Sprawa C-793/19

Streszczenie wniosku o wydanie orzeczenia w trybie prejudycjalnym zgodnie z art. 98 § 1 regulaminu postępowania przed Trybunałem Sprawiedliwości

Data wpływu:

29 października 2019 r.

Oznaczenie sądu odsyłającego:

Bundesverwaltungsgericht (Niemcy)

Data wydania postanowienia o wystąpieniu z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym:

25 września 2019 r.

Strona skarżąca i druga strona postępowania rewizyjnego:

SpaceNet AG

Druga strona postępowania i strona wnosząca skargę rewizyjną:

Republika Federalna Niemiec

Przedmiot postępowania głównego

Skarga o stwierdzenie, że spółka SpaceNet nie jest zobowiązana do przechowywania wymienionych w § 113 b ust. 3 TKG danych o ruchu klientów, na których rzecz świadczy ona usługi dostępu do Internetu.

Przedmiot i podstawa prawna odesłania prejudycjalnego

Wykładnia prawa Unii, w szczególności art. 15 ust. 1 dyrektywy 2002/58 oraz wyroku Trybunału w sprawie Tele2 Sverige i Watson i in.; art. 267 TFUE.

Pytanie prejudycjalne

Czy w świetle art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej z jednej strony i art. 6 Karty praw podstawowych Unii Europejskiej oraz art. 4 Traktatu o Unii Europejskiej z drugiej strony art. 15 dyrektywy 2002/58/WE należy interpretować w ten sposób, że stoi on na przeszkodzie

uregulowaniu krajowemu, które nakłada na operatorów dostępnych publicznie usług łączności elektronicznej obowiązek zatrzymywania danych o ruchu i lokalizacji użytkowników końcowych tych usług, jeżeli obowiązek ten

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

– przedmiotem obowiązku przechowywania przy świadczeniu dostępnych publicznie usług telefonicznych – w tym transmisji krótkich wiadomości tekstowych, wiadomości multimedialnych lub podobnych wiadomości oraz w przypadku połączeń nieodebranych lub nieudanych – są następujące dane:

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

  – data i godzina rozpoczęcia i zakończenia połączenia lub w przypadku transmisji krótkiej wiadomości tekstowej, wiadomości multimedialnej lub podobnej wiadomości – data wysłania i otrzymania informacji ze wskazaniem bazowej strefy czasowej;

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

  – ponadto w przypadku usług telefonii komórkowej:

    – międzynarodowy numer tożsamości telefonicznej abonenta mobilnego nadawcy i odbiorcy połączenia;

    – międzynarodowy numer fabryczny aparatu telefonicznego nadawcy i odbiorcy połączenia;

    – data i godzina pierwszej aktywacji usługi wraz ze wskazaniem bazowej strefy czasowej, w przypadku gdy usługi zostały opłacone z góry;

    – oznaczenie komórek, które zostały wykorzystane przez numer wywołujący i wywołany na początku połączenia;

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

– przedmiotem obowiązku przechowywania przy świadczeniu dostępnych publicznie usług dostępu do Internetu są następujące dane:

  – adres IP przypisany abonentowi w celu korzystania z Internetu;

  - jednoznaczny identyfikator łącza, przez które następuje korzystanie z Internetu, oraz przypisany identyfikator użytkownika;
  - data i godzina rozpoczęcia i zakończenia korzystania z Internetu pod przypisanym adresem IP ze wskazaniem bazowej strefy czasowej;
  - w przypadku korzystania mobilnego oznaczenie komórki wykorzystanej na początku połączenia internetowego;
- nie mogą być przechowywane następujące dane:
  - treść komunikatu;
  - dane dotyczące przeglądanych stron internetowych;
  - dane usług poczty elektronicznej;
  - dane leżące u podstawi połączeń z lub do określonych numerów osób, organów i organizacji w sferach społecznych lub religijnych;
- okres zatrzymywania danych wynosi w przypadku danych dotyczących lokalizacji, czyli oznaczenia wykorzystanej komórki, cztery tygodnie, a w przypadku pozostałych danych – dziesięć tygodni;
- zapewniona jest skuteczna ochrona zatrzymywanych danych przed ryzykiem nadużyć oraz przed nieuprawnionym dostępem, oraz
- zatrzymywane dane mogą być wykorzystywane wyłącznie w celu ścigania szczególnie ciężkich przestępstw oraz zapobiegania konkretnym zagrożeniom dla zdrowia, życia lub wolności danej osoby, lub dla istnienia państwa federalnego lub kraju związkowego, z wyjątkiem adresu IP przypisanego abonentowi w celu korzystania z Internetu, którego używanie jest dozwolone w ramach udzielania informacji na temat zgromadzonych danych w celu ścigania wszystkich przestępstw, w celu zapobiegania zagrożeniom dla bezpieczeństwa i porządku publicznego oraz w celu wykonywania zadań służb wywiadowczych?

Przywołane przepisy prawa Unii

Karta praw podstawowych Unii Europejskiej (zwana dalej „kartą”), art. 6, 7, 8, 11, 52

Traktat o Unii Europejskiej (zwany dalej „TUE”): art. 4, 6;

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), zmieniona dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady z dnia

25 listopada 2009 r. (zwana dalej „dyrektywą 2002/58”), art. 5, 6, 8, 9, w szczególności art. 15; motyw 11

Przywołane przepisy prawa krajowego

Telekommunikationsgesetz (ustawa o telekomunikacji, zwana dalej „TKG”), § 113a ust. 1 zdanie pierwsze (zatytułowany „Podmioty zobowiązane”), § 113b (zatytułowany „Obowiązki dotyczące przechowywania danych o ruchu”), § 113c (zatytułowany „Wykorzystywanie danych”), § 113d (zatytułowany „Zapewnienie bezpieczeństwa danych”), § 113e (zatytułowany „Protokołowanie” [przez podmiot zobowiązany dostępu do przechowywanych danych]), § 113f (zatytułowany „Katalog wymogów” [w odniesieniu do przepisów technicznych i innych środków]), § 99 ust. 2 (zatytułowany „Wykaz indywidualnych połączeń”, podmioty wyłączone z identyfikacji w wykazie indywidualnych połączeń)

Strafprozessordnung (kodeks postępowania karnego, zwany dalej „StPO”), § 100g ust. 2 (zatytułowany „Gromadzenie danych o ruchu”, o których mowa w § 113b TKG)

Przywołane orzecznictwo Trybunału

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970 (zwany dalej „wyrokiem Tele2 Sverige i Watson i in.”)

Wyrok z dnia 8 kwietnia 2014 r., Digital Rights Ireland i Seitlinger i in., C-293/12 i C-594/12, EU:C:2014:238 (zwany dalej „wyrokiem Digital Rights Ireland i in.”)

Opinia nr 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592

Ponadto wyroki: z dnia 29 lipca 2019 r., Funke Medien, C-469/17, EU:C:2019:623; z dnia 9 marca 1978 r., Simmenthal, 106/77, EU:C:1978:49; z dnia 3 maja 2005 r., Berlusconi i in., C-387/02, C-391/02 i C-403/02, EU:C:2005:270: z dnia 22 czerwca 2010 r., Melki i Abdeli, C-188/10 i C-189/10, EU:C:2010:363: z dnia 18 września 2014 r., Vueling Airlines, C-487/12, EU:C:2014:2232

Zwięzłe przedstawienie okoliczności faktycznych i przebiegu postępowania

1 Skarżąca, SpaceNetAG (zwana dalej „skarżącą” lub „spółką SpaceNet”), świadczy dostępne publicznie usługi dostępu do Internetu. Kwestionuje ona nałożony na nią na podstawie § 113a ust. 1 w związku z § 113b Telekommunikationsgesetz (TKG) zmienionej ustawą z dnia 10 grudnia 2015 r. obowiązek zatrzymywania od dnia 1 lipca 2017 r. danych o ruchu telekomunikacyjnym jej klientów.

2 W pierwszej instancji sąd administracyjny stwierdził, że spółka SpaceNet nie jest zobowiązana do przechowywania wymienionych w § 113b ust. 3 TKG danych o ruchu telekomunikacyjnym jej klientów, na których rzecz świadczy usługę dostępu do Internetu. Druga strona postępowania, Republika Federalna Niemiec (zwana dalej „stroną przeciwną") zaskarżyła wyrok sądu administracyjnego w drodze bezpośredniej skargi rewizyjnej („Sprungrevision").

3 Skarga rewizyjna będzie skuteczna tylko wtedy, gdy przewidziany w wymienionych przepisach TKG, ciążący na podmiocie świadczącym dostępne publicznie usługi telekomunikacyjne (zwanym dalej „dostawcą usług telekomunikacyjnych") obowiązek zatrzymywania danych o ruchu telekomunikacyjnym nie jest sprzeczny z prawem Unii.

4 Ciążący na dostawcach usług telekomunikacyjnych obowiązek przechowywania przez ograniczony czas niektórych danych o ruchu został uregulowany na nowo w Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten z dnia 10 grudnia 2015 r. (ustawie wprowadzającej obowiązek przechowywania i maksymalny termin przechowywania danych o ruchu, zwanej dalej „ustawą z dnia 10 grudnia 2015 r.").

5 Nowe uregulowanie było konieczne po tym, jak Bundesverfassungsgericht (federalny trybunał konstytucyjny) stwierdził w wyroku z 2010 r. nieważność wcześniejszych przepisów regulujących zatrzymywanie danych z powodu naruszenia praw podstawowych oraz po tym, jak w 2014 r. w wyroku Digital Rights Ireland i in. stwierdzono nieważność dyrektywy 2006/24, która została przetransponowana za pomocą tych wcześniejszych przepisów. Ustawa z dnia 10 grudnia 2015 r. ma wypełniać luki w ściganiu karnym i zapobieganiu zagrożeniom i jednocześnie uwzględniać wynikające z wymienionych orzeczeń wymogi konstytucyjne i unijne.

6 Udzielenie odpowiedzi na pytanie, czy przewidziany w § 113a ust. 1 w związku z § 113b TKG obowiązek przechowywania danych jest sprzeczny z prawem Unii, wymaga dokonania wykładni dyrektywy 2002/58 przez Trybunał Sprawiedliwości, a w szczególności wyjaśnienia, jak należy rozumieć wyrok Tele2 Sverige i Watson i in.

Zwięzłe uzasadnienie odesłania prejudycjalnego

7 Obowiązek przechowywania danych o ruchu telekomunikacyjnym uregulowany w § 113a ust. 1 zdanie pierwsze w związku z § 113b TKG ogranicza prawa, o których mowa w art. 5 ust. 1, art. 6 ust. 1 i art. 9 ust. 1 dyrektywy 2002/58.

8 Stanowi on ingerencję w poufność łączności elektronicznej, chronioną na podstawie art. 5 ust. 1 zdanie pierwsze dyrektywy, i jest sprzeczny z zasadą, zgodnie z którą każdej osobie innej niż użytkownik nie wolno co do zasady przechowywać bez jego zgody danych o ruchu związanych z łącznością elektroniczną.

9 Ponadto nie spełnia on przewidzianego w art. 6 dyrektywy wymogu, zgodnie z którym dane o ruchu mogą być przetwarzane i przechowywane wyłącznie w celu naliczania opłat za usługi, ich wprowadzania do obrotu oraz świadczenia usług tworzących wartość dodaną, w zakresie i przez czas niezbędny do tego rodzaju usług.

10 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, art. 9 ust. 1 zdanie pierwsze dyrektywy 2002/58 stanowi, że 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. Ustawowa regulacja odbiega również od tego wymogu w zakresie, w jakim na podstawie § 113b ust. 1 pkt 2 w związku z ust. 4 TKG przechowywaniu podlegają również wymienione tam dane.

11 Ograniczenie praw, o których mowa w art. 5 ust. 1, art. 6 ust. 1 i art. 9 ust. 1 dyrektywy 2002/58/WE, jest uzasadnione tylko wtedy, gdy uregulowanie zawarte w § 113a ust. 1 zdanie pierwsze w związku z § 113b TKG może zostać oparte na art. 15 ust. 1 dyrektywy 2002/58.

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

13 Zgodnie z wywodami Trybunału zawartymi w wyroku Tele2 Sverige i Watson i in., w szczególności w pkt 82 i nast. oraz 108 i nast. tego wyroku, dopuszczalność krajowego uregulowania dotyczącego zatrzymywania danych na podstawie art. 15 ust. 1 dyrektywy 2002/58 wymaga istnienia wystarczającego powodu. Oznacza to, że chodzi o osoby, w odniesieniu do których istnieją wskazówki świadczące o tym, że mają one związek z poważnymi przestępstwami, że ograniczenie ma zastosowanie do regionu, okresu oraz środków komunikacji, które są istotne dla danego powodu, oraz że są objęte jedynie dane niezbędne do wyjaśnienia wskazanych przestępstw.

14 Stanowisko strony przeciwnej, że już samą okoliczność korzystania z usług dostępu do Internetu lub usług telefonicznych należy ocenić jako wystarczający

powód do przechowywania danych, w sposób oczywisty nie jest zgodne z powyższymi wnioskami. Wyrażonego w wyroku Tele2 Sverige i Watson i in. założenia występowania ogólnej niezgodności z prawem Unii w przypadku każdego niewymagającego uzasadnienia zatrzymania danych nie podważa również powołanie się przez stronę przeciwną na opinię Trybunału z dnia 26 lipca 2017 r. dotyczącą Umowy między Kanadą a Unią Europejską o przekazywaniu danych dotyczących przelotu pasażera. Prawdą jest, że w ramach konieczności związanych z tą umową ingerencji w prawa podstawowe do poszanowania życia prywatnego i do ochrony danych osobowych Trybunał podkreślił, że dane PNR mogą być przekazywane do Kanady niezależnie od istnienia obiektywnych okoliczności wskazujących na to, że pasażerowie stwarzają zagrożenie dla bezpieczeństwa publicznego w Kanadzie. Jednakże nie chodzi tutaj o niewymagające uzasadnienia zatrzymywanie danych, ponieważ przechowywanie i przekazywanie danych jest związane z kontrolą graniczną, której na podstawie obowiązujących przepisów prawa kanadyjskiego podlegają wszyscy pasażerowie pragnący wjechać do Kanady lub wyjechać z Kanady. Wraz z wyjazdem pasażerów ustaje powód do przechowywania danych. Dlatego też dalsze zatrzymywanie danych po tej chwili wymaga – jako nowego powodu – istnienia obiektywnych okoliczności wskazujących na to, że odnośni pasażerowie mogą stanowić zagrożenie związane z walką z terroryzmem i poważną przestępczością międzynarodową.

15 Jeżeli orzecznictwo Trybunału powinno być rozumiane w ten sposób, że niewymagające uzasadnienia zatrzymywanie danych nie jest w żadnych okolicznościach zgodne z prawem Unii, wówczas skarga rewizyjna wniesiona przez stronę przeciwną na zaskarżony wyrok sądu administracyjnego nie może być skuteczna. Tak jak szwedzkie i brytyjskie uregulowania dotyczące zatrzymywania danych, które były przedmiotem wyroku Tele2 Sverige i Watson i in., § 113a ust. 1 zdanie pierwsze w związku z § 113b TKG nie wymaga bowiem wykraczającego poza zwykłe korzystanie z usług dostępu do Internetu lub usług telefonicznych powodu do przechowywania danych ani związku pomiędzy przechowywanymi danymi a przestępstwem lub zagrożeniem dla bezpieczeństwa publicznego. Przeciwnie, chodzi o uregulowanie, które przewiduje niewymagające uzasadnienia, kompletne i niezróżnicowane pod względem osobowym, czasowym i geograficznym przechowywanie znacznej części wszystkich istotnych danych o ruchu telekomunikacyjnym.

16 Jednakże mimo wywodów przedstawionych w wyroku Tele2 Sverige i Watson i in. sąd odsyłający nie wyklucza, że obowiązek niewymagającego uzasadnienia zatrzymywania danych o ruchu telekomunikacyjnym przewidziany w § 113a ust. 1 zdanie pierwsze w związku z § 113b TKG może zostać oparty na art. 15 ust. 1 dyrektywy 2002/58, i to z następujących powodów:

17 Po pierwsze, sporne przepisy TKG nie wymagają przechowywania wszystkich danych o ruchu telekomunikacyjnym wszystkich abonentów i zarejestrowanych użytkowników w odniesieniu do wszystkich środków łączności elektronicznej. Z obowiązku przechowywania jest wyłączona nie tylko treść komunikatów, ale

także nie mogą być przechowywane dane dotyczące przeglądanych stron internetowych, dane usług poczty elektronicznej oraz dane stanowiące podstawę połączeń do lub z niektórych linii w sferach społecznych lub religijnych (zob. § 113b ust. 5 i 6 TKG). O ile pewne środki łączności lub kategorie danych są wyłączone z obowiązku przechowywania, o tyle nie pozwala to wprawdzie na wyeliminowanie ryzyka sporządzenia kompletnego profilu pewnych osób, lecz może co najmniej ograniczyć w znaczący sposób to ryzyko.

18 Sąd odsyłający uważa, że jeszcze bardziej znacząca różnica między spornymi w niniejszej sprawie przepisami TKG i wcześniejszym uregulowaniem dyrektywy 2006/24 bądź opartymi na tej dyrektywie uregulowaniami szwedzkimi i brytyjskimi, które były przedmiotem wyroku Tele2 Sverige i Watson i in., polega po drugie na tym, że termin przechowywania wynoszących od sześciu miesięcy do dwóch lat (zob. art. 6 dyrektywy 2006/24) został zgodnie z § 113b ust. 1 TKG znacznie skrócony, odpowiednio, do czterech i dziesięciu tygodni.

19 Ryzyko sporządzenia kompletnego profilu pewnych osób należy uznać za o tyle mniejsze, im krótsze są okresy, w których są przechowywane dane o ruchu. Im krótszy jest okres przechowywania, tym bardziej niepełny będzie siłą rzeczy profil osobowościowy i tym mniejsza intensywność ingerencji w prawo podstawowe.

20 Po trzecie, sporne w niniejszej sprawie przepisy TKG podlegają surowym ograniczeniom w zakresie ochrony przechowywanych danych oraz dostępu do nich. Z jednej strony wymogi § 113d i nast. TKG gwarantują skuteczną ochronę zatrzymywanych danych przed ryzykiem nadużyć oraz przed każdym nieuprawnionym dostępem. Z drugiej strony zgodnie z § 113c ust. 1 TKG zatrzymywane dane mogą być wykorzystywane wyłącznie w celu zwalczania poważnych przestępstw lub zapobiegania konkretnemu zagrożeniu dla zdrowia, życia lub wolności osoby lub istnienia państwa federalnego lub kraju związkowego.

21 Gromadzenie danych o ruchu dla celów ścigania karnego zakłada zgodnie z § 100g ust. 2 StPO, że istnieje podejrzenie jednego ze szczególnie ciężkich przestępstw wymienionych enumeratywnie w ustawie, czyn ma szczególną wagę również w konkretnym przypadku, ustalenie stanu faktycznego lub określenie miejsca pobytu oskarżonego w inny sposób byłoby znacznie utrudnione lub bez szans na powodzenie oraz że gromadzenie danych jest proporcjonalne do znaczenia sprawy. Gromadzenie lub wykorzystywanie danych o ruchu osób zobowiązanych do zachowania tajemnicy zawodowej, o których mowa w § 53 ust. 1 zdanie drugie pkt 1–5 StPO, w tym na przykład adwokatów, lekarzy lub dziennikarzy, jest niedopuszczalne na podstawie § 100 g ust. 4 StPO. Paragraf 101a ust. 1 StPO przewiduje ponadto kompetencję decyzyjną sądu w zakresie gromadzenia danych o ruchu, o którym mowa w § 100 g StPO.

22 Prawdą jest, że te ograniczające uregulowania w zakresie dostępu nie mają zastosowania do adresu IP przypisanego abonentowi w celu korzystania z Internetu. Zgodnie bowiem z § 113c ust. 1 pkt 3 TKG może być on również

używany w ramach udzielania informacji o zgromadzonych danych w celu ścigania wszystkich przestępstw, zapobiegania zagrożeniom dla bezpieczeństwa i porządku publicznego oraz generalnie w celu wykonywania zadań służb wywiadowczych. Należy jednak przyjąć, że informacja na temat tego, który właściciel łącza był zalogowany w Internecie pod znanym już adresem IP, nie zezwala na sporządzanie profili osobowościowych i ruchomych.

23 Nawet gdyby zgodzić się z argumentacją spółki SpaceNet i przyjąć, że w coraz większej mierze zastosowanie mają procedury techniczne, w przypadku których adres IP nie może już jednoznacznie identyfikować danego połączenia telekomunikacyjnego, lecz jedynie większą grupę połączeń, i że w związku z tym instytucja udzielania informacji o zgromadzonych przybrała postać środka o bardzo szerokim zakresie, intensywność ingerencji takiej instytucji jest nadal znacznie mniejsza od tej, która ma miejsce przy uzyskiwaniu i wykorzystywaniu danych o ruchu telekomunikacyjnym.

24 Po czwarte, za uznaniem, że obowiązek niewymagającego uzasadnienia zatrzymywania danych o ruchu telekomunikacyjnym uregulowany w § 113a ust. 1 zdanie pierwsze w związku z § 113b TKG może zostać oparty na art. 15 ust. 1 dyrektywy 2002/58, przemawia również okoliczność, iż ustawodawca krajowy wypełnił w ten sposób obowiązki działania, które wynikają dla państw członkowskich z prawa do bezpieczeństwa zagwarantowanego w art. 6 karty. W wyroku Digital Rights Ireland i in. Trybunał wyraźnie wymienił art. 6 karty i wskazał w tym kontekście, że walka z międzynarodowym terroryzmem w celu utrzymania światowego pokoju i bezpieczeństwa międzynarodowego stanowi cel leżący w ogólnym interesie Unii i że to samo dotyczy walki z poważną przestępczością w celu zagwarantowania bezpieczeństwa publicznego.

25 W tym kontekście sąd odsyłający ma wątpliwości, czy dotychczasowe orzecznictwo Trybunału należy rozumieć w ten sposób, że niewymagające uzasadnienia zatrzymywanie danych nie tylko w konkretnej postaci, jaką przybrało ono w dyrektywie 2006/24 oraz w opartych na niej uregulowaniach szwedzkich i brytyjskich, ale również ogólnie nie może zostać na art. 15 ust. 1 dyrektywie 2002/58. Podstawowej koncepcji zatrzymywania danych nie da się bowiem pogodzić ze sformułowanym bez ograniczeń żądaniem Trybunału, by dane podlegające zatrzymywaniu były różnicowane według osób, okresów i obszarów geograficznych.

26 Z punktu widzenia sądu odsyłającego przeciwko uznaniu, że niepodlegające uzasadnieniu zatrzymywanie danych o ruchu jest sprzeczne *per se* z kartą, przemawia również wymóg zachowania równowagi pomiędzy, z jednej strony, obowiązkiem państw członkowskich polegającym na zapewnieniu bezpieczeństwa osób przebywających na ich terytorium, a z drugiej strony poszanowaniem praw podstawowych ustanowionych w art. 7 i 8 karty.

27 Sąd odsyłający nie jest zatem w stanie wywieść w sposób jednoznaczny z orzecznictwa Trybunału, że ustawodawcy krajowi nie mają już możliwości

wprowadzenia na podstawie całościowej oceny niewymagającego uzasadnienia zatrzymywania danych, w razie potrzeby uzupełnionego surowymi uregulowaniami w zakresie dostępu, w celu uwzględnienia szczególnego potencjału zagrożeń, który wiąże się z nowymi środkami telekomunikacji.

28 Po piąte, sąd odsyłający zwraca uwagę, że w sytuacji, w której niewymagające uzasadnienia zatrzymywanie danych generalnie nie może zostać oparte na art. 15 ust. 1 dyrektywy 2002/58 i że w związku z tym konkretne przepisy dotyczące odnośnych środków łączności, kategorii danych, które mają być zatrzymywane, okresu przechowywania, warunków dostępu do przechowywanych danych oraz ochrony przed ryzykiem nadużyć nie mają znaczenia, swoboda działania ustawodawcy krajowego w dziedzinie ścigania karnego i bezpieczeństwa publicznego, która zgodnie z art. 4 ust. 2 zdanie drugie TUE w każdym razie należy nadal co do zasady do wyłącznej odpowiedzialności każdego państwa członkowskiego, byłaby znacznie ograniczona.

29 Wreszcie po szóste, dla sądu odsyłającego nie jest jasne w kontekście niedawnego orzecznictwa Europejskiego Trybunału Praw Człowieka (zwanego dalej „ETPC”), czy wywody Trybunału zawarte w wyroku Tele2 Sverige i Watson i in. należy rozumieć jako skierowany do państw członkowskich zakaz oparcia wprowadzenia obowiązku zatrzymywania danych o ruchu telekomunikacyjnym na art. 15 ust. 1 dyrektywy 2002/58.

30 ETPC orzekł ostatnio w wyroku z dnia 19 czerwca 2018 r., że szwedzkie przepisy prawne dotyczące masowego nadzoru nad transgranicznym ruchem danych są zgodne z art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności (EKPC). Zważywszy na zagrożenia, na które państwa są obecnie narażone, w tym plaga globalnego terroryzmu i inne ciężkie przestępstwa, takie jak handel narkotykami, handel ludźmi, seksualne wykorzystywanie dzieci i przestępczość internetowa, jak również z powodu postępu technicznego, który ułatwia terrorystom i przestępcom uniknięcie ich wykrycia w Internecie, oraz z uwagi na nieprzewidywalność dróg przekazywania danych elektronicznych decyzja o ustanowieniu masowego systemu nadzoru w celu rozpoznania nieznanych dotychczas zagrożeń dla bezpieczeństwa narodowego należy nadal do zakresu uznania przysługującego państwu [wyrok ETPC z dnia 19 czerwca 2018 r., nr 35252/08 (ECLI:CE:ECHR:2018:0619JUD003525208), Centrum för Rättvisa/Szwecja, pkt 112]. W zakresie, w jakim ETPC wskazuje na nieprzewidywalność dróg przekazywania danych elektronicznych, jak również postęp techniczny, który ułatwia terrorystom i przestępcom unikanie ich wykrycia w Internecie, podkreśla on mocniej niż Trybunał Sprawiedliwości Unii Europejskiej szczególny potencjał zagrożeń, który wiąże się z nowymi środkami telekomunikacji.

31 Sąd odsyłający wskazuje na motyw 11 dyrektywy 2002/58 i art. 52 ust. 3 karty, z których wynika, że konieczna spójność między prawami ustanowionymi w karcie i odpowiadającymi im prawami zagwarantowanymi w EKPC powinna

być wprowadzona w życie bez naruszenia autonomii prawa Unii i Trybunału Sprawiedliwości Unii Europejskiej.

32 Na koniec sąd odsyłający przywołuje inne toczące się postępowania prejudycjalne dotyczące interpretacji wyroku Tele2 Sverige i Watson i in., a więc tego, czy wynika z niego generalny zakaz niewymagającego uzasadnienia zatrzymywania danych, którego to zakazu nie można łamać ani ze względu na znaczenie zagrożeń dla bezpieczeństwa publicznego, które mają być zwalczane, ani w ramach „kompensacji" przez restrykcyjne uregulowania w zakresie dostępu do danych oraz wysokie wymogi bezpieczeństwa.

33 Wymienione zostały wnioski o wydanie orzeczenia w trybie prejudycjalnym złożone przez Investigatory Powers Tribunal – London (Zjednoczone Królestwo) (C-623/17), wnioski o wydanie orzeczenia w trybie prejudycjalnym złożone przez Conseil d'État (Francja) (C-511/18 i C-512/18) oraz wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez belgijski trybunał konstytucyjny (C-520/18).