którą uregulowanie krajowe rozpatrywane w postępowaniu głównym ma transponować, została w wyroku Digital Rights uznana za nieważną, ale strony nie są zgodne co do zakresu zastosowania tego wyroku oraz jego wpływu na to uregulowanie, które normuje zatrzymywanie danych o ruchu i danych o lokalizacji, jak również dostęp do tych danych przez właściwe organy krajowe.

64 Należy na wstępie zbadać, czy uregulowanie krajowe takie jak to będące przedmiotem postępowania głównego jest objęte zakresem zastosowania tego prawa Unii.

W przedmiocie zakresu stosowania dyrektywy 2002/58

65 Państwa członkowskie, które przedstawiły Trybunałowi uwagi na piśmie, wyraziły rozbieżne opinie w kwestii tego, czy i w jakim zakresie przepisy krajowe dotyczące zatrzymywania danych o ruchu i danych o lokalizacji oraz dostępu do tych danych przez organy krajowe do celów zwalczania przestępczości należą do zakresu stosowania dyrektywy 2002/58. Podczas gdy w szczególności rządy belgijski, duński, niemiecki, estoński i Irlandia oraz rząd niderlandzki uważają, że na pytanie to należy udzielić odpowiedzi twierdzącej, rząd czeski proponuje odpowiedź przeczącą, zauważając, że uregulowania te mają na celu wyłącznie zwalczanie przestępczości. Natomiast rząd Zjednoczonego Królestwa podnosi, że w zakres stosowania tej dyrektywy wchodzą tylko przepisy dotyczące zatrzymywania danych, a nie dotyczące dostępu do tych danych przez organy krajowe właściwe w dziedzinie ścigania.

66 Co się tyczy wreszcie Komisji, to chociaż podniosła ona w swoich uwagach na piśmie przedłożonych Trybunałowi w sprawie C-203/15, że uregulowanie krajowe rozpatrywane w postępowaniu głównym jest objęte zakresem stosowania dyrektywy 2002/58, to w swych uwagach pisemnych w sprawie C-698/15 wskazała, że objęte zakresem zastosowania tej dyrektywy są tylko przepisy krajowe dotyczące zatrzymywania danych, lecz już nie przepisy dotyczące dostępu organów krajowych do danych. Przepisy te powinny jednak jej zdaniem zostać uwzględnione w celu dokonania oceny, czy przepisy krajowe dotyczące zatrzymywania danych przez dostawców usług łączności elektronicznej stanowią proporcjonalną ingerencję w prawa podstawowe gwarantowane w art. 7 i 8 karty.

67 W tym względzie należy zauważyć, że zakres zastosowania dyrektywy 2002/58 należy oceniać przy uwzględnieniu, w szczególności, jej ogólnej systematyki.

68 Zgodnie z jej art. 1 ust. 1 dyrektywa 2002/58/WE przewiduje między innymi harmonizację przepisów krajowych wymaganych do 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 oraz w celu zapewnienia swobodnego przepływu w Unii tego typu danych oraz urządzeń i usług łączności elektronicznej.

69 Artykuł 1 ust. 3 tej dyrektywy 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 (zob. analogicznie, w odniesieniu do art. 3 ust. 2 tiret pierwsze dyrektywy 95/46, wyroki: z dnia 6 listopada 2003 r., Lindqvist, C-101/01, EU:C:2003:596, pkt 43; a także z dnia 16 grudnia 2008 r., Satakunnan Markkinapörssi i Satamedia, C-73/07, EU:C:2008:727, pkt 41).

70 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.

71 Artykuł 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". Artykuł 15 ust. 1 zdanie drugie tej dyrektywy wskazuje, jako przykład środków, które mogą być w tym zakresie podejmowane przez państwa członkowskie, środki „przewidujące przechowywanie danych".

72 Prawdą jest, że środki ustawodawcze, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, odnoszą się do działalności właściwej państwom lub władzom państwowym i niezwiązanej z dziedzinami, w których prowadzą działalność jednostki (zob. podobnie wyrok z dnia 29 stycznia 2008 r., Promusicae, C-275/06, EU:C:2008:54, pkt 51). Co więcej, cele, do których, zgodnie z tym przepisem, środki te muszą prowadzić, w niniejszym przypadku ochrona bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobieganie, dochodzenie, wykrywanie i karanie przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, pokrywają się zasadniczo z celami działalności, o których mowa w art. 1 ust. 3 tej dyrektywy.

73 Niemniej jednak, z uwagi na ogólną systematykę dyrektywy 2002/58, elementy wskazane w poprzedzającym punkcie niniejszego wyroku nie pozwalają na stwierdzenie, że środki ustawodawcze, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, są wyłączone z zakresu stosowania tej dyrektywy, gdyż brak tego wyłączenia oznaczałby pozbawienie rzeczonego art. 15 ust. 1 wszelkiej skuteczności (effet utile). Przy stosowaniu tego przepisu należy bowiem założyć, że środki krajowe, które są w nim wymienione, takie jak te dotyczące zatrzymywania danych w celu zwalczania poważnej przestępczości, wchodzą w zakres stosowania tej dyrektywy, ponieważ ta ostatnia upoważnia wyraźnie państwa członkowskie do ich przyjmowania wyłącznie z poszanowaniem ustanowionych w niej warunków.

74 Ponadto środki ustawodawcze, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, normują działalność dostawców usług łączności elektronicznej do celów, o których mowa w tym przepisie. Tym samym art. 15 ust. 1 w związku z art. 3 tej dyrektywy należy interpretować w ten sposób, że owe środki ustawodawcze są objęte zakresem jej stosowania.

75 W szczególności do tego zakresu stosowania należy środek ustawodawczy taki jak ten rozpatrywany w postępowaniu głównym, który nakłada na dostawców obowiązek zatrzymywania danych o ruchu i danych o lokalizacji, ponieważ taka działalność niewątpliwie wiąże się z przetwarzaniem przez nich danych osobowych.

76 Należy również do tego zakresu stosowania środek ustawodawczy taki jak w sprawie w postępowaniu głównym, dotyczący dostępu organów władz krajowych do danych zatrzymywanych przez dostawców usług łączności elektronicznej.

77 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.

78 W tych okolicznościach środek ustawodawczy, na mocy którego państwo członkowskie nakłada na podstawie art. 15 ust. 1 tej dyrektywy na dostawców usług łączności elektronicznej, do celów wymienionych w tym przepisie, obowiązek zapewnienia organom władz krajowym, na warunkach określonych przez ów środek, dostępu do danych zatrzymanych przez dostawców, dotyczy przetwarzania przez nich danych osobowych, które to przetwarzanie jest objęte zakresem stosowania tej dyrektywy.

79 Ponadto ze względu na to, że dane są zatrzymywane wyłącznie w celu zapewnienia, w stosownych przypadkach, dostępności danych dla właściwych organów krajowych, uregulowanie krajowe przewidujące to zatrzymywanie danych musi co do zasady pociągać za sobą przyjęcie przepisów regulujących dostęp właściwych organów władz krajowych do danych zatrzymywanych przez dostawców usług łączności elektronicznej.

80 Wykładnia ta znajduje potwierdzenie w art. 15 ust. 1b dyrektywy 2002/58, zgodnie z którym dostawcy ustanawiają wewnętrzne procedury umożliwiające ustosunkowanie się do wniosków o dostęp do danych osobowych użytkownika w oparciu o krajowe przepisy przyjęte zgodnie z art. 15 ust. 1 tej dyrektywy.

81 Z powyższego wynika, że uregulowanie krajowe takie jak uregulowanie będące przedmiotem postępowań głównych w sprawach C-203/15 i C-698/15 jest objęte zakresem stosowania dyrektywy 2002/58.

W przedmiocie wykładni art. 15 ust. 1 dyrektywy 2002/58/WE, z uwzględnieniem art. 7, 8 i 11 oraz art. 52 ust. 1 karty

82 Należy przypomnieć, że zgodnie z art. 1 ust. 2 dyrektywy 2002/58 jej przepisy „dookreślają i uzupełniają" dyrektywę 95/46. Jak wskazuje jej motyw 2, dyrektywa 2002/58 ma na celu zwłaszcza zapewnienie pełnego poszanowania praw określonych w art. 7 i 8 karty. W tym względzie, jak wynika z uzasadnienia projektu dyrektywy Parlamentu Europejskiego i Rady w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej [COM(2000) 385 wersja ostateczna], leżącego u źródła dyrektywy 2002/58, prawodawca Unii zamierzał „zapewnić wysoki poziom ochrony danych osobowych i prywatności, które są nieprzerwanie gwarantowane dla wszystkich usług łączności elektronicznej, bez względu na zastosowane technologie" [tłumaczenie nieoficjalne].

83 W tym celu dyrektywa 2002/58 zawiera przepisy szczególne mające na celu, jak wynika w szczególności z motywów 6 i 7, ochronę użytkowników usług łączności elektronicznej przed zagrożeniami danych osobowych i prywatności związanymi z nowymi technologiami i zwiększoną pojemnością automatycznego przechowywania i przetwarzania danych.

84 W szczególności art. 5 ust. 1 tej dyrektywy przewiduje, że państwa członkowskie powinny zapewnić, poprzez swoje ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej.

85 Zasada poufności łączności elektronicznej ustanowiona przez dyrektywę 2002/58 obejmuje między innymi – jak wynika z jej art. 5 ust. 1 zdanie drugie – co do zasady zakaz przechowywania przez osoby inne niż użytkownicy, bez ich zgody, danych o ruchu związanych z łącznością elektroniczną. Jedyny wyjątek stanowią podmioty posiadające upoważnienia zgodnie z art. 15 ust. 1 dyrektywy oraz techniczne przechowywanie, które jest niezbędne do przekazania komunikatu (zob. podobnie wyrok z dnia 29 stycznia 2008 r., Promusicae, C-275/06, EU:C:2008:54, pkt 47).

86 Tak więc, jak wynika to również z pkt 22 i 26 dyrektywy 2002/58, przetwarzanie i przechowywanie danych o ruchu są zgodnie z art. 6 tej dyrektywy dopuszczone w zakresie i przez czas niezbędny do naliczania opłat za usługi, wprowadzania ich do obrotu i świadczenia usług o wartości dodanej (zob. podobnie wyrok z dnia 29 stycznia 2008 r., Promusicae, C-275/06, EU:C:2008:54, pkt 47, 48). Co się tyczy w szczególności naliczania opłat, przetwarzanie takie jest dozwolone tylko do końca okresu, w którym rachunek może być zgodnie z prawem zakwestionowany lub w którym można dochodzić jego zapłaty. Po upływie tego okresu dane, które podlegały przetwarzaniu i przechowywaniu, powinny zostać usunięte lub uczynione anonimowymi. W odniesieniu do danych dotyczących lokalizacji innych niż dane o ruchu art. 9 ust. 1 tej dyrektywy przewiduje, że dane te mogą być przetwarzane wyłącznie po spełnieniu pewnych warunków i po ich anonimizacji lub za zgodą użytkowników lub abonentów.

87 Zakres stosowania przepisów art. 5, 6 i art. 9 ust. 1 dyrektywy 2002/58, które mają zapewnić poufność łączności i związanych z nią danych oraz zminimalizować ryzyko nadużyć, powinien być oceniany w świetle motywu 30 tej dyrektywy, zgodnie z którym „[s]ystemy dostarczania sieci i usług łączności elektronicznej powinny być zaprojektowane w taki sposób, aby ograniczać ilość niezbędnych danych osobowych do ścisłego minimum”.

88 Prawdą jest, że art. 15 ust. 1 dyrektywy 2002/58 stwarza państwom członkowskim możliwość wprowadzenia wyjątków od ustanowionego w art. 5 ust. 1 tej dyrektywy zasadniczego obowiązku zapewnienia poufności danych osobowych oraz od związanych z nim obowiązków, o których mowa w szczególności w art. 6 i 9 tej dyrektywy (zob. podobnie wyrok z dnia 29 stycznia 2008 r., Promusicae, C-275/06, EU:C:2008:54, pkt 50).

89 Niemniej jednak, w zakresie, w jakim art. 15 ust. 1 dyrektywy 2002/58 zezwala państwom członkowskim na ograniczenie zakresu tego mającego zasadnicze znaczenie obowiązku zapewnienia poufności łączności oraz związanych z nią danych o ruchu, zgodnie z utrwalonym orzecznictwem Trybunału podlega on wykładni zawężającej (zob. analogicznie wyrok z dnia 22 listopada 2012 r., Probst, C-119/12, EU:C:2012:748, pkt 23). Taki przepis nie może zatem uzasadniać uczynienia reguły z odstępstwa od tego mającego zasadnicze znaczenie obowiązku, a szczególności od zakazu przechowywania tych danych, ustanowionego w art. 5 tej dyrektywy, gdyż w znacznym stopniu pozbawiłoby to ten przepis jego znaczenia.

90 W tym względzie należy wskazać, że art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 przewiduje, że środki ustawodawcze, których dotyczy i które stanowią odstępstwo od zasady poufności łączności i związanych z nią danych o ruchu, powinny prowadzić do celu w postaci „zapewnienia bezpieczeństwa narodowego (tzn. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej” lub winny realizować jeden z innych celów, o których mowa w art. 13 ust. 1 dyrektywy 95/46, do którego odsyła art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 (zob. podobnie wyrok z dnia 29 stycznia 2008 r., Promusicae, C-275/06, EU:C:2008:54, pkt 53). Takie wyliczenie celów ma charakter wyczerpujący, jak jasno wynika z art. 15 ust. 1 zdanie drugie tej dyrektywy, zgodnie z którym środki ustawodawcze muszą być uzasadnione „na podstawie

zasad ustanowionych” w tym art. 15 ust. 1 zdanie pierwsze dyrektywy. W związku z tym państwa członkowskie nie mogą przyjmować takich środków dla celów innych niż te wymienione w tym ostatnim przepisie.

91 Ponadto art. 15 ust. 1 zdanie trzecie dyrektywy 2002/58 stanowi, że „wszystkie środki określone [w art. 15 ust. 1 tej dyrektywy] są zgodne z ogólnymi zasadami prawa [Unii], w tym zasadami określonymi w art. 6 ust. 1 i 2 TUE”, wśród których znajdują się ogólne zasady prawa i prawa podstawowe, które są zagwarantowane w karcie. Artykuł 15 ust. 1 dyrektywy 2002/58 należy zatem interpretować w świetle praw podstawowych gwarantowanych przez kartę (zob. analogicznie, w odniesieniu do dyrektywy 95/46, wyroki: z dnia 20 maja 2003 r., Österreichischer Rundfunk i in., C-465/00, C-138/01 i C-139/01, EU:C:2003:294, pkt 68; z dnia 13 maja 2014 r., Google Spain i Google, C-131/12, EU:C:2014:317, pkt 68; a także wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 38).

92 W tym względzie należy podkreślić, że nałożony na dostawców usług łączności elektronicznej przez uregulowanie krajowe takie jak to rozpatrywane w postępowaniu głównym obowiązek zatrzymywania danych o ruchu w celu ewentualnego udostępniania ich właściwym organom władz krajowych rodzi pytania dotyczące zgodności nie tylko z art. 7 i 8 karty, które są wyraźnie wskazane w pytaniach prejudycjalnych, lecz również z prawem do wolności wypowiedzi zagwarantowanym w art. 11 karty (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 25, 70).

93 Podobnie przy wykładni art. 15 ust. 1 dyrektywy 2002/58 musi być uwzględniona waga zarówno prawa do poszanowania życia prywatnego, gwarantowanego w art. 7 karty, jak i prawa do ochrony danych osobowych zagwarantowanego w art. 8 karty, w postaci wynikającej z orzecznictwa Trybunału (zob. podobnie wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 39 i przytoczone tam orzecznictwo). To samo dotyczy prawa do wolności wypowiedzi ze względu na znaczenie, jakie ma ono w społeczeństwie demokratycznym. 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 12 czerwca 2003 r., Schmidberger, C-112/00, EU:C:2003:333, pkt 79; a także z dnia 6 września 2011 r., Patriciello, C-163/10, EU:C:2011:543, pkt 31).

94 W tym względzie należy przypomnieć, że zgodnie z art. 52 ust. 1 karty wszystkie ograniczenia w korzystaniu z praw i wolności uznanych w karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności ograniczenia w korzystaniu z tych praw i wolności mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób (wyrok z dnia 15 lutego 2016 r., N., C-601/15 PPU, EU:C:2016:84, pkt 50).

95 W tym względzie art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 przewiduje, że państwa członkowskie mogą przyjąć środki stanowiące odstępstwo od zasady poufności komunikacji i związanych z nią danych o ruchu, jeżeli jest to „niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego” w świetle celów realizowanych przez ten przepis. Jeśli chodzi o motyw 11 tej dyrektywy, uściśla on, że tego rodzaju środek musi być „współmierny” w stosunku do zamierzonego celu. Co się tyczy w szczególności przechowywania danych, to art. 15 ust. 1 zdanie drugie dyrektywy 2002/58 wymaga, aby miało ono miejsce wyłącznie „przez określony czas” i gdy jest to „uzasadnione” przez jeden z celów, o których mowa w art. 15 ust. 1 zdanie pierwsze tej dyrektywy.

96 Wymóg poszanowania zasady proporcjonalności wynika również z orzecznictwa Trybunału, zgodnie z którym ochrona prawa podstawowego do poszanowania życia prywatnego na poziomie Unii wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co absolutnie konieczne (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 77; Digital Rights, pkt 52; a także wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 92).

97 Jeśli chodzi o kwestię, czy uregulowanie krajowe takie jak to będące przedmiotem sprawy C-203/15 spełnia te wymogi, należy stwierdzić, że przewiduje ono uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników w odniesieniu do wszystkich środków łączności elektronicznej i że nakłada ono na dostawców usług łączności elektronicznej obowiązek zatrzymywania tych danych w sposób regularny i ciągły, i to bez żadnych wyjątków. Jak wynika z postanowienia odsyłającego, kategorie danych, o których mowa w tych przepisach, odpowiadają zasadniczo danym, których zatrzymywanie było przewidziane przez dyrektywę 2006/24.

98 Dane, do których zatrzymywania zobowiązani są dostawcy usług łączności elektronicznej, pozwalają na odnalezienie i ustalenie źródła oraz odbiorcy połączenia, określenie daty, godziny i czasu trwania połączenia oraz jego rodzaju, określenie narzędzia komunikacji i identyfikację lokalizacji urządzenia komunikacji ruchomej. Wśród owych danych znajdują się w szczególności nazwisko i imię oraz adres abonenta lub zarejestrowanego użytkownika, numer nadawcy i odbiorcy połączenia, a także adres IP w przypadku usług internetowych. Dane te pozwalają w szczególności ustalić, z jaką osobą i za pomocą jakiego środka komunikował się abonent lub zarejestrowany użytkownik, a także – czas połączenia oraz miejsce, z którego zostało ono nawiązane. Dzięki nim można też ustalić częstotliwość komunikowania się abonenta lub zarejestrowanego użytkownika z określonymi osobami w danym okresie (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 26).

99 Całokształt tych danych może dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, których dane są zatrzymywane, takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazyjnie pokonywane trasy, podejmowane czynności, relacje społeczne i środowiska społeczne, w których osoby te się obracają (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 27). W szczególności, jak zauważył rzecznik generalny w pkt 253, 254–257 i 259 opinii, dane te dają możność ustalenia profilu danych osób, która to informacja jest z punktu widzenia prawa do poszanowania życia prywatnego równie newralgiczna co sama treść komunikatów.

100 Należy stwierdzić, że uregulowanie takie stanowi szczególnie daleko posuniętą ingerencję w prawa podstawowe, o których mowa w art. 7 i 8 karty. Okoliczność, że użytkownicy usług łączności elektronicznej nie wiedzą o tym, że dane te są zatrzymywane, może pociągnąć za sobą powstanie po ich stronie wrażenia, iż ich prywatne życie podlega ciągłej obserwacji (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 37).

101 Nawet jeżeli takie uregulowanie nie zezwala na zatrzymywanie treści komunikatu, a zatem nie jest w stanie naruszyć istoty tych praw (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 39), to obowiązek zatrzymywania danych o ruchu i danych o lokalizacji może mieć wpływ na korzystanie ze środków łączności elektronicznej, a w konsekwencji – na korzystanie przez użytkowników owych środków z zagwarantowanej w art. 11 karty swobody wypowiedzi (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 28).

102 Ze względu na wagę ingerencji w rozpatrywane prawa podstawowe, jaką niosą ze sobą przepisy krajowe przewidujące obowiązek zatrzymywania danych o ruchu i danych o lokalizacji do celów zwalczania przestępczości, uzasadniać taki środek może jedynie walka z poważną przestępczością (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 60).

103 Ponadto o ile skuteczność walki z poważną przestępczością, a zwłaszcza z przestępczością zorganizowaną i terroryzmem, może w znacznym stopniu zależeć od wykorzystania nowoczesnych technik dochodzeniowo-śledczych, tego rodzaju cel interesu ogólnego, niezależnie od jego

fundamentalnego znaczenia, nie może sam w sobie uzasadniać stwierdzenia, że przepisy krajowe przewidujące uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji należy uznać za konieczne do celów prowadzenia tej walki (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 51).

104 W tym względzie należy, po pierwsze, zauważyć, że takie uregulowanie, ze względu na swe cechy charakterystyczne opisane w pkt 97 niniejszego wyroku, prowadzi do tego, że zatrzymywanie danych o ruchu i danych o lokalizacji staje się regułą, podczas gdy system ustanowiony przez dyrektywę 2002/58 ustanawia wymóg, by takie zatrzymywanie danych było wyjątkiem.

105 Po drugie, uregulowanie krajowe takie jak to będące przedmiotem postępowania głównego, które obejmuje w sposób uogólniony wszystkich abonentów i zarejestrowanych użytkowników i dotyczy wszystkich środków łączności elektronicznej i wszystkich danych o ruchu, nie przewiduje jakiegokolwiek zróżnicowania, ograniczenia ani wyjątku zależnego od zamierzonego celu. Obejmuje ono całościowo wszystkie korzystające z usług łączności elektronicznej osoby, nawet wtedy, gdy nie ma wobec nich żadnych podstaw, nawet pośrednich, do wszczęcia postępowania karnego. Ma ono zastosowanie nawet wobec tych osób, co do których brak jest dowodów mogących sugerować, że ich zachowanie może mieć związek, chociażby pośredni i daleki, z poważnymi przestępstwami. Ponadto dyrektywa nie przewiduje żadnych wyjątków, a więc w rezultacie ma zastosowanie nawet wobec tych osób, których łączność na gruncie przepisów prawa krajowego objęta jest tajemnicą zawodową (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 57, 58).

106 Takie uregulowanie nie wymaga istnienia żadnego związku między danymi, których zatrzymywanie nakazuje, a zagrożeniem dla bezpieczeństwa publicznego. Nie zawiera ono zwłaszcza żadnych ograniczeń czasowych czy geograficznych ani ograniczeń do grupy osób, które można podejrzewać o taki czy inny rodzaj uczestnictwa w poważnym przestępstwie, tak by obowiązek zatrzymywania danych obejmował tylko te dane, co do których z jakiegoś powodu można zakładać, że mają znaczenie dla walki z przestępczością (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 59).

107 Uregulowanie krajowe takie jak uregulowanie będące przedmiotem sporu zawisłego przed sądem krajowym wykracza więc poza granice tego, co jest absolutnie konieczne, i nie można go uznać za uzasadnione w demokratycznym społeczeństwie, jak tego wymaga art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty.

108 Natomiast nie jest sprzeczne z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty przyjęcie przez państwa członkowskie przepisów krajowych dopuszczających w ramach prewencji indywidualne zatrzymywanie danych dotyczących ruchu i danych o lokalizacji w celu zwalczania poważnej przestępczości, pod warunkiem że takie zatrzymywanie danych – w zakresie dotyczącym kategorii danych podlegających zatrzymywaniu, stosowanych środków łączności, zaangażowanych w ten proces podmiotów oraz przyjętego okresu przechowywania danych – nie będzie wykraczać poza to, co jest absolutnie konieczne.

109 Aby spełniać wymogi określone w poprzednim punkcie niniejszego wyroku, rozpatrywane uregulowanie krajowe musi, w pierwszej kolejności, zawierać jasne i dokładne reguły dotyczące zakresu i sposobu stosowania rozpatrywanego środka związanego z zatrzymywaniem danych, a także ustanawiać minimalne zabezpieczenia służące temu, aby osoby, których dane zostały zatrzymane, miały wystarczające gwarancje rzeczywistej ochrony ich danych osobowych przed ryzykiem nadużyć. Uregulowanie to winno w szczególności wskazywać okoliczności i warunki, w których środek związany z zatrzymywaniem danych może zostać zastosowany tytułem prewencji, co pozwoli zagwarantować, by środek ów ograniczał się do tego, co jest absolutnie konieczne (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 54 i przytoczone tam orzecznictwo).

110 W drugiej kolejności, jeżeli chodzi o materialne przesłanki, jakie musi spełnić uregulowanie krajowe umożliwiające w ramach zwalczania przestępczości na prewencyjne zatrzymywanie danych o ruchu i danych o lokalizacji, aby zagwarantować, że będzie ono ograniczone do tego, co jest absolutnie konieczne, należy zauważyć, że chociaż przesłanki te mogą się różnić w zależności od środków podjętych w celu zapobiegania, dochodzenia, wykrywania i ścigania poważnych przestępstw, to jednak zatrzymywanie danych musi zawsze spełniać obiektywne kryteria określające związek między danymi, które mają być zatrzymywane, a realizowanym celem. W szczególności przesłanki te muszą w praktyce umożliwiać określenie rzeczywistego zakresu środka, a w konsekwencji – grona objętych nim osób.

111 Jeśli chodzi o ograniczenie środka do kategorii ewentualnie objętych nim osób i sytuacji, przepisy krajowe winny opierać się na obiektywnych elementach umożliwiających namierzenie osób, których dane mogą mieć związek, nawet pośredni, z poważną przestępczością, przyczyniać się w taki lub inny sposób do walki z ową przestępczością lub też zapobiegać powstawaniu poważnych zagrożeń dla bezpieczeństwa publicznego. Tego rodzaju określenie może być dokonane w oparciu o kryterium geograficzne, gdy właściwe władze krajowe na podstawie obiektywnych elementów uważają, że w jednym lub kilku obszarach geograficznych istnieje wysokie ryzyko przygotowania lub popełnienia takich czynów.

112 Mając na względzie całość powyższych rozważań, należy na pierwsze pytanie w sprawie C-203/15 odpowiedzieć, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8, 11 i art. 52 ust. 1 karty należy interpretować w ten sposób, iż stoi on na przeszkodzie uregulowaniu krajowemu przewidującemu do celów zwalczania przestępczości uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej.

W przedmiocie pytania drugiego w sprawie C-203/15 i pytania pierwszego w sprawie C-698/15

113 Należy zauważyć tytułem wstępu, że Kammarrätten i Stockholm (sąd administracyjny w Sztokholmie) przedłożył pytanie drugie w sprawie C-203/15 tylko na wypadek odpowiedzi przeczącej na swe pytanie pierwsze. Niemniej jednak jego pytanie drugie jest niezależne od kwestii tego, czy dane są zatrzymywane w sposób uogólniony, czy też indywidualny, w znaczeniu opisanym w pkt 108–111 niniejszego wyroku. Należy zatem udzielić wspólnej odpowiedzi na pytanie drugie w sprawie C-203/15 i pytanie pierwsze w sprawie C-698/15, które zostało zadane niezależnie od zakresu obowiązku zatrzymywania danych nałożonego na dostawców usług łączności elektronicznej.

114 Za pomocą swych pytań – drugiego w sprawie C-203/15 i pierwszego w sprawie C-698/15 – sądy odsyłające zmierzają w istocie do ustalenia, czy art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i art. 52 ust. 1 karty należy interpretować w ten sposób, że stoi on na przeszkodzie obowiązywaniu uregulowań krajowych dotyczących ochrony i bezpieczeństwa danych o ruchu i danych o lokalizacji, a w szczególności dostępu właściwych organów krajowych do przechowywanych danych, nie ograniczając tego dostępu jedynie do celów walki z poważną przestępczością, bez poddania owego dostępu uprzedniej kontroli przez sąd lub niezależny organ administracyjny i bez wymogu, aby dane te były przechowywane na obszarze Unii.

115 Jeśli chodzi o cele mogące uzasadniać przepisy krajowe stanowiące odstępstwo od zasady poufności łączności elektronicznej należy przypomnieć, że w zakresie, w jakim, jak zostało to stwierdzone w pkt 90 i 102 niniejszego wyroku, wyliczenie celów dokonane w art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 ma charakter wyczerpujący, dostęp do zatrzymanych danych powinien rzeczywiście odpowiadać wyłącznie jednemu z tych celów. Ponadto ze względu na to, że cel realizowany przez przepis powinien być powiązany z wagą ingerencji w prawa podstawowe, jaką dostęp taki pociąga za sobą, dostęp do zatrzymanych danych w ramach zapobiegania, dochodzenia, wykrywania i ścigania przestępstw może uzasadniać jedynie walka z poważną przestępczością.

116 Co się tyczy poszanowania zasady proporcjonalności, przepisy krajowe normujące warunki, w których dostawcy usług łączności elektronicznej powinni zapewnić właściwym organom władz krajowych dostęp do przechowywanych danych, muszą zapewniać, zgodnie z tym, co zostało stwierdzone w pkt 95 i 96 niniejszego wyroku, że taki dostęp może mieć miejsce tylko w zakresie, w jakim jest to absolutnie konieczne.

117 Ponadto środki ustawodawcze, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, muszą, zgodnie z motywem 11 dyrektywy, „podlegać stosownym zabezpieczeniom", ponieważ, jak wynika z orzecznictwa przytoczonego w pkt 109 niniejszego wyroku, środek taki powinien ustanawiać jasne i dokładne reguły określające, w jakich okolicznościach i pod jakimi warunkami dostawcy usług łączności elektronicznej powinni udzielać właściwym organom władz krajowym dostępu do tych danych. Ponadto tego rodzaju środek musi być prawnie wiążący w prawie krajowym.

118 Aby zagwarantować, że dostęp właściwych organów władz krajowych do zatrzymanych danych jest ograniczony do tego, co ściśle niezbędne, warunki, w jakich dostawcy usług łączności elektronicznej udzielają owego dostępu, muszą być oczywiście określone w prawie krajowym. Niemniej jednak rozpatrywane przepisy krajowe nie mogą ograniczać się do ustanowienia wymogu, by dostęp ten uwzględniał jeden z realizowanych przez dyrektywę 2002/58 i określonych w jej art. 15 ust. 1 celów, nawet jeśli jest nim prowadzenie walki z poważną przestępczością. Takie uregulowanie krajowe powinno bowiem ustanawiać również materialne i proceduralne warunki regulujące dostęp odpowiednich organów władz krajowych do przechowywanych danych (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 61).

119 I tak, jeśli powszechny dostęp do zatrzymanych danych, niezależnie od jakiegokolwiek związku, nawet pośredniego, z realizowanym celem, nie może być uważany za ograniczony do tego, co absolutnie konieczne, rozpatrywane przepisy krajowe winny opierać się na obiektywnych kryteriach umożliwiających określenie okoliczności i warunków przyznania dostępu właściwym organom władz krajowych do danych abonentów lub zarejestrowanych użytkowników. W tym względzie, biorąc pod uwagę cel polegający na zwalczaniu poważnej przestępczości, dostęp ten może co do zasady zostać przyznany jedynie w odniesieniu do danych dotyczących osób podejrzewanych o planowanie, popełnianie czy też popełnienie już poważnego przestępstwa bądź też zaangażowanych w taki czy inny sposób w takie przestępstwo (zob. analogicznie wyrok ETPC z dnia 4 grudnia 2015 r., Zakharov przeciwko Rosji, CE:ECHR:2015:1204JUD004714306, § 260). Niemniej jednak w szczególnych sytuacjach, takich jak te, w których istotne interesy związane z bezpieczeństwem narodowym, obroną czy też bezpieczeństwem publicznym są zagrożone wskutek działań terrorystycznych, dostęp do danych dotyczących innych osób może zostać przyznany również wówczas, gdy istnieją obiektywne elementy pozwalające uznać, że dane te mogłyby w konkretnym przypadku rzeczywiście przyczynić się do zwalczania takich działań.

120 W celu zapewnienia w praktyce pełnej zgodności z tymi warunkami ważne jest, aby dostęp organów krajowych do zatrzymanych danych był co do zasady, z wyjątkiem należycie uzasadnionych pilnych przypadków, uzależniony od uprzedniej kontroli sądu lub niezależnego organu administracyjnego, a decyzja tego sądu lub organu była wydawana na uzasadniony wniosek owych organów, złożony w szczególności w ramach postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 62; zob. również analogicznie, w odniesieniu do art. 8 EKPC, wyrok ETPC z dnia 12 stycznia 2016 r., Szabó i Vissy przeciwko Węgrom, CE:ECHR:2016:0112JUD003713814, §§ 77, 80).

121 Podobnie ważne jest, aby właściwe organy władz krajowych, którym przyznano dostęp do przechowywanych danych, informowały o tym zainteresowane osoby w trybie właściwego postępowania krajowego, od chwili, w której informacja taka nie będzie mogła narazić na szwank prowadzonych przez te organy postępowań dochodzeniowo-śledczych. Informacja ta jest bowiem niezbędna do tego, aby umożliwić im w szczególności wykonanie prawa do wniesienia skargi, wyraźnie przewidziane

w art. 15 ust. 2 dyrektywy 2002/58 w związku z art. 22 dyrektywy 95/46 w przypadku naruszenia ich praw (zob. analogicznie wyrok z dnia 7 maja 2009 r., Rijkeboer, C-553/07, EU:C:2009:293, pkt 52; a także wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 95).

122 W odniesieniu do reguł związanych z bezpieczeństwem i ochroną danych zatrzymywanych przez dostawców usług łączności elektronicznej należy stwierdzić, że art. 15 ust. 1 dyrektywy 2002/58 nie pozwala państwom członkowskim na odstąpienie od art. 4 ust. 1 oraz art. 4 ust. 1a tej dyrektywy. Przepisy te ustanawiają wymóg, aby dostawcy zastosowali właściwe środki techniczne i organizacyjne niezbędne dla zapewnienia skutecznej ochrony zatrzymanych danych przed ryzykiem nadużyć oraz przed jakimkolwiek niedozwolonym dostępem do tych danych. Uwzględniając ilość zatrzymywanych danych, ich newralgiczny charakter oraz prawdopodobieństwo bezprawnego uzyskania dostępu do nich, dostawcy usług łączności elektronicznej, aby zapewnić integralność i poufność tych danych, muszą zapewnić za pomocą środków technicznych i organizacyjnych szczególnie wysoki poziom ochrony i bezpieczeństwa. W szczególności uregulowanie krajowe powinno ustanawiać zarówno wymóg przechowywania danych na terytorium Unii, jak też nieodwracalnego ich niszczenia po upływie okresu ich przechowywania (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 66–68).

123 W każdym wypadku państwa członkowskie mają zapewnić, by niezależny organ nadzorował przestrzeganie poziomu ochrony zagwarantowanego przez prawo Unii w zakresie ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych, ponieważ wymóg takiej kontroli został wyraźnie ustanowiony w art. 8 ust. 3 karty i stanowi, jak wynika z orzecznictwa Trybunału, zasadniczy element poszanowania ochrony osób fizycznych w zakresie przetwarzania danych osobowych. W przeciwnym przypadku osoby, których dane osobowe zostały zatrzymane, zostałyby pozbawione zagwarantowanego przez art. 8 ust. 1 i 3 karty prawa do zwrócenia się do krajowych organów nadzorczych ze skargą służącą ochronie ich danych (zob. podobnie wyrok Digital Rights, pkt 68; a także wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 41, 58).

124 Zadaniem sądów odsyłających jest zbadanie, czy i w jakim stopniu uregulowania krajowe rozpatrywane w postępowaniu głównym spełniają wymogi wynikające z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, tak jak określono w pkt 115–123 niniejszego wyroku, zarówno w odniesieniu do dostępu organów krajowych do zatrzymanych danych, jak i ochrony oraz bezpieczeństwa tych danych.

125 Mając na względzie całość powyższych rozważań, należy na pytanie drugie w sprawie C-203/15 i pytanie pierwsze w sprawie C-698/15 odpowiedzieć, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty należy interpretować w ten sposób, iż stoi on na przeszkodzie obowiązywaniu uregulowań krajowych dotyczących ochrony i bezpieczeństwa danych o ruchu i danych o lokalizacji, a w szczególności dostępu właściwych organów władz krajowych do przechowywanych danych, które to przepisy, w ramach zwalczania przestępczości nie ograniczają tego dostępu jedynie do celów walki z poważną przestępczością, nie uzależniają przyznania tego dostępu od uprzedniej kontroli sądowej lub niezależnego organu administracyjnego i nie ustanawiają wymogu, aby dane te były przechowywane na obszarze Unii.

W przedmiocie pytania drugiego w sprawie C-698/15

126 Za pomocą pytania drugiego w sprawie C-698/15 Court of Appeal (England & Wales) (Civil Division) (wydział cywilny sądu apelacyjnego dla Anglii i Walii) zmierza do ustalenia, czy w wyroku Digital Rights Trybunał dokonał wykładni art. 7 lub art. 8 karty w sposób wykraczający poza wykładnię art. 8 EKPC dokonaną przez Europejski Trybunał Praw Człowieka.

127 Na wstępie należy przypomnieć, że jakkolwiek zgodnie z art. 6 ust. 3 TUE prawa podstawowe chronione na mocy EKPC są częścią prawa Unii jako jego zasady ogólne, wspomniana konwencja, do czasu przystąpienia do niej Unii, nie stanowi aktu prawnego formalnie obowiązującego w unijnym porządku prawnym (zob. podobnie wyrok z dnia 15 lutego 2016 r., N., C-601/15 PPU, EU:C:2016:84, pkt 45 i przytoczone tam orzecznictwo).

128 Tym samym w niniejszej sprawie wykładni dyrektywy 2002/58 należy dokonywać wyłącznie w świetle praw podstawowych gwarantowanych przez kartę (zob. podobnie wyrok z dnia 15 lutego 2016 r., N., C-601/15 PPU, EU:C:2016:84, pkt 46 i przytoczone tam orzecznictwo).

129 Ponadto należy przypomnieć, że wyjaśnienia związane z art. 52 karty wskazują, iż celem art. 52 ust. 3 jest zapewnienie niezbędnej spójności między kartą a EKPC, co jednak nie może mieć „negatywnego wpływu na autonomię prawa Unii i Trybunału Sprawiedliwości Unii Europejskiej" (wyrok z dnia 15 lutego 2016 r., N., C-601/15 PPU, EU:C:2016:84, pkt 47). W szczególności, jak przewiduje wyraźnie art. 52 ust. 3 zdanie drugie karty, art. 52 ust. 3 zdanie pierwsze nie stanowi przeszkody, aby prawo Unii przyznawało ochronę szerszą niż EKPC. Do tego dochodzi wreszcie fakt, że art. 8 karty dotyczy prawa podstawowego odrębnego od prawa przewidzianego w art. 7 karty, które nie ma odpowiednika w EKPC.

130 Tymczasem zgodnie z utrwalonym orzecznictwem Trybunału uzasadnieniem zwrócenia się z pytaniem prejudycjalnym nie może być zamiar uzyskania opinii doradczych w odniesieniu do pytań o charakterze ogólnym czy hipotetycznym; winna nim być potrzeba związana nierozerwalnie z rzeczywistym rozstrzygnięciem sporu dotyczącego prawa Unii (zob. podobnie wyroki: z dnia 24 kwietnia 2012 r., Kamberaj, C-571/10, EU:C:2012:233, pkt 41; z dnia 26 lutego 2013 r., Åkerberg Fransson, C-617/10, EU:C:2013:105, pkt 42; a także z dnia 27 lutego 2014 r., Pohotovosť, C-470/12, EU:C:2014:101, pkt 29).

131 W niniejszej sprawie, z uwagi na rozważania zawarte w pkt 128 i 129 niniejszego wyroku, pytanie, czy ochrona przyznana w art. 7 i 8 karty jest szersza od ochrony zagwarantowanej w art. 8 EKPC, pozostaje bez wpływu na wykładnię, w kontekście karty, dyrektywy 2002/58, która jest rozpatrywana w postępowaniu głównym będącym u podstaw sprawy C-698/15.

132 Nie wydaje się zatem, aby odpowiedź na pytanie drugie w sprawie C-698/15 mogła dostarczyć takich kryteriów wykładni prawa Unii, które są konieczne do rozstrzygnięcia rzeczonego sporu w świetle tego prawa.

133 Wynika stąd, że drugie pytanie w sprawie C-698/15 jest niedopuszczalne.

W przedmiocie kosztów

134 Dla stron w postępowaniu głównym niniejsze postępowanie ma charakter incydentalny, dotyczy bowiem kwestii podniesionej przed tym sądem; 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 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 dotycząca prywatności i łączności elektronicznej), zmienionej dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r., w związku z art. 7, 8, 11 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej, należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu**

przewidującemu do celów zwalczania przestępczości uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej.

2) **Artykuł 15 ust. 1 dyrektywy 2002/58, po zmianach wprowadzonych dyrektywą 2009/136, w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych należy interpretować w ten sposób, że stoi on na przeszkodzie obowiązywaniu uregulowań krajowych dotyczących ochrony i bezpieczeństwa danych o ruchu i danych o lokalizacji, a w szczególności dostępu właściwych organów władz krajowych do przechowywanych danych, które to przepisy, w ramach zwalczania przestępczości, nie ograniczają tego dostępu jedynie do celów walki z poważną przestępczością, nie uzależniają przyznania go od uprzedniej kontroli sprawowanej przez sąd lub niezależny organ administracyjny i nie ustanawiają wymogu, aby dane te były przechowywane na obszarze Unii.**

3) **Drugie z zadanych przez Court of Appeal (England & Wales) (Civil Division) (wydział cywilny sądu apelacyjnego dla Anglii i Walii, Zjednoczone Królestwo) pytań jest niedopuszczalne.**

Podpisy