Zbiór Orzeczeń

WYROK TRYBUNAŁU (wielka izba)

z dnia 5 kwietnia 2022 r.*

Odesłanie prejudycjalne – Przetwarzanie danych osobowych w sektorze łączności elektronicznej – Poufność komunikacji – Dostawcy usług łączności elektronicznej – Uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji – Dostęp do zatrzymanych danych – Następcza kontrola sądowa – Dyrektywa 2002/58/WE – Artykuł 15 ust. 1 – Karta praw podstawowych Unii Europejskiej – Artykuły 7, 8 i 11 oraz art. 52 ust. 1 – Możliwość ograniczenia przez sąd krajowy skutków w czasie stwierdzenia nieważności dotyczącego uregulowania krajowego niezgodnego z prawem Unii – Wyłączenie

W sprawie C-140/20

mającej za przedmiot wniosek o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożony przez Supreme Court (sąd najwyższy, Irlandia) postanowieniem z dnia 25 marca 2020 r., które wpłynęło do Trybunału w tym samym dniu, w postępowaniu:

G.D.

przeciwko

Commissioner of An Garda Síochána,

Minister for Communications, Energy and Natural Resources,

Attorney General,

TRYBUNAŁ (wielka izba),

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

rzecznik generalny: M. Campos Sánchez-Bordona,

sekretarz: D. Dittert, kierownik wydziału,

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

* Język postępowania: angielski.

rozważywszy uwagi, które przedstawili:

– w imieniu G.D. – J. Dunphy, solicitor, R. Kennedy i R. Farrell, SC, oraz K. McCormack, BL,

– w imieniu Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources oraz Attorney General – M. Browne, S. Purcell, C. Stone, J. Quaney i A. Joyce, w charakterze pełnomocników, których wspierali S. Guerin i P. Gallagher, SC, oraz D. Fennelly i L. Dwyer, BL,

– w imieniu rządu belgijskiego – P. Cottin i J.C. Halleux, w charakterze pełnomocników, których wspierał J. Vanpraet, advocaat,

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

– w imieniu rządu duńskiego – początkowo J. Nymann-Lindegren, M. Jespersen i M. Wolff, a następnie M. Wolff i V. Jørgensen, w charakterze pełnomocników,

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

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

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

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

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

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

– w imieniu rządu portugalskiego – L. Inez Fernandes, P. Barros da Costa i I. Oliveira, w charakterze pełnomocników,

– w imieniu rządu fińskiego – M. Pere i A. Laine, w charakterze pełnomocników,

– w imieniu rządu szwedzkiego – O. Simonsson, J. Lundberg, H. Shev, C. Meyer-Seitz, A. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson i H. Eklinder, w charakterze pełnomocników,

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

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

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

wydaje następujący

Wyrok

1 Wniosek o wydanie orzeczenia w trybie prejudycjalnym dotyczy 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 (dyrektywy 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 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą").

2 Wniosek ten został przedstawiony w ramach sporu między G.D. a Commissioner of An Garda Síochána (szefem policji krajowej, Irlandia), Minister for Communications, Energy and Natural Resources (ministrem łączności, energetyki i zasobów naturalnych, Irlandia) oraz Attorney General (prokuratorem generalnym, Irlandia) w przedmiocie ważności Communications (Retention of Data) Act 2011 [ustawy z 2011 r. o łączności (zatrzymywanie danych)], zwanej dalej „ustawą z 2011 r."].

Ramy prawne

Prawo Unii

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

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

[…]

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

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

[…]

(11) Niniejsza dyrektywa, podobnie jak dyrektywa 95/46/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 [Unii]. Dyrektywa nie zmienia zatem istniejącej równowagi między prawem do prywatności osoby fizycznej a możliwością państw

członkowskich do podejmowania środków określonych w art. 15 ust. 1 niniejszej dyrektywy, niezbędnych do ochrony bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając gospodarczy dobrobyt państwa, gdy działania dotyczą zagadnień bezpieczeństwa państwa) i wykonywania prawa karnego. Wskutek tego niniejsza dyrektywa nie wpływa na możliwości państw członkowskich do zgodnego z prawem przejmowania danych w łączności elektronicznej lub podejmowania innych środków, jeżeli jest to konieczne dla któregokolwiek z tych celów i zgodne z europejską Konwencją o ochronie praw człowieka i podstawowych wolności [podpisaną w Rzymie dnia 4 listopada 1950 r.], dla której wykładnię stanowi orzecznictwo Europejskiego Trybunału Praw Człowieka. Środki tego rodzaju muszą być właściwe, [ściśle] 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".

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

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

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

3. Niniejsza dyrektywa nie ma zastosowania do działalności, która wykracza poza zakres [traktatu FUE], 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. 2002, L 108, s. 33)].

Stosuje się również następujące definicje:

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

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

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

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

[…]”.

6 Artykuł 3 dyrektywy 2002/58, zatytułowany „Usługi”, przewiduje:

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

7 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 [chyba że osoby te są do tego upoważnione przez prawo zgodnie 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 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”.

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

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

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

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

[…]

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

[…]”.

9 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 […]”.

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

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

Prawo irlandzkie

11 Jak wynika z wniosku o wydanie orzeczenia w trybie prejudycjalnym, ustawa z 2011 r. została wydana, aby przetransponować do irlandzkiego porządku prawnego dyrektywę 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 zmieniającą dyrektywę 2002/58/WE (Dz.U. 2006, L 105, s. 54).

12 Artykuł 1 ustawy z 2011 r. definiuje termin „dane" jako oznaczający „dane o ruchu i lokalizacji oraz powiązane dane niezbędne do identyfikacji abonenta lub użytkownika", zaś termin „poważne przestępstwo" jako oznaczający przestępstwo zagrożone karą co najmniej 5 lat pozbawienia wolności lub jedno z innych przestępstw wymienionych w załączniku 1 do tej ustawy.

13 Artykuł 3 ust. 1 owej ustawy nakłada na wszystkich dostawców usług łączności elektronicznej obowiązek zatrzymywania danych, o których mowa w części 1 załącznika 2 do tej ustawy, przez okres dwóch lat, oraz danych, o których mowa w części 2 tego załącznika 2, przez okres jednego roku.

14 Część 1 załącznika 2 do omawianej ustawy odnosi się między innymi do danych dotyczących telefonii stacjonarnej i telefonii ruchomej pozwalających zidentyfikować źródło i odbiorcę połączenia, ustalić datę i godzinę rozpoczęcia oraz zakończenia połączenia, ustalić rodzaj danego połączenia oraz zidentyfikować rodzaj i położenie geograficzne wykorzystanych urządzeń komunikacyjnych. W szczególności pkt 6 części 1 tego załącznika 2 przewiduje zatrzymywanie danych koniecznych do zlokalizowania środka ruchomej łączności elektronicznej, przy czym danymi tymi są, po pierwsze, identyfikator komórki, a po drugie, dane pozwalające ustalić położenie geograficzne komórek poprzez odniesienie się do ich etykiet lokalizacji (identyfikatorów komórki) przez okres, w którym są zatrzymywane dane dotyczące połączenia.

15 Część 2 załącznika 2 do ustawy z 2011 r. odnosi się do danych dotyczących dostępu do Internetu, poczty elektronicznej i telefonii internetowej oraz obejmuje między innymi numery identyfikatora i telefonu, adresy IP oraz datę i godzinę rozpoczęcia i zakończenia połączenia. Treść połączeń nie należy do tego rodzaju danych.

16 Na podstawie art. 4 i 5 ustawy z 2011 r. dostawcy usług łączności elektronicznej muszą podejmować określone środki, aby zapewnić ochronę danych przed nieupoważnionym do nich dostępem.

17 Artykuł 6 tej ustawy, który przewiduje warunki, w jakich można złożyć wniosek o udzielenie dostępu, stanowi w ust. 1:

„Funkcjonariusz policji krajowej, który ma co najmniej stopień nadinspektora, może zażądać od dostawy usług przekazania mu danych zatrzymanych przez tego dostawcę zgodnie z art. 3, jeżeli funkcjonariusz ten uzna, że określone dane są konieczne do celów:

(a) zapobiegania poważnym przestępstwom, ich wykrywania, dochodzenia lub ścigania,

(b) ochrony bezpieczeństwa państwa,

(c) ochrony życia ludzkiego".

18 Artykuł 7 wspomnianej ustawy nakłada na dostawców usług łączności elektronicznej obowiązek uwzględniania wniosków, o których mowa w art. 6 tej ustawy.

19 Do mechanizmów kontroli decyzji funkcjonariusza policji krajowej opisanej w art. 6 ustawy z 2011 r. należą postępowanie zażaleniowe przewidziane w art. 10 tej ustawy oraz postępowanie przed *designated judge* (wyznaczonym sędzią) w rozumieniu art. 12 owej ustawy, który jest odpowiedzialny za zbadanie zastosowania przepisów rzeczonej ustawy.

Postępowanie główne i pytania prejudycjalne

20 W marcu 2015 r. G.D. został skazany na karę dożywotniego pozbawienia wolności za zabójstwo osoby, która zaginęła w sierpniu 2012 r. i której zwłoki zostały znalezione dopiero we wrześniu 2013 r. W apelacji od wyroku skazującego zainteresowany zarzucił między innymi sądowi pierwszej instancji, że błędnie dopuścił jako dowody dane o ruchu i dane o lokalizacji dotyczące rozmów telefonicznych, uzasadniając to tym, że ustawa z 2011 r., która reguluje zatrzymywanie tych danych i na podstawie której śledczy policji krajowej uzyskali dostęp do owych danych, narusza prawa, jakie przyznaje mu prawo Unii. To postępowanie apelacyjne jest obecnie w toku.

21 Aby móc zakwestionować w ramach postępowania karnego dopuszczalność owych dowodów, G.D. wszczął przed High Court (wysokim trybunałem, Irlandia) postępowanie cywilne mające na celu stwierdzenie nieważności niektórych przepisów ustawy z 2011 r. Orzeczeniem z dnia 6 grudnia 2018 r. sąd ten uwzględnił argumentację G.D. i uznał, że art. 6 ust. 1 lit. a) tej ustawy jest niezgodny z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7 i 8 oraz art. 52 ust. 1 karty. Irlandia wniosła apelację od tego orzeczenia do Supreme Court (sądu najwyższego, Irlandia), będącego sądem odsyłającym.

22 Postępowanie karne zawisłe przed Court of Appeal (sądem apelacyjnym, Irlandia) zostało zawieszone do czasu wydania orzeczenia sądu odsyłającego w ramach głównego postępowania cywilnego.

23 Przed sądem odsyłającym Irlandia utrzymywała, że aby ustalić, czy ingerencja w prawo do poszanowania życia prywatnego zagwarantowane w art. 7 karty, wynikająca z zatrzymania danych o ruchu i danych o lokalizacji na podstawie ustawy z 2011 r., jest proporcjonalna, należy zbadać cele systemu ustanowionego przez tę ustawę rozpatrywanego całościowo. Ponadto zdaniem tego państwa członkowskiego omawiana ustawa ustanowiła szczegółowe ramy regulujące dostęp do zatrzymanych danych, na podstawie których jednostce odpowiedzialnej w policji krajowej za wstępne badanie wniosków o udzielenie dostępu przysługuje niezależność funkcjonalna w stosunku do policji krajowej w wykonywaniu jej zadań, w związku z czym spełnia ona wymóg uprzedniej kontroli sprawowanej przez niezależną jednostkę administracyjną. Ten system kontroli uzupełniają postępowanie zażaleniowe i kontrola sądowa. Wreszcie owo państwo członkowskie twierdzi, że gdyby ostatecznie zostało stwierdzone, iż ustawa z 2011 r. jest sprzeczna z prawem Unii, wszelkie stwierdzenia wywiedzione stąd przez sąd odsyłający powinny obowiązywać – z punktu widzenia ich skutków w czasie – na przyszłość.

24 Z kolei G.D. twierdził, że system uogólnionego i niezróżnicowanego zatrzymywania danych ustanowiony w ustawie z 2011 r. oraz system dostępu do tych danych przewidziany w tej ustawie są niezgodne z prawem Unii, tak jak zostało ono w szczególności zinterpretowane przez Trybunał w pkt 120 wyroku z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970).

25 Sąd odsyłający wyjaśnił tytułem wstępu, że do niego należy jedynie dokonanie oceny, czy High Court (wysoki trybunał) słusznie orzekł, że art. 6 ust. 1 lit. a) ustawy z 2011 r. jest niezgodny z prawem Unii, natomiast kwestia dopuszczalności dowodów przedstawionych w ramach procesu karnego należy do wyłącznej kompetencji Court of Appeal (sądu apelacyjnego), do którego została wniesiona apelacja od wyroku skazującego.

26 W tym kontekście sąd odsyłający zastanawia się przede wszystkim nad wymogami prawa Unii w odniesieniu do zatrzymywania danych w celu walki z poważną przestępczością. W tym względzie uważa on zasadniczo, że jedynie uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji pozwala walczyć w skuteczny sposób z poważną przestępczością, na co nie pozwalały indywidualne zatrzymywanie i szybkie zatrzymywanie (*quick freeze*). Jeśli chodzi o indywidualne zatrzymywanie, sąd odsyłający zastanawia się nad możliwością przyjęcia za cel określonych grup lub stref geograficznych do celów walki z poważną przestępczością, gdyż niektóre poważne przestępstwa rzadko wiążą się z okolicznościami znanymi właściwym organom krajowym, pozwalającym im podejrzewać popełnienie przestępstwa przed jego popełnieniem. Ponadto indywidualne zatrzymywanie może prowadzić do dyskryminacji. Jeśli chodzi o szybkie zatrzymywanie, sąd odsyłający uważa, że jest ono przydatne tylko w sytuacjach, gdy istnieje podejrzany, którego można zidentyfikować na wczesnym etapie dochodzenia.

27 Następnie w odniesieniu do dostępu do danych zatrzymywanych przez dostawców usług łączności elektronicznej sąd odsyłający podkreśla, że policja krajowa ustanowiła w ramach swojej struktury mechanizm autocertyfikacji wniosków o udzielenie dostępu kierowanych do tych dostawców. I tak z dowodów przedłożonych przed High Court (wysokim trybunałem) wynika, że szef policji krajowej zdecydował – tytułem środka wewnętrznego – że wnioski o udzielenie dostępu złożone na podstawie ustawy z 2011 r. muszą być rozpatrywane w scentralizowany sposób przez tylko jednego funkcjonariusza policji krajowej, mającego status nadinspektora, czyli szefa wydziału ds. bezpieczeństwa i wywiadu. Jeżeli ten ostatni uważa, że określone dane są konieczne między innymi do celów zapobiegania poważnym przestępstwom, ich wykrywania, dochodzenia lub ścigania, może on skierować wniosek o udzielenie dostępu do dostawców usług łączności elektronicznej. Ponadto szef policji krajowej ustanowił w ramach jej struktury niezależną jednostkę zwaną *Telecommunications Liaison Unit* (jednostkę łącznikową w dziedzinie telekomunikacji, zwaną dalej „TLU"), aby zapewnić wsparcie szefowi wydziału ds. bezpieczeństwa i wywiadu w wykonywaniu jego funkcji oraz służyć jako jedyny punkt kontaktowy z tymi samymi dostawcami usług.

28 Sąd odsyłający dodaje, że w okresie objętym dochodzeniem karnym wszczętym przeciwko G.D. wszystkie wnioski o udzielenie dostępu musiały zostać zatwierdzone w pierwszej kolejności przez komisarza lub inspektora pełniącego obowiązki komisarza, zanim zostały one przesłane TLU w celu ich rozpatrzenia, oraz że śledczy zostali wezwani do opatrywania swoich wniosków o udzielenie dostępu wystarczająco szczegółowymi informacjami, aby mogła zostać podjęta świadoma decyzja. Co więcej, TLU i szef wydziału ds. bezpieczeństwa i wywiadu byli zobowiązani badać zgodność z prawem, konieczność i proporcjonalności wniosków o udzielenie dostępu, mając na uwadze okoliczność, że szef ten mógł zostać wezwany do odpowiedzialności za swoją decyzję przed sędzią wyznaczonym przez High Court (wysoki trybunał). Ponadto TLU podlega kontroli ze strony Data Protection Commissioner (komisarza ds. ochrony danych, Irlandia).

29 Wreszcie sąd odsyłający zastanawia się nad znaczeniem i skutkami w czasie ewentualnego stwierdzenia niezgodności ustawy z 2011 r. z prawem Unii. W tym względzie wyjaśnił on, że takie stwierdzenie może obowiązywać jedynie w stosunku do przyszłości, uzasadniając to tym, że dane wykorzystane jako dowody w postępowaniu karnym przeciwko G.D. były przedmiotem

zatrzymania i dostępu pod koniec roku 2013, czyli w okresie, w którym Irlandia była zobowiązana stosować przepisy ustawy z 2011 r., transponującej dyrektywę 2006/24. Zdaniem Irlandii takie rozwiązanie jest także odpowiednie, gdyż jego brak mógłby mieć istotny wpływ na dochodzenie i ściganie poważnych przestępstw w Irlandii oraz na sytuację osób już osądzonych i skazanych.

30 W tych okolicznościach Supreme Court (sąd najwyższy) postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„1) Czy ogólny lub powszechny system zatrzymywania danych – nawet poddany rygorystycznym ograniczeniom w zakresie zatrzymywania i dostępu – jest sam w sobie sprzeczny z art. 15 dyrektywy [2002/58], interpretowanym w świetle karty?

2) Czy przy badaniu ewentualnej niezgodności środka krajowego wprowadzonego na podstawie dyrektywy [2006/24], wprowadzającego ogólny system zatrzymywania danych (z zastrzeżeniem niezbędnych rygorystycznych kontroli w zakresie zatrzymywania danych lub uzyskiwania do nich dostępu), w szczególności przy ocenie proporcjonalności takiego systemu, sąd krajowy może uwzględnić okoliczność, że dane mogą być zgodnie z prawem zatrzymywane przez usługodawców do własnych celów handlowych oraz że ich zatrzymanie może być wymagane ze względów bezpieczeństwa narodowego wyłączonych z przepisów dyrektywy [2002/58]?

3) Dokonując oceny, w kontekście stwierdzenia zgodności z prawem Unii, w szczególności z kartą, krajowego środka dostępu do zatrzymanych danych, jakimi kryteriami powinien kierować się sąd krajowy, badając, czy tego rodzaju system dostępu przewiduje uprzednią i niezależną kontrolę wymaganą przez Trybunał Sprawiedliwości w jego orzecznictwie? Czy w tym kontekście sąd krajowy może, przy dokonywaniu takiej oceny, wziąć pod uwagę istnienie kontroli sądowej ex post lub niezależnej kontroli?

4) W każdym wypadku: czy sąd krajowy jest zobowiązany do stwierdzenia niezgodności środka krajowego z art. 15 dyrektywy [2002/58], jeżeli środek krajowy przewiduje ogólny system zatrzymywania danych na potrzeby zwalczania poważnych przestępstw, a sąd krajowy uznał – na podstawie wszystkich dostępnych dowodów – że takie zatrzymywanie jest zarazem istotne i ściśle niezbędne do realizacji celu polegającego na zwalczaniu poważnej przestępczości?

5) Jeżeli sąd krajowy jest zobowiązany uznać, że środek krajowy jest niezgodny z art. 15 dyrektywy 2002/58, interpretowanym w świetle karty, to czy jest on uprawniony do ograniczenia w czasie skutków takiego uznania, jeśli jest przekonany o tym, że przyjęcie odmiennego podejścia doprowadziłoby do »chaosu i uszczerbku dla interesu ogółu« [zgodnie ze stanowiskiem przyjętym na przykład w sprawie R (National Council for Civil Liberties) przeciwko Secretary of State for Home Department i Secretary of State for Foreign Affairs (2018) EWHC 975, pkt 46]?

6) Czy sąd krajowy, do którego zwrócono się o stwierdzenie niezgodności prawa krajowego z art. 15 dyrektywy 2002/58 lub o odstąpienie od jego stosowania, lub o stwierdzenie, że stosowanie takiego prawa skutkowało naruszeniem praw jednostki, czy to w ramach postępowania wszczętego w celu ułatwienia polemiki w przedmiocie dopuszczalności dowodów w ramach postępowania karnego, czy w innym celu, może odmówić zastosowania takiego rozwiązania w odniesieniu do danych zatrzymanych na mocy przepisu krajowego ustanowionego na podstawie wynikającego z art. 288 TFUE obowiązku skutecznego

wprowadzenia do prawa krajowego przepisów dyrektywy lub ograniczyć takie stwierdzenie do okresu następującego po stwierdzeniu nieważności dyrektywy 2006/24 [w wyroku z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in. (C-293/12 i C-594/12, EU:C:2014:238]?".

W przedmiocie pytań prejudycjalnych

W przedmiocie pytań pierwszego, drugiego i czwartego

31 Za pomocą pytań pierwszego, drugiego i czwartego, które należy zbadać łącznie, sąd krajowy chce się zasadniczo dowiedzieć, czy 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, że stoi on na przeszkodzie uregulowaniu krajowemu przewidującemu do celów zwalczania poważnej przestępczości uogólnione i niezróżnicowane zatrzymywanie danych o ruchu oraz danych dotyczących lokalizacji.

32 Tytułem wstępu należy przypomnieć, że zgodnie z utrwalonym orzecznictwem przy dokonywaniu wykładni przepisu prawa Unii należy uwzględniać nie tylko jego brzmienie, lecz także jego kontekst oraz cele aktu prawnego, którego jest on częścią, oraz w szczególności genezę tego uregulowania (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 105 i przytoczone tam orzecznictwo).

33 Z samego brzmienia art. 15 ust. 1 dyrektywy 2002/58 wynika, że środki ustawodawcze, do których przyjmowania upoważnia państwa członkowskie ta dyrektywa na określonych w niej warunkach, mogą mieć jedynie na celu „ograniczeni[e] zakresu" praw i obowiązków przewidzianych między innymi w art. 5, 6 i 9 dyrektywy 2002/58.

34 W odniesieniu do systemu ustanowionego przez tę dyrektywę, w jaki wpisuje się także art. 15 ust. 1 tej dyrektywy, należy przypomnieć, że na podstawie art. 5 ust. 1 zdania pierwsze i drugie wspomnianej dyrektywy państwa członkowskie są zobowiązane zapewnić, poprzez ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. W szczególności ciąży na nich zobowiązanie do zakazania słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy bez zgody zainteresowanych użytkowników, chyba że osoby te są do tego upoważnione przez prawo zgodnie z art. 15 ust. 1 tej samej dyrektywy.

35 W tym względzie Trybunał orzekł już, że w art. 5 ust. 1 dyrektywy 2002/58 ustanowiono zasadę poufności zarówno łączności elektronicznej, jak i związanych z nią danych o ruchu, co oznacza w szczególności zakaz – nałożony co do zasady na każdą osobę inną niż użytkownicy – przechowywania tych komunikatów i tych danych bez ich zgody (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 107).

36 Przepis ten odzwierciedla cel, który przyświecał prawodawcy Unii przy wydawaniu dyrektywy 2002/58. Z uzasadnienia wniosku odnoszącego się do dyrektywy Parlamentu Europejskiego i Rady dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej [COM(2000) 385 wersja ostateczna], leżącego u podstaw dyrektywy 2002/58, wynika bowiem, że prawodawca Unii zamierzał „zapewnić, aby wysoki poziom ochrony danych osobowych i życia prywatnego był nadal zagwarantowany w odniesieniu do wszystkich usług łączności elektronicznej, bez względu na zastosowaną technologię". Wspomniana dyrektywa ma zatem na celu, jak wynika w szczególności z jej motywów 6 i 7, ochronę użytkowników usług

łączności elektronicznej przed zagrożeniami wynikającymi dla ich danych osobowych i ich życia prywatnego z nowych technologii, a w szczególności ze zwiększonej zdolności do automatycznego przechowywania i przetwarzania danych. W szczególności, jak wskazuje motyw 2 tej dyrektywy, wolą prawodawcy Unii jest zapewnienie pełnego poszanowania praw określonych w art. 7 i 8 karty (zob. podobnie wyroki: z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970, pkt 83; a także z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 106).

37 Przyjmując dyrektywę 2002/58, prawodawca Unii skonkretyzował zatem te prawa w taki sposób, że użytkownicy środków łączności elektronicznej mają prawo co do zasady oczekiwać, że ich komunikacja i związane z nią dane pozostaną anonimowe i nie będą mogły być rejestrowane bez ich zgody (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 109).

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

39 Wobec tego dyrektywa 2002/58 nie ogranicza się do określenia ram dostępu do takich danych za pomocą gwarancji mających na celu zapobieganie nadużyciom, ale także ustanawia w szczególności zasadę zakazu ich przechowywania przez osoby trzecie.

40 W zakresie, w jakim art. 15 ust. 1 dyrektywy 2002/58 pozwala państwom członkowskim przyjmować środki ustawodawcze mające na celu „ograniczeni[e] zakresu" praw i obowiązków przewidzianych w szczególności w art. 5, 6 i 9 tej dyrektywy, wynikających z zasad poufności komunikacji i zakazu przechowania związanych z nią danych, przypomnianych w pkt 35 niniejszego wyroku, przepis ten ustanawia wyjątek od ogólnej reguły przewidzianej w szczególności w tych art. 5, 6 i 9 i powinien zatem – zgodnie z utrwalonym orzecznictwem – być ściśle interpretowany. Taki przepis nie może zatem uzasadniać tego, że odstępstwo od obowiązku zapewnienia poufności łączności elektronicznej i danych z nią związanych, a w szczególności od zakazu przechowywania tych danych, przewidzianego w art. 5 wspomnianej dyrektywy, stanie się regułą, gdyż pozbawiłoby to w znacznym stopniu ten przepis jego znaczenia (zob. podobnie wyroki: z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970, pkt 89; a także z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 111).

41 Jeśli chodzi o cele, które mogą uzasadniać ograniczenie praw i obowiązków przewidzianych w szczególności w art. 5, 6 i 9 dyrektywy 2002/58, Trybunał orzekł już, że wyliczenie celów dokonane w art. 15 ust. 1 zdanie pierwsze tej dyrektywy ma charakter wyczerpujący, wobec czego środek ustawodawczy przyjęty na podstawie tego przepisu powinien odpowiadać rzeczywiście i ściśle jednemu z tych celów (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 112 i przytoczone tam orzecznictwo).

42 Ponadto z art. 15 ust. 1 zdanie trzecie dyrektywy 2002/58 wynika, że środki ustawodawcze przyjmowane przez państwa członkowskie na podstawie tego przepisu muszą przestrzegać zasad ogólnych prawa Unii, do których należy zasada proporcjonalności, i zapewniać poszanowanie praw podstawowych gwarantowanych w karcie. W tym względzie Trybunał orzekł już, że nałożony przez państwo członkowskie na dostawców usług łączności elektronicznej w przepisach krajowych obowiązek zatrzymywania danych o ruchu w celu udzielenia właściwym organom krajowym dostępu do nich w razie potrzeby budzi wątpliwości co do zgodności nie tylko z art. 7 i 8 karty, dotyczącymi, odpowiednio, ochrony życia prywatnego oraz ochrony danych osobowych, lecz również z art. 11 karty, dotyczącym wolności wypowiedzi (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 113 i przytoczone tam orzecznictwo).

43 Tak więc przy wykładni art. 15 ust. 1 dyrektywy 2002/58 należy uwzględnić wagę zarówno prawa do poszanowania życia prywatnego, gwarantowanego w art. 7 karty, jak i prawa do ochrony danych osobowych, gwarantowanego w art. 8 karty, w postaci wynikającej z orzecznictwa Trybunału, a także prawa do wolności wypowiedzi, ponieważ to prawo podstawowe, zagwarantowane w art. 11 karty, stanowi jeden z istotnych fundamentów demokratycznego i pluralistycznego społeczeństwa, stanowiąc część wartości, na jakich zgodnie z art. 2 TUE opiera się Unia (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 114 i przytoczone tam orzecznictwo).

44 Należy uściślić w tym względzie, że zatrzymywanie danych o ruchu i danych o lokalizacji stanowi samo w sobie z jednej strony odstępstwo od przewidzianego w art. 5 ust. 1 dyrektywy 2002/58 zakazu przechowywania tych danych przez inne osoby niż użytkownicy, a z drugiej strony ingerencję w prawa podstawowe do poszanowania życia prywatnego i do ochrony danych osobowych, o których mowa w art. 7 i 8 karty, bez względu na to, czy rozpatrywane informacje dotyczące życia prywatnego są danymi szczególnie chronionymi, czy nie, ani czy osoby, których dane dotyczą, ucierpiały z powodu ewentualnych niedogodności wynikających z tej ingerencji, jak również bez względu na to, czy zatrzymane dane są następnie wykorzystywane (zob. podobnie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 115, 116 i przytoczone tam orzecznictwo).

45 Wniosek ten jest tym bardziej uzasadniony, że dane o ruchu i dane o lokalizacji mogą ujawnić informacje o wielu aspektach życia prywatnego osób, których dane dotyczą, w tym informacje newralgiczne, takie jak orientacja seksualna, poglądy polityczne, przekonania religijne, filozoficzne, społeczne lub inne, jak również stan zdrowia, podczas gdy takie dane korzystają ponadto ze szczególnej ochrony w prawie Unii. Całokształt omawianych danych umożliwia wyciągnięcie bardzo precyzyjnych wniosków dotyczących życia prywatnego osób, których dane są zatrzymywane, takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazyjnie pokonywane trasy, prowadzona działalność, relacje towarzyskie tych osób i środowiska społeczne, w których osoby te się obracają. W szczególności dane te dają możność ustalenia profilu danych osób, która to informacja jest z punktu widzenia prawa do poszanowania życia prywatnego równie newralgiczna co sama treść komunikatów (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 117 i przytoczone tam orzecznictwo).

46 W związku z tym, po pierwsze, zatrzymywanie danych o ruchu i danych o lokalizacji w celach policyjnych może samo w sobie naruszać prawo do poszanowania komunikowania się, ustanowione w art. 7 karty, i wpłynąć zniechęcająco na wykonywanie przez użytkowników środków łączności elektronicznej ich wolności wypowiedzi zagwarantowanej w jej art. 11, zaś

skutki te są tym dotkliwsze, że zatrzymywane dane są bardzo obszerne i zróżnicowane. Po drugie, biorąc pod uwagę okoliczność, że znaczna liczba danych o ruchu i danych o lokalizacji może być zatrzymywana w sposób ciągły przy użyciu środka uogólnionego i niezróżnicowanego zatrzymywania oraz że informacje wynikające z tych danych są szczególnie chronione, samo zatrzymywanie omawianych danych przez dostawców usług łączności elektronicznej grozi nadużyciem i nieuprawnionym dostępem (zob. podobnie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 118, 119 i przytoczone tam orzecznictwo).

47 W tym względzie należy podkreślić, że zatrzymywanie tych danych i dostęp do nich stanowią – jak wynika z orzecznictwa przypomnianego w pkt 44 niniejszego wyroku – odrębne ingerencje w prawa podstawowe zagwarantowane w art. 7 i 11 karty, wymagające odrębnego uzasadnienia na podstawie art. 52 ust. 1 tej karty. Wynika stąd, że przepisy krajowe zapewniające pełne poszanowanie warunków wynikających z orzecznictwa, w którym dokonano wykładni dyrektywy 2002/58 w dziedzinie dostępu do zatrzymanych danych, nie mogą jako takie ani ograniczyć, ani zaradzić poważnej ingerencji, która wynikałaby z uogólnionego zatrzymywania tych danych przewidzianego w tych przepisach krajowych, w prawa zagwarantowane w art. 5 i 6 tej dyrektywy oraz przez prawa podstawowe, których te artykuły stanowią konkretyzację.

48 Niemniej jednak w zakresie, w jakim art. 15 ust. 1 dyrektywy 2002/58 pozwala państwom członkowskim na ograniczenie praw i obowiązków, o których mowa w pkt 34–37 niniejszego wyroku, odzwierciedla on okoliczność, że prawa ustanowione w art. 7, 8 i 11 karty nie wydają się stanowić prerogatyw o charakterze absolutnym, lecz należy je rozważać z uwzględnieniem ich funkcji społecznej. Jak bowiem wynika z art. 52 ust. 1 karty, dopuszcza ona ograniczenia wykonywania tych praw, o ile ograniczenia te są przewidziane ustawą, szanują istotę omawianych praw oraz – z zastrzeżeniem zasady proporcjonalności – są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. A zatem wykładnia art. 15 ust. 1 dyrektywy 2002/58 w świetle karty wymaga uwzględnienia również znaczenia praw ustanowionych w art. 3, 4, 6 i 7 karty oraz znaczenia, jakie mają cele ochrony bezpieczeństwa narodowego i walki z poważną przestępczością, przyczyniające się do ochrony praw i wolności innych osób (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 120–122 i przytoczone tam orzecznictwo).

49 Natomiast jeśli chodzi w szczególności o skuteczną walkę z przestępstwami, których ofiarami są zwłaszcza małoletni i inne osoby podatne na zagrożenia, należy uwzględnić okoliczność, że z art. 7 karty mogą wynikać pozytywne obowiązki przyjęcia przez organy publiczne środków prawnych w celu ochrony życia prywatnego i rodzinnego. Takie obowiązki mogą również wynikać ze wspomnianego art. 7 w zakresie ochrony domu i komunikowania się, a także z art. 3 i 4 w odniesieniu do ochrony integralności fizycznej i psychicznej osób, jak również zakazu tortur i nieludzkiego lub poniżającego traktowania (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 126 i przytoczone tam orzecznictwo).

50 W obliczu tych różnych pozytywnych obowiązków należy zatem pogodzić ze sobą różne wchodzące w rachubę uzasadnione interesy i prawa. Europejski Trybunał Praw Człowieka orzekł bowiem, że pozytywne obowiązki wynikające z art. 3 i 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, którym odpowiadają gwarancje zawarte w art. 4 i 7 karty, oznaczają w szczególności przyjęcie przepisów materialnych i proceduralnych oraz środków praktycznych pozwalających na skuteczne zwalczanie przestępstw przeciwko osobom w drodze

skutecznego dochodzenia i ścigania, przy czym obowiązek ten jest tym ważniejszy, gdy zagrożony jest fizyczny i psychiczny dobrostan dziecka. Jednakże środki, których podjęcie należy do właściwych organów, muszą być w pełni zgodne z możliwościami ochrony prawnej i innymi gwarancjami, które mogą ograniczać zakres uprawnień dochodzeniowych w sprawach karnych, oraz z innymi wolnościami i prawami. W szczególności zdaniem tego sądu należy ustanowić ramy prawne pozwalające pogodzić różne uzasadnione interesy i prawa podlegające ochronie (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 127, 128 i przytoczone tam orzecznictwo).

51 W tych ramach z samego brzmienia art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 wynika, że państwa członkowskie mogą uchwalić środek stanowiący odstępstwo od zasady poufności komunikacji wspomnianej w pkt 35 niniejszego wyroku, gdy taki środek jest „niezbędny, właściwy i proporcjonalny w ramach społeczeństwa demokratycznego", gdyż motyw 11 tej dyrektywy wskazuje w tym celu, iż środek tego rodzaju musi być „ściśle" proporcjonalny do zamierzonego celu (zob. podobnie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 129).

52 W tym względzie należy przypomnieć, że ochrona prawa podstawowego do poszanowania życia prywatnego zgodnie z utrwalonym orzecznictwem Trybunału wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia mieściły się w ramach tego, co ściśle niezbędne. Ponadto nie można dążyć do celu interesu ogólnego bez uwzględnienia okoliczności, że należy pogodzić go z prawami podstawowymi, których dotyczy środek, dokonując zbilansowanego wyważenia między celem interesu ogólnego z jednej strony a rozpatrywanymi prawami z drugiej strony (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 130 i przytoczone tam orzecznictwo).

53 Konkretniej rzecz ujmując, z orzecznictwa Trybunału wynika, że możliwość uzasadnienia przez państwa członkowskie ograniczenia praw i obowiązków przewidzianych w szczególności w art. 5, 6 i 9 dyrektywy 2002/58 należy oceniać poprzez przeprowadzenie badania wagi ingerencji, jaką stanowi takie ograniczenie, oraz sprawdzenie, czy znaczenie celu interesu ogólnego, do którego zmierza to ograniczenie, pozostaje w relacji do tej wagi (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 131 i przytoczone tam orzecznictwo).

54 Aby spełniać wymóg proporcjonalności, uregulowanie krajowe musi zawierać jasne i precyzyjne przepisy regulujące zakres i sposób stosowania rozpatrywanego środka oraz ustanawiające minimalne wymogi służące temu, aby osoby, o których dane osobowe chodzi, miały wystarczające gwarancje pozwalające na skuteczną ochronę tych danych przed ryzykiem nadużyć. Uregulowanie to musi być prawnie wiążące w prawie wewnętrznym i w szczególności wskazywać, w jakich okolicznościach i pod jakimi warunkami można przyjąć środek przewidujący przetwarzanie takich danych, gwarantując w ten sposób, że ingerencja zostanie ograniczona do tego, co ściśle niezbędne. Konieczność dysponowania takimi gwarancjami jest jeszcze istotniejsza w sytuacji, gdy dane osobowe podlegają automatycznemu przetwarzaniu, w szczególności kiedy występuje znaczne ryzyko nieuprawnionego dostępu do tych danych. Rozważania te dotyczą zwłaszcza sytuacji, gdy w grę wchodzi ochrona tej szczególnej kategorii danych osobowych, jakimi są dane szczególnie chronione (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 132 i przytoczone tam orzecznictwo).

55 Zatem uregulowanie krajowe przewidujące zatrzymywanie danych osobowych powinno zawsze spełniać obiektywne kryteria wykazujące związek między danymi podlegającymi zatrzymaniu a zamierzonym celem. W szczególności w przypadku walki z poważną przestępczością dane, które mają być zatrzymywane, muszą być w stanie przyczynić się do zapobiegania poważnym przestępstwom oraz ich wykrywania lub ścigania (zob. podobnie wyroki: z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 59; a także z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 133).

56 Jeśli chodzi o cele interesu ogólnego mogące uzasadniać środek przyjęty na podstawie art. 15 ust. 1 dyrektywy 2002/58, z orzecznictwa Trybunału, w szczególności z wyroku z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791), wynika, że zgodnie z zasadą proporcjonalności istnieje hierarchia wśród tych celów w zależności od znaczenia każdego z nich oraz że znaczenie celu przyświecającego takiemu środkowi musi pozostawać w związku z wagą ingerencji, która z niego wynika.

57 W tym względzie Trybunał orzekł już, że znaczenie celu ochrony bezpieczeństwa narodowego, w świetle art. 4 ust. 2 TUE, zgodnie z którym ochrona bezpieczeństwa narodowego pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego, przewyższa znaczeniem inne cele, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, w szczególności cele zwalczania przestępstw w ogólności, choćby poważnych, a także ochrony bezpieczeństwa publicznego. Z zastrzeżeniem poszanowania innych wymogów przewidzianych w art. 52 ust. 1 karty cel ochrony bezpieczeństwa narodowego może więc uzasadniać środki związane z dalej idącą ingerencją w prawa podstawowe niż środki, które mogłyby być uzasadnione tymi innymi celami (zob. podobnie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 135, 136).

58 Z tego właśnie względu Trybunał stwierdził, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty nie stoi na przeszkodzie przepisom ustawodawczym umożliwiającym, w celu ochrony bezpieczeństwa narodowego, posłużenie się skierowanym do dostawców usług łączności elektronicznej nakazem uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji, w sytuacjach gdy dane państwo członkowskie napotyka poważne zagrożenie dla bezpieczeństwa narodowego, które okazuje się rzeczywiste i aktualne lub możliwe do przewidzenia, przy czym decyzja o wydaniu takiego nakazu może być przedmiotem skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja wywiera wiążący skutek, mającej na celu weryfikację występowania jednej z takich sytuacji oraz poszanowania warunków i gwarancji, które powinny zostać przewidziane, zaś wspomniany nakaz można wydać jedynie na określony czas, ograniczony do tego, co ściśle niezbędne, jednak z możliwością przedłużenia w przypadku utrzymywania się tego zagrożenia (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 168).

59 Jeśli chodzi o cel polegający na zapobieganiu przestępstwom, ich dochodzeniu, wykrywaniu i ściganiu, Trybunał zauważył, że zgodnie z zasadą proporcjonalności jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniom dla bezpieczeństwa publicznego mogą uzasadniać poważne ingerencje w prawa podstawowe ustanowione w art. 7 i 8 karty, takie jak te, które są związane z zatrzymywaniem danych o ruchu i danych o lokalizacji. A zatem jedynie takie ingerencje we wspomniane prawa podstawowe, które nie mają poważnego charakteru, mogą być

uzasadnione celem polegającym na zapobieganiu przestępstwom w ogólności, ich dochodzeniu, wykrywaniu i ściganiu (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 140 i przytoczone tam orzecznictwo).

60 Na rozprawie Komisja Europejska utrzymywała, że szczególnie poważna przestępczość może być utożsamiana z zagrożeniem dla bezpieczeństwa narodowego.

61 Tymczasem Trybunał orzekł już, że cel polegający na ochronie bezpieczeństwa narodowego odpowiada pierwszorzędnemu interesowi w ochronie podstawowych funkcji państwa i podstawowych interesów społeczeństwa poprzez zapobieganie i ściganie działalności mogącej poważnie zdestabilizować podstawowe struktury konstytucyjne, polityczne, ekonomiczne lub społeczne kraju, w szczególności bezpośrednio zagrozić społeczeństwu, ludności lub państwu jako takiemu, zwłaszcza takiej jak działalność terrorystyczna (zob. podobnie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 135).

62 Należy ponadto zauważyć, że w odróżnieniu od przestępczości, nawet szczególnie poważnej, zagrożenie dla bezpieczeństwa narodowego musi być rzeczywiste i aktualne lub przynajmniej przewidywalne, co zakłada wystąpienie wystarczająco konkretnych okoliczności, aby móc uzasadnić środek w postaci uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji przez określony czas. Takie zagrożenie różni się zatem – ze względu na swój charakter, wagę i szczególny charakter składających się na nie okoliczności – od ogólnego i stałego ryzyka, jakim jest ryzyko wystąpienia napięć lub zakłóceń, nawet poważnych, dla bezpieczeństwa publicznego lub ryzyko poważnych przestępstw (zob. podobnie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 136, 137).

63 A zatem przestępczości, nawet szczególnie poważnej, nie można utożsamiać z zagrożeniem dla bezpieczeństwa narodowego. Jak bowiem zauważył rzecznik generalny w pkt 49 i 50 opinii, takie utożsamienie mogłoby wprowadzić kategorię pośrednią między bezpieczeństwem narodowym a bezpieczeństwem publicznym w celu zastosowania do tego drugiego wymogów właściwych dla tego pierwszego.

64 Wynika stąd również, że wymieniona w drugim pytaniu prejudycjalnym okoliczność, iż dane o ruchu i dane dotyczące lokalizacji zostały zatrzymane zgodnie z prawem w celu ochrony bezpieczeństwa narodowego, nie ma wpływu na zgodność z prawem ich zatrzymania do celów zwalczania poważnej przestępczości.

65 W odniesieniu do celu polegającego na zwalczaniu poważnej przestępczości Trybunał orzekł już, że uregulowanie krajowe przewidujące w związku z tym uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji wykracza poza granice tego, co absolutnie niezbędne, i nie może być uważane za uzasadnione w społeczeństwie demokratycznym. Z uwagi bowiem na to, że informacje mogące wynikać z danych o ruchu i danych o lokalizacji są szczególnie chronione, ich poufność ma zasadnicze znaczenie dla prawa do poszanowania życia prywatnego. A zatem, z uwagi na, po pierwsze, zniechęcający wpływ na wykonywanie praw podstawowych ustanowionych w art. 7 i 11 karty, o którym mowa w pkt 46 niniejszego wyroku, jaki może wywrzeć zatrzymywanie tych danych, a po drugie, wagę ingerencji, jaką pociąga za sobą takie zatrzymywanie, w społeczeństwie demokratycznym, ważne jest, jak przewiduje system ustanowiony przez dyrektywę 2002/58, aby było ono wyjątkiem, a nie regułą, i aby dane te nie mogły być zatrzymywane w sposób systemowy i stały. Wniosek ten nasuwa się nawet jeśli uwzględnić cele zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla

bezpieczeństwa publicznego oraz wagę, jaką należy im nadać (zob. podobnie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 141, 142 i przytoczone tam orzecznictwo).

66 Ponadto Trybunał podkreślił, że uregulowanie krajowe przewidujące uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji obejmuje łączność elektroniczną prawie całej ludności, bez dokonania jakiegokolwiek rozróżnienia, ograniczenia ani wyjątku w zależności 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 zatem zastosowanie nawet do osób, co do których brak jest jakichkolwiek wskazówek mogących sugerować, że ich zachowanie może mieć związek, chociażby pośredni i daleki, z tym celem zwalczania poważnych przestępstw, a w szczególności bez wykazania związku między danymi, których zatrzymywanie jest przewidziane, a zagrożeniem dla bezpieczeństwa publicznego. W szczególności, jak orzekł już Trybunał, takie uregulowanie nie jest ograniczone do zatrzymywania danych w określonym czasie lub obszarze geograficznym czy też danych dotyczących kręgu osób, które mogłyby być powiązane w taki czy inny sposób z poważnym przestępstwem, lub też osób, których zatrzymane dane mogłyby w inny sposób przyczynić się do walki z poważną przestępczością (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 143, 144 i przytoczone tam orzecznictwo).

67 Natomiast w pkt 168 wyroku z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791) Trybunał wyjaśnił, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty nie stoi na przeszkodzie przepisom ustawodawczym przewidującym, do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego:

– ukierunkowane zatrzymywanie danych o ruchu i danych o lokalizacji, którego granice zostają wyznaczone na podstawie obiektywnych i niedyskryminacyjnych przesłanek w zależności od kręgu osób, których dane dotyczą, lub kryterium geograficznego, na okres ograniczony do tego, co ściśle niezbędne, ale odnawialny;

– uogólnione i niezróżnicowane zatrzymywanie adresów IP przydzielonych źródłu połączenia, w okresie ograniczonym do tego, co ściśle niezbędne;

– uogólnione i niezróżnicowane zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej; oraz

– posłużenie się skierowanym do dostawców usług łączności elektronicznej, w drodze decyzji właściwego organu poddanej skutecznej kontroli sądowej, nakazem szybkiego zatrzymania *(quick freeze)* przez określony czas danych o ruchu i danych o lokalizacji, którymi dysponują ci dostawcy usług,

jeśli środki te zawierają jasne i precyzyjne przepisy zapewniające, że rozpatrywane zatrzymywanie danych jest uzależnione od spełnienia związanych z nim materialnych i proceduralnych przesłanek oraz że osoby, których dane dotyczą, dysponują skutecznymi gwarancjami chroniącymi przed ryzykiem nadużyć.

68 W rozpatrywanym tu wniosku o wydanie orzeczenia w trybie prejudycjalnym, który wpłynął do Trybunału przed ogłoszeniem wyroków z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791) i z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej) (C-746/18, EU:C:2021:152), sąd odsyłający uznał jednak, że jedynie uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji pozwala walczyć w skuteczny sposób z poważną przestępczością. Na rozprawie w dniu 13 września 2021 r. w szczególności Irlandia i rząd francuski podniosły, że takiego wniosku nie podważa okoliczność, iż państwa członkowskie mogą posłużyć się środkami, o których mowa w poprzednim punkcie.

69 W tym względzie w pierwszej kolejności należy zauważyć, że skuteczność ścigania karnego zależy zazwyczaj nie od jednego instrumentu dochodzeniowego, lecz od wszystkich instrumentów dochodzeniowych, jakimi dysponują właściwe organy krajowe w tym celu.

70 W drugiej kolejności należy podkreślić, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, zgodnie z jego wykładnią dokonaną w orzecznictwie przypomnianym w pkt 67 niniejszego wyroku, pozwala państwom członkowskim przyjmować – w celu zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego – nie tylko przepisy ustanawiające ukierunkowane zatrzymywanie i szybkie zatrzymywanie, ale także przepisy przewidujące uogólnione i niezróżnicowane zatrzymywanie, po pierwsze, danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej, a po drugie, adresów IP przypisanych do źródła połączenia.

71 W tym względzie jest bezsporne, że zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej może przyczynić się do zwalczania poważnej przestępczości, pod warunkiem że dane te pozwalają zidentyfikować osoby, które korzystały z takich środków w ramach przygotowywania lub popełnienia poważnego przestępstwa.

72 Otóż, jak wynika z orzecznictwa podsumowanego w pkt 67 niniejszego wyroku, dyrektywa 2002/58 nie stoi na przeszkodzie uogólnionemu zatrzymywaniu danych dotyczących tożsamości cywilnej do celów zwalczania ogółu przestępczości. W tych okolicznościach należy uściślić, że ani ta dyrektywa, ani żaden inny akt prawa Unii nie stoją na przeszkodzie uregulowaniu krajowemu, mającemu na celu zwalczanie poważnej przestępczości, na podstawie którego nabycie środka łączności elektronicznej, takiego jak opłaconej z góry karty SIM, jest uzależnione od sprawdzenia urzędowych dokumentów ustalających tożsamość nabywcy i od zarejestrowania przez sprzedawcę wynikających z nich informacji, gdyż sprzedawca jest w stosownym wypadku zobowiązany do udzielenia dostępu do tych informacji właściwym organom krajowym.

73 Ponadto należy przypomnieć, że uogólnione zatrzymywanie adresów IP źródła połączenia stanowi poważną ingerencję w prawa podstawowe ustanowione w art. 7 i 8 karty, ponieważ te adresy IP mogą pozwolić na wyciągnięcie dokładnych wniosków na temat życia prywatnego użytkownika danego środka łączności elektronicznej, i może ono mieć zniechęcające skutki dla wykonywania wolności wypowiedzi zagwarantowanej w art. 11 karty. Niemniej w odniesieniu do takiego zatrzymywania Trybunał stwierdził, że do celów wymaganego przez orzecznictwo koniecznego pogodzenia wchodzących w rachubę praw i uzasadnionych interesów, o którym mowa w pkt 50–53 niniejszego wyroku, należy uwzględnić okoliczność, iż w przypadku przestępstwa popełnionego w Internecie, zwłaszcza w przypadku nabywania, rozpowszechniania, przekazywania lub udostępniania w Internecie pornografii dziecięcej w rozumieniu art. 2 lit. c) dyrektywy Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego

dzieci oraz pornografii dziecięcej, zastępującej decyzję ramową Rady 2004/68/WSiSW (Dz.U. 2011, L 335, s. 1) adres IP może stanowić jedyny środek dochodzeniowy umożliwiający ustalenie tożsamości osoby, której adres ten był przypisany w chwili popełnienia tego przestępstwa (zob. podobnie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 153, 154).

74 Wobec tego Trybunał orzekł, że takie uogólnione i niezróżnicowane zatrzymywanie jedynie adresów IP przypisanych do źródła połączenia nie wydaje się co do zasady sprzeczne z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 karty, pod warunkiem że możliwość ta zostanie uzależniona od ścisłego spełnienia przesłanek materialnych i proceduralnych, które winny regulować wykorzystywanie tych danych, o których to przesłankach jest mowa w pkt 155 i 156 wyroku z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791).

75 W trzeciej kolejności, jeśli chodzi o środki ustawodawcze przewidujące ukierunkowane zatrzymywanie i szybkie zatrzymywanie danych o ruchu i danych o lokalizacji, wskazówki zawarte we wniosku o wydanie orzeczenia w trybie prejudycjalnym świadczą o węższym zrozumieniu zakresu tych środków niż zakres przyjęty w orzecznictwie przypomnianym w pkt 67 niniejszego wyroku. Choć bowiem zgodnie z tym, co zostało przypomniane w pkt 40 niniejszego wyroku, te polegające na zatrzymywaniu środki powinny mieć charakter odstępstwa w systemie ustanowionym w dyrektywie 2002/58, dyrektywa ta jednak, interpretowana w świetle praw podstawowych ustanowionych w art. 7, 8 i 11 oraz art. 52 ust. 1 karty, nie uzależnia możliwości wydania nakazu przewidującego ukierunkowane zatrzymywanie od warunku, by były z góry znane miejsca mogące być sceną poważnych przestępstw oraz osoby podejrzane o udział w takim przestępstwie. Podobnie dyrektywa ta nie wymaga, by nakaz przewidujący szybkie zatrzymywanie był ograniczony do podejrzanych zidentyfikowanych przed wydaniem takiego nakazu.

76 Po pierwsze, jeśli chodzi o ukierunkowane zatrzymywanie, Trybunał orzekł, że art. 15 ust. 1 dyrektywy 2002/58 nie stoi na przeszkodzie uregulowaniu krajowemu opartemu na obiektywnych elementach, umożliwiającemu objęcie osób, których dane o ruchu i dane o lokalizacji mogą ujawnić związek, przynajmniej pośredni, z poważnymi przestępstwami, przyczynić się do walki z poważną przestępczością lub zapobiegać poważnemu ryzyku dla bezpieczeństwa publicznego bądź ryzyku dla bezpieczeństwa narodowego (wyroki: z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970, pkt 111; a także z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 148).

77 Trybunał wyjaśnił w tym względzie, że chociaż te obiektywne elementy mogą się różnić w zależności od środków podjętych w celu zapobiegania poważnym przestępstwom, ich dochodzenia, wykrywania i ścigania, takie środki mogą obejmować w szczególności te osoby, które zostały wcześniej zidentyfikowane w ramach właściwych procedur krajowych oraz na podstawie obiektywnych i niedyskryminacyjnych przesłanek jako stwarzające zagrożenie dla bezpieczeństwa publicznego lub bezpieczeństwa narodowego danego państwa członkowskiego (zob. podobnie wyroki: z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970, pkt 110; a także z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 149).

78 Państwa członkowskie mają zatem w szczególności możliwość przyjmowania środków polegających na zatrzymywaniu danych odnoszących się do osób, które – tytułem takiej identyfikacji – są objęte dochodzeniem lub innymi aktualnymi środkami nadzoru lub wpisem w krajowym rejestrze karnym wspominającym o wcześniejszym skazaniu za poważne

przestępstwa, mogącym oznaczać wysokie ryzyko recydywy. Otóż gdy taka identyfikacja opiera się na określonych przez prawo krajowe obiektywnych i niedyskryminacyjnych przesłankach, ukierunkowane zatrzymywanie danych obejmujące zidentyfikowane w ten sposób osoby jest uzasadnione.

79 Z drugiej strony środek polegający na ukierunkowanym zatrzymywaniu danych o ruchu i danych o lokalizacji może – zgodnie z wyborem ustawodawcy krajowego i w ścisłym poszanowaniu zasady proporcjonalności – być również oparty na kryterium geograficznym, jeżeli właściwe organy krajowe uznają, na podstawie obiektywnych i niedyskryminacyjnych przesłanek, że na jednym lub większej liczbie obszarów geograficznych istnieje wysokie ryzyko przygotowania lub popełnienia poważnych przestępstw. Obszarami tymi mogą być w szczególności miejsca charakteryzujące się dużą liczbą poważnych przestępstw, miejsca szczególnie narażone na popełnianie poważnych przestępstw, takie jak miejsca lub infrastruktura, w których regularnie przebywa bardzo wiele osób, lub też miejsca strategiczne, takie jak porty lotnicze, dworce, porty morskie lub strefy poboru opłat za przejazd (zob. podobnie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 150 i przytoczone tam orzecznictwo).

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

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

82 Należy jeszcze zauważyć, że strefy geograficzne objęte takim ukierunkowanym zatrzymywaniem danych mogą, a w stosownym wypadku muszą zostać zmodyfikowane, w zależności od zmiany warunków, które uzasadniały ich wybór, pozwalając tym samym reagować na zmiany w walce z poważną przestępczością. Trybunał orzekł już bowiem, że czas obowiązywania środków polegających na ukierunkowanym zatrzymywaniu danych, opisanych w pkt 76–81 niniejszego wyroku, nie może przekraczać okresu, który jest ściśle niezbędny w świetle zamierzonego celu

oraz okoliczności je uzasadniających, bez uszczerbku dla ewentualnego przedłużenia ze względu na utrzymywanie się konieczności takiego zatrzymywania (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 151).

83 Jeśli chodzi o możliwość przewidzenia odróżniających kryteriów innych niż kryterium osobowe lub geograficzne w celu wprowadzenia w życie ukierunkowanego zatrzymywania danych o ruchu i danych o lokalizacji, nie można wykluczyć, że pod uwagę mogą zostać wzięte inne obiektywne i niedyskryminacyjne kryteria, aby zapewnić, by zakres ukierunkowanego zatrzymywania danych był ograniczony do tego, co jest ściśle niezbędne, oraz ustalić przynajmniej pośredni związek między poważnymi przestępstwami a osobami, których dane są zatrzymywane. Niemniej, jako że art. 15 ust. 1 dyrektywy 2002/58 odnosi się do środków ustawodawczych państw członkowskich, to do tych państw, a nie do Trybunału należy ustalenie takich kryteriów, przy czym nie może być mowy o ponownym wprowadzeniu w ten sposób uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji.

84 W każdym wypadku, jak zauważył rzecznik generalny M. Campos Sánchez-Bordona w pkt 50 opinii w sprawach połączonych SpaceNet i Telekom Deutschland (C-793/19 i C-794/19, EU:C:2021:939), ewentualne istnienie trudności w dokładnym określeniu przesłanek i warunków, na jakich można dokonać ukierunkowanego zatrzymywania danych, nie może uzasadniać wprowadzenia przez państwa członkowskie, w drodze przyjęcia wyjątku za regułę, uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji.

85 Po drugie, w odniesieniu do szybkiego zatrzymywania danych o ruchu i danych o lokalizacji przetwarzanych i przechowywanych przez dostawców usług łączności elektronicznej na podstawie art. 5, 6 i 9 dyrektywy 2002/58 lub środków ustawodawczych przyjętych na podstawie art. 15 ust. 1 tej dyrektywy, należy przypomnieć, że takie dane powinny co do zasady zostać, w zależności od przypadku, usunięte lub zanonimizowane po upływie ustawowych terminów, w których zgodnie z krajowymi przepisami transponującymi ową dyrektywę powinno nastąpić ich przetwarzanie i przechowywanie. Trybunał orzekł jednak, że podczas tego przetwarzania i tego przechowywania danych mogą występować sytuacje, w których zachodzi konieczność zatrzymywania rzeczonych danych po upływie tych terminów w celu wyjaśnienia poważnych przestępstw lub naruszeń bezpieczeństwa narodowego, i to zarówno w sytuacji, gdy te przestępstwa lub te naruszenia już zostały stwierdzone, jak i w sytuacji, w której ich istnienie po przeprowadzeniu obiektywnego badania wszystkich istotnych okoliczności może być racjonalnie podejrzewane (zob. podobnie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 160, 161).

86 W takiej sytuacji, z uwagi na konieczność pogodzenia wchodzących w grę praw i uzasadnionych interesów, o której mowa w pkt 50–53 niniejszego wyroku, państwa członkowskie mogą przewidzieć w uregulowaniu przyjętym na podstawie art. 15 ust. 1 dyrektywy 2002/58 możliwość nakazania dostawcom usług łączności elektronicznej, w drodze decyzji właściwego organu poddanej skutecznej kontroli sądowej, szybkiego zatrzymywania przez określony czas danych o ruchu i danych o lokalizacji, którymi ci dysponują (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 163).

87 Jako że cel takiego szybkiego zatrzymywania nie odpowiada już celom, dla których dane zostały pierwotnie zgromadzone i zatrzymane, a wszelkie przetwarzanie danych powinno na mocy art. 8 ust. 2 karty odpowiadać określonym celom, państwa członkowskie powinny określić w swoim ustawodawstwie cel, dla którego może nastąpić szybkie zatrzymywanie danych. Ze względu na poważny charakter ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty, jaką może

stanowić takie zatrzymywanie, jedynie walka z poważną przestępczością i, a fortiori, ochrona bezpieczeństwa narodowego mogą uzasadniać tę ingerencję, pod warunkiem że ten środek oraz dostęp do zatrzymanych w ten sposób danych przestrzegają granic tego, co ściśle niezbędne, takich jak te wskazane w pkt 164–167 wyroku z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791).

88 Trybunał wyjaśnił, że tego rodzaju środek polegający na zatrzymywaniu danych nie może być ograniczony do danych osób zidentyfikowanych uprzednio jako stanowiące zagrożenie dla bezpieczeństwa publicznego lub bezpieczeństwa narodowego danego państwa członkowskiego lub osób konkretnie podejrzewanych o popełnienie poważnego przestępstwa lub naruszenie bezpieczeństwa narodowego. Zdaniem Trybunału taki środek, przy poszanowaniu ram ustanowionych w art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, może bowiem z uwagi na rozważania zawarte w pkt 55 niniejszego wyroku – zgodnie z wyborem ustawodawcy krajowego i przy poszanowaniu granic tego, co ściśle niezbędne – zostać rozszerzony na dane o ruchu i dane o lokalizacji dotyczące osób innych niż te, które są podejrzewane o planowanie lub popełnienie poważnego przestępstwa lub naruszenie bezpieczeństwa narodowego, o ile dane te mogą w oparciu o obiektywne i niedyskryminacyjne kryteria przyczynić się do wyjaśnienia takiego przestępstwa lub takiego naruszenia bezpieczeństwa narodowego, takie jak dane ofiary tego przestępstwa lub naruszenia, jej otoczenia społecznego lub zawodowego (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 165).

89 A zatem środek ustawodawczy może zezwalać na skorzystanie ze skierowanego do dostawców usług łączności elektronicznej nakazu dokonania szybkiego zatrzymania danych o ruchu i danych o lokalizacji, w szczególności osób, z którymi – przed wystąpieniem poważnego zagrożenia dla bezpieczeństwa publicznego lub popełnienia poważnego przestępstwa – ofiara była w kontakcie przy użyciu swoich środków łączności elektronicznej.

90 Takie szybkie zatrzymywanie danych może – zgodnie z orzecznictwem Trybunału przypomnianym w pkt 88 niniejszego wyroku oraz w tych samych warunkach, o których mowa w tym punkcie – także zostać rozszerzone na określone strefy geograficzne, takie jak miejsca popełnienia i przygotowania danego przestępstwa lub naruszenia bezpieczeństwa narodowego. Należy doprecyzować, że przedmiotem takiego środka mogą być również dane o ruchu i dane lokalizacji związane z miejscem, w którym osoba będąca potencjalnie ofiarą poważnego przestępstwa zaginęła, pod warunkiem że ten środek oraz dostęp do zatrzymanych w ten sposób danych przestrzegają granic tego, co ściśle niezbędne do celów walki z poważną przestępczością lub ochrony bezpieczeństwa narodowego, takich jak granice wskazane w pkt 164–167 wyroku z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791).

91 Ponadto należy uściślić, że art. 15 ust. 1 dyrektywy 2002/58 nie stoi na przeszkodzie temu, by właściwe organy krajowe zarządziły środek polegający na szybkim zatrzymywaniu danych już na pierwszym etapie dochodzenia dotyczącego poważnego zagrożenia dla bezpieczeństwa publicznego lub ewentualnego poważnego przestępstwa, czyli w chwili, w której zgodnie z właściwymi przepisami prawa krajowego organy te mogą wszcząć takie dochodzenie.

92 W odniesieniu do różnorodności środków polegających na zatrzymywaniu danych o ruchu i danych o lokalizacji, o których mowa w pkt 67 niniejszego wyroku, należy uściślić, że te różne środki mogą – zgodnie z wyborem ustawodawcy krajowego i przy poszanowaniu granic tego, co ściśle niezbędne – znaleźć wspólnie zastosowanie. W tych okolicznościach art. 15 ust. 1 dyrektywy

2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, w wykładni nadanej mu w orzecznictwie wynikającym z wyroku z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791), nie stoi na przeszkodzie połączeniu tych środków.

93 W czwartej kolejności należy wreszcie podkreślić, że proporcjonalność środków przyjętych na podstawie art. 15 ust. 1 dyrektywy 2002/58 wymaga – zgodnie z utrwalonym orzecznictwem Trybunału, które zostało podsumowane w wyroku z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791) – spełnienia nie tylko wymogów zdatności i konieczności, ale także wymogu odnoszącego się do proporcjonalnego charakteru tych środków w stosunku do zamierzonego celu.

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

95 W tym samym duchu Trybunał wyjaśnił w pkt 145 wyroku z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791), że nawet pozytywne obowiązki państw członkowskich, które mogą wynikać, w zależności od przypadku, z art. 3, 4 i 7 karty i które, jak zauważono w pkt 49 niniejszego wyroku, dotyczą ustanowienia przepisów umożliwiających skuteczne zwalczanie przestępstw, nie mogą uzasadniać tak poważnych ingerencji jak te wynikające z przepisów krajowych przewidujących zatrzymywanie danych o ruchu i danych o lokalizacji w prawa podstawowe ustanowione w art. 7 i 8 karty prawie całej ludności, gdy dane zainteresowanych osób nie wykazują związku, choćby pośredniego, z zamierzonym celem.

96 Na rozprawie rząd duński utrzymywał, że zgodnie z orzecznictwem wynikającym z wyroku z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 135–139) właściwe organy krajowe powinny móc mieć dostęp do celów walki z poważną przestępczością do danych o ruchu i danych o lokalizacji, które zostały zatrzymane w sposób uogólniony i niezróżnicowany, aby stawić czoła poważnemu zagrożeniu dla bezpieczeństwa narodowego, które jest rzeczywiste i aktualne lub przewidywalne.

97 Należy od razu zauważyć, że fakt zezwolenia na dostęp do celów walki z poważną przestępczością do danych o ruchu i danych o lokalizacji, które zostały zatrzymane w sposób uogólniony i niezróżnicowany, spowodowałby uzależnienie tego dostępu od okoliczności niezwiązanych z tym celem, w zależności od istnienia lub nieistnienia w danym państwie członkowskim poważnego zagrożenia dla bezpieczeństwa narodowego, takiego jak to wspomniane w poprzednim punkcie, podczas gdy w świetle jedynego celu w postaci zwalczania poważnej przestępczości, który powinien uzasadniać zatrzymywanie tych danych i dostęp do nich, nic nie uzasadnia różnicy w traktowaniu w szczególności wśród państw członkowskich.

98 Jak już orzekł Trybunał, dostęp do danych o ruchu i do danych o lokalizacji zatrzymywanych przez dostawców w zastosowaniu środka przyjętego na podstawie art. 15 ust. 1 dyrektywy 2002/58, co musi mieć miejsce w pełnym poszanowaniu warunków wynikających z orzecznictwa, w którym dokonano wykładni dyrektywy 2002/58, może co do zasady być uzasadniony jedynie celem

interesu ogólnego, dla którego dostawcy ci zostali zobowiązani do takiego zatrzymywania. Inaczej jest jedynie wtedy, gdy znaczenie celu przyświecającego dostępowi jest większe niż znaczenie celu, który uzasadniał zatrzymywanie danych (zob. podobnie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 165, 166).

99 Tymczasem argumentacja rządu duńskiego odnosi się do sytuacji, w której cel planowanego wniosku o udzielenie dostępu, to jest zwalczanie poważnej przestępczości, ma w hierarchii celów interesu ogólnego mniejsze znaczenie niż cel, który uzasadniał zatrzymywanie danych, czyli ochrona bezpieczeństwa narodowego. Zezwolenie w takiej sytuacji na dostęp do zatrzymanych danych pozostawałoby w sprzeczności z tą hierarchią celów interesu ogólnego, przypomnianą w poprzednim punkcie, jak również w pkt 53, 56, 57 i 59 niniejszego wyroku.

100 Ponadto należy przede wszystkim stwierdzić, że zgodnie z orzecznictwem przypomnianym w pkt 65 niniejszego wyroku dane o ruchu i dane o lokalizacji nie mogą być przedmiotem uogólnionego i niezróżnicowanego zatrzymywania danych do celów walki z poważną przestępczością, a tym samym dostęp do tych danych nie może być uzasadniony to tychże celów. Otóż jeżeli te dane zostały wyjątkowo zatrzymane w sposób uogólniony i niezróżnicowany do celów ochrony bezpieczeństwa narodowego przed zagrożeniem, które okazuje się rzeczywiste i aktualne lub przewidywalne, w warunkach wskazanych w pkt 58 niniejszego wyroku, organy krajowe właściwe w zakresie dochodzeń w sprawach karnych nie mogą mieć dostępu do owych danych w ramach ścigania karnego, pod rygorem pozbawienia wszelkiej skuteczności (effet utile) zakazu takiego zatrzymywania do celów walki z poważną przestępczością, przypomnianego w pkt 65.

101 W świetle całości powyższych rozważań na pytania pierwsze, drugie i czwarte należy odpowiedzieć, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty należy interpretować w ten sposób, iż stoi on na przeszkodzie środkom ustawodawczym przewidującym, do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji. Natomiast wspomniany art. 15 ust. 1 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty nie stoi na przeszkodzie środkom ustawodawczym przewidującym, do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego:

– ukierunkowane zatrzymywanie danych o ruchu i danych o lokalizacji, którego granice zostają wyznaczone na podstawie obiektywnych i niedyskryminacyjnych przesłanek w zależności od kategorii osób, których dane dotyczą, lub za pomocą kryterium geograficznego, przez okres ograniczony do tego, co ściśle niezbędne, ale odnawialny;

– uogólnione i niezróżnicowane zatrzymywanie adresów IP przydzielonych źródłu połączenia, przez okres ograniczony do tego, co ściśle niezbędne;

– uogólnione i niezróżnicowane zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej; oraz

– posłużenie się skierowanym do dostawców usług łączności elektronicznej, w drodze decyzji właściwego organu poddanej skutecznej kontroli sądowej, nakazem szybkiego zatrzymania przez określony czas danych o ruchu i danych o lokalizacji, którymi dysponują ci dostawcy usług,

o ile środki te, za pomocą jasnych i precyzyjnych przepisów, zapewniają, że odnośne zatrzymywanie danych jest uzależnione od spełnienia związanych z nim materialnych i proceduralnych przesłanek oraz że osoby, których dane dotyczą, dysponują skutecznymi gwarancjami chroniącymi przed ryzykiem nadużyć.

W przedmiocie pytania trzeciego

102 W pytaniu trzecim sąd odsyłający zastanawia się zasadniczo, czy art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8, 11 oraz art. 52 ust. 1 karty należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu, na podstawie którego scentralizowane rozpatrywanie pochodzących od policji wniosków o udzielenie dostępu do zatrzymanych danych, w ramach wykrywania i ścigania poważnych przestępstw, należy do funkcjonariusza policji, wspieranego przez jednostkę ustanowioną w obrębie policji, której przysługuje pewien stopień autonomii w wykonywaniu powierzonego jej zadania i której decyzje mogą być następnie przedmiotem kontroli sądowej.

103 Tytułem wstępu należy przypomnieć, że o ile do prawa krajowego należy określenie warunków, na jakich dostawcy usług łączności elektronicznej powinni udzielać właściwym organom państwowym dostępu do danych będących w ich posiadaniu, o tyle uregulowanie krajowe musi, aby spełnić wymóg proporcjonalności przypomniany w pkt 54 niniejszego wyroku, zawierać jasne i precyzyjne przepisy regulujące zakres i sposób stosowania danego środka oraz ustanawiające minimalne wymogi służące temu, aby osoby, o których dane osobowe chodzi, miały wystarczające gwarancje pozwalające na skuteczną ochronę tych danych przed ryzykiem nadużyć [zob. podobnie wyrok z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C-746/18, EU:C:2021:152, pkt 48 i przytoczone tam orzecznictwo].

104 W szczególności uregulowanie krajowe regulujące dostęp właściwych organów do zatrzymanych danych o ruchu i danych o lokalizacji, przyjęte na podstawie art. 15 ust. 1 dyrektywy 2002/58, nie może ograniczać się do wymagania, aby dostęp organów do danych odpowiadał celowi, do którego zmierza to uregulowanie, ale musi również przewidywać przesłanki materialne i proceduralne regulujące to wykorzystanie [wyrok z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C-746/18, EU:C:2021:152, pkt 49 i przytoczone tam orzecznictwo].

105 I tak, ponieważ powszechnego dostępu do zatrzymanych danych, niezależnie od jakiegokolwiek związku, nawet pośredniego, z realizowanym celem, nie można uważać za ograniczony do tego, co ściśle konieczne, dane uregulowanie krajowe powinno opierać się na obiektywnych kryteriach umożliwiających określenie okoliczności i warunków przyznania dostępu właściwym organom państwowym do spornych danych. W tym względzie, z uwagi na cel polegający na zwalczaniu poważnej przestępczości, taki dostęp może co do zasady zostać przyznany jedynie w odniesieniu do danych dotyczących osób podejrzewanych o planowanie, popełnianie czy też popełnienie poważnego przestępstwa bądź też zaangażowanych w taki czy inny sposób w takie przestępstwo. 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 [wyrok z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C-746/18, EU:C:2021:152, pkt 50 i przytoczone tam orzecznictwo].

106 W celu zapewnienia w praktyce pełnej zgodności z tymi warunkami ważne jest, aby dostęp właściwych organów krajowych do zatrzymanych danych był 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 przestępstwom, ich wykrywanie lub ściganie karne [wyrok z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C-746/18, EU:C:2021:152, pkt 51 i przytoczone tam orzecznictwo].

107 Ta uprzednia kontrola wymaga między innymi, aby sąd lub organ odpowiedzialny za przeprowadzenie tej kontroli dysponował wszelkimi uprawnieniami i gwarancjami niezbędnymi do pogodzenia różnych wchodzących w grę uzasadnionych interesów i praw. Jeśli chodzi w szczególności o dochodzenie w sprawach karnych, taka kontrola wymaga, aby ten sąd lub organ był w stanie zapewnić właściwą równowagę pomiędzy z jednej strony uzasadnionymi interesami związanymi z potrzebami dochodzenia w ramach zwalczania przestępczości, a z drugiej strony prawami podstawowymi do poszanowania życia prywatnego i ochrony danych osobowych osób, których dane są udostępniane [wyrok z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C-746/18, EU:C:2021:152, pkt 52].

108 Jeżeli kontrola ta jest dokonywana nie przez sąd, lecz przez niezależny organ administracyjny, organ ten musi posiadać status pozwalający mu działać w wykonywaniu swoich obowiązków w sposób obiektywny i bezstronny i w tym celu powinien on pozostawać poza jakimkolwiek wpływem z zewnątrz. A zatem wymóg niezależności, który powinien spełniać organ odpowiedzialny za przeprowadzenie uprzedniej kontroli, wymaga, aby organ ten miał status strony trzeciej w stosunku do organu wnoszącego o udzielenie dostępu do danych, tak aby ten pierwszy był w stanie przeprowadzić tę kontrolę w sposób obiektywny i bezstronny, poza jakimkolwiek wpływem z zewnątrz. W szczególności w dziedzinie prawa karnego wymóg niezależności oznacza, że organ odpowiedzialny za tę uprzednią kontrolę, po pierwsze, nie jest zaangażowany w prowadzenie danego dochodzenia karnego, a po drugie, zajmuje neutralną pozycję wobec stron postępowania karnego [zob. podobnie wyrok z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C-746/18, EU:C:2021:152, pkt 53, 54].

109 I tak Trybunał uznał w szczególności, że prokuraturze, która kieruje postępowaniem dochodzeniowym i w stosownych przypadkach sprawuje funkcję oskarżyciela publicznego, nie można przyznać statusu strony trzeciej w stosunku do wchodzących w grę uzasadnionych interesów, ponieważ jej zadaniem nie jest rozstrzygnięcie sporu przy zachowaniu całkowitej niezależności, lecz skierowanie sporu, w stosownym wypadku, do właściwego sądu, jako strona postępowania, która wnosi akt oskarżenia. W konsekwencji prokuratura nie jest w stanie przeprowadzić uprzedniej kontroli wniosków o udzielenie dostępu do zatrzymanych danych [zob. podobnie wyrok z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C-746/18, EU:C:2021:152, pkt 55, 57].

110 Wreszcie niezależna kontrola wymagana zgodnie z art. 15 ust. 1 dyrektywy 2002/58 powinna mieć miejsce przed uzyskaniem wszelkiego dostępu do zatrzymanych danych, z wyjątkiem pilnych i należycie uzasadnionych przypadków, w których powinna ona nastąpić w krótkim czasie. Późniejsza kontrola nie pozwala bowiem osiągnąć celu uprzedniej kontroli, polegającego na uniemożliwieniu udzielania zezwoleń na dostęp do rozpatrywanych danych, który wykracza poza granice tego, co ściśle niezbędne (zob. podobnie wyroki: z dnia 6 października 2020 r., La

Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 189; a także z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C-746/18, EU:C:2021:152, pkt 58].

111 W niniejszym przypadku z wniosku o wydanie orzeczenia w trybie prejudycjalnym wynika przede wszystkim, że ustawa z 2011 r. przyznaje funkcjonariuszowi policji, który ma co najmniej stopień nadinspektora, kompetencję do dokonywania uprzedniej kontroli wniosków o udzielenie dostępu do danych pochodzących od służb dochodzeniowych policji oraz do żądania od dostawców usług łączności elektronicznej przekazania mu danych zatrzymanych przez tych dostawców. Jako że funkcjonariusz ten nie ma statusu strony trzeciej w stosunku do tych służb, nie spełnia on wymogów niezależności i bezstronności przypomnianych w pkt 108 niniejszego wyroku, mimo okoliczności, że w wykonywaniu tego zadania wspiera go jednostka policji, w niniejszym przypadku TLU, której przysługuje pewien stopień autonomii w wykonywaniu jej zadania.

112 Co więcej, choć ustawa z 2011 r. przewiduje mechanizmy następczej kontroli decyzji właściwego funkcjonariusza policji w postaci postępowania zażaleniowego i postępowania przed sędzią odpowiedzialnym za zbadanie zastosowania przepisów rzeczonej ustawy, z orzecznictwa przypomnianego w pkt 110 niniejszego wyroku wynika, że kontrola sprawowana a posteriori nie może zastąpić wymogu – przypomnianego w pkt 106 niniejszego wyroku – niezależnej i uprzedniej kontroli, z wyjątkiem pilnych i należycie uzasadnionych przypadków.

113 Wreszcie ustawa z 2011 r. nie przewiduje obiektywnych kryteriów określających dokładnie warunki i okoliczności, w których organom krajowym należy przyznać dostęp do danych, ponieważ funkcjonariusz policji odpowiedzialny za rozpatrywanie wniosków o udzielenie dostępu do zatrzymanych danych jest wyłącznie właściwy, jak potwierdziła Irlandia na rozprawie, do dokonywania oceny podejrzeń ciążących na danych osobach oraz konieczności dostępu do danych dotyczących tych osób.

114 W związku z powyższym na pytanie trzecie należy odpowiedzieć, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8, 11 oraz art. 52 ust. 1 karty należy interpretować w ten sposób, iż stoi on na przeszkodzie uregulowaniu krajowemu, na podstawie którego scentralizowane rozpatrywanie pochodzących od policji wniosków o udzielenie dostępu do danych zatrzymanych przez dostawców usług łączności elektronicznej, w ramach wykrywania i ścigania poważnych przestępstw, należy do funkcjonariusza policji, wspieranego przez jednostkę ustanowioną w obrębie policji, której przysługuje pewien stopień autonomii w wykonywaniu powierzonego jej zadania i której decyzje mogą być następnie przedmiotem kontroli sądowej.

W przedmiocie pytań piątego i szóstego

115 Poprzez pytania piąte i szóste, które należy zbadać łącznie, sąd odsyłający dąży w istocie do ustalenia, czy prawo Unii należy interpretować w ten sposób, iż sąd krajowy może ograniczyć w czasie skutki stwierdzenia nieważności, którego ma on dokonać na podstawie prawa krajowego w odniesieniu do uregulowania krajowego nakładającego na dostawców usług łączności elektronicznej obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji, a to ze względu na niezgodność tego uregulowania z art. 15 ust. 1 dyrektywy 2002/58 w związku z kartą.

116 Z informacji dostarczonych przez sąd odsyłający wynika, że uregulowanie krajowe będące przedmiotem sporu w postępowaniu głównym, czyli ustawa z 2011 r., zostało wydane w celu przetransponowania do prawa krajowego dyrektywy 2006/24, której nieważność stwierdził następnie Trybunał w wyroku z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in. (C-293/12 i C-594/12, EU:C:2014:238).

117 Ponadto sąd odsyłający zauważył, że choć badanie dopuszczalności powołanych przeciwko G.D. w ramach postępowania karnego dowodów opartych na danych zatrzymanych na podstawie ustawy z 2011 r. należy do sędziego karnego, jednak to do sądu odsyłającego należy orzeczenie – w ramach postępowania cywilnego – w przedmiocie ważności spornych przepisów tej ustawy oraz skutków w czasie stwierdzenia nieważności tych przepisów. A zatem choć jedyną kwestią, która powstaje przed sądem odsyłającym, jest kwestia ważności przepisów ustawy z 2011 r., sąd ten uważa jednak za konieczne zwrócenie się do Trybunału z pytaniem dotyczącym wpływu ewentualnego stwierdzenia nieważności na dopuszczalność dowodów uzyskanych za pomocą uogólnionego i niezróżnicowanego zatrzymywania danych, na które pozwalała ta ustawa.

118 Tytułem wstępu należy przypomnieć, że zasada pierwszeństwa prawa Unii ustanawia prymat prawa Unii nad prawem państw członkowskich. Zasada ta nakłada zatem na wszystkie organy państw członkowskich obowiązek zapewnienia pełnej skuteczności różnych norm prawa Unii, a prawo państw członkowskich nie może mieć wpływu na skuteczność przyznaną tym różnym normom na terytorium wspomnianych państw. Zgodnie z tą zasadą w razie niemożności dokonania wykładni uregulowania krajowego w sposób zgodny z wymogami określonymi w prawie Unii sąd krajowy, do którego należy w ramach jego kompetencji stosowanie przepisów prawa Unii, jest zobowiązany zapewnić pełną ich skuteczność, w razie potrzeby powstrzymując się od stosowania, z własnej inicjatywy, wszelkich sprzecznych z nimi przepisów prawa krajowego, także późniejszych, bez konieczności żądania uprzedniego uchylenia tych przepisów w drodze ustawodawczej lub w jakimkolwiek innym trybie konstytucyjnym ani bez konieczności oczekiwania na takie uchylenie [zob. podobnie wyroki: z dnia 15 lipca 1964 r., Costa, 6/64, EU:C:1964:66, s. 1159, 1160; z dnia 19 listopada 2019 r., A.K. i in. (Niezależność Izby Dyscyplinarnej Sądu Najwyższego), C-585/18, C-624/18 i C-625/18, EU:C:2019:982, pkt 157, 158, 160; a także z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 214, 215].

119 Jedynie Trybunał może, w drodze wyjątku, kierując się nadrzędnymi względami pewności prawa, tymczasowo zawiesić wywierany przez prawo Unii skutek w postaci uchylenia przepisów prawa krajowego sprzecznych z prawem Unii. Takie ograniczenie w czasie skutków wykładni prawa Unii dokonanej przez Trybunał może zostać orzeczone jedynie w samym wyroku, w którym Trybunał rozstrzyga w przedmiocie wykładni, o którą się do niego zwrócono. Do naruszenia pierwszeństwa i jednolitego stosowania prawa Unii doszłoby, gdyby sądy krajowe były uprawnione do przyznania, choćby tymczasowo, przepisom krajowym pierwszeństwa przed prawem Unii, z którym te przepisy są sprzeczne (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 216, 217 i przytoczone tam orzecznictwo).

120 Prawdą jest, iż Trybunał uznał w sprawie dotyczącej zgodności z prawem środków przyjętych z naruszeniem ustanowionego w prawie Unii obowiązku przeprowadzenia uprzedniej oceny oddziaływania przedsięwzięcia na środowisko i na teren chroniony, że sąd krajowy może wyjątkowo utrzymać w mocy skutki takich środków, w przypadku gdy prawo krajowe na to zezwala, jeżeli to utrzymanie w mocy jest uzasadnione nadrzędnymi względami związanymi z koniecznością uniknięcia rzeczywistego i poważnego zagrożenia polegającego na przerwaniu

dostaw energii elektrycznej w danym państwie członkowskim, któremu nie można zaradzić za pomocą innych środków i rozwiązań alternatywnych, w szczególności w ramach rynku wewnętrznego, przy czym wspomniane utrzymanie w mocy może obejmować jedynie okres ściśle niezbędny do usunięcia tej niezgodności z prawem (zob. podobnie wyrok z dnia 29 lipca 2019 r., Inter-Environnement Wallonie i Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, pkt 175, 176, 179, 181).

121 Niemniej, w przeciwieństwie do pominięcia obowiązku proceduralnego takiego jak uprzednia ocena oddziaływania przedsięwzięcia, wpisującego się w szczególną dziedzinę ochrony środowiska, naruszenie art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty nie może być przedmiotem konwalidacji w drodze procedury porównywalnej z tą, o której mowa w poprzednim punkcie (zob. podobnie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 219).

122 Utrzymanie w mocy skutków uregulowania krajowego takiego jak ustawa z 2011 r. oznaczałoby bowiem, że uregulowanie to w dalszym ciągu nakładałoby na dostawców usług łączności elektronicznej obowiązki, które są sprzeczne z prawem Unii i które powodują poważną ingerencję w prawa podstawowe osób, których dane są zatrzymywane (zob. analogicznie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 219).

123 W związku z tym sąd odsyłający nie może ograniczyć w czasie skutków stwierdzenia nieważności, którego ma on dokonać na podstawie prawa krajowego w odniesieniu do uregulowania krajowego rozpatrywanego w postępowaniu głównym (zob. analogicznie wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 220).

124 W tym względzie, jak zauważył zasadniczo rzecznik generalny w pkt 75 opinii, okoliczność, że to uregulowanie krajowe zostało wydane w celu przetransponowania dyrektywy 2006/24 do prawa krajowego, jest pozbawiona znaczenia, gdyż z powodu stwierdzenia przez Trybunał nieważności tej dyrektywy – zważywszy że skutki tej nieważności sięgają daty jej wejścia w życie (zob. podobnie wyrok z dnia 8 lutego 1996 r., FMC i in., C-212/94, EU:C:1996:40, pkt 55) – sąd odsyłający powinien ocenić ważność tego uregulowania krajowego w świetle dyrektywy 2002/58 i karty, w wykładni nadanej im przez Trybunał.

125 W szczególności w odniesieniu do wykładni dyrektywy 2002/58 i karty przyjętej przez Trybunał między innymi w wyrokach z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970) i z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791) należy przypomnieć, że zgodnie z utrwalonym orzecznictwem wykładnia przepisu prawa Unii, jakiej dokonuje Trybunał w ramach wykonywania kompetencji przyznanej mu w art. 267 TFUE, wyjaśnia i precyzuje znaczenie oraz zakres tego przepisu, tak jak powinien lub powinien był być on rozumiany i stosowany od chwili jego wejścia w życie. Wynika stąd, że sądy mogą i powinny stosować zinterpretowany w ten sposób przepis do stosunków prawnych powstałych przed wydaniem wyroku w sprawie wniosku o dokonanie wykładni, jeżeli ponadto spełnione są wszystkie przesłanki wszczęcia przed właściwym sądem postępowania w sprawie związanej ze stosowaniem takiego przepisu (wyrok z dnia 16 września 2020 r., Romenergo i Aris Capital, C-339/19, EU:C:2020:709, pkt 47 i przytoczone tam orzecznictwo).

126 W tym względzie należy jeszcze uściślić, że ograniczenie w czasie skutków przyjętej wykładni nie zostało dokonane w wyrokach z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970) i z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791), w związku z czym, zgodnie z orzecznictwem przypomnianym w pkt 119 niniejszego wyroku, nie może ono nastąpić w wyroku Trybunału późniejszym od wspomnianych wyroków.

127 Wreszcie w odniesieniu do wpływu stwierdzenia ewentualnej niezgodności ustawy z 2011 r. z dyrektywą 2002/58, odczytywaną w świetle karty, na dopuszczalność dowodów powołanych przeciwko G.D. w ramach postępowania karnego wystarczy odesłać do orzecznictwa Trybunału w tej dziedzinie, a w szczególności do zasad przypomnianych w pkt 41–44 wyroku z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej) (C-746/18, EU:C:2021:152), z którego to orzecznictwa wynika, że zgodnie z zasadą autonomii proceduralnej państw członkowskich kwestia tej dopuszczalności należy do prawa krajowego, z zastrzeżeniem poszanowania w szczególności zasad równoważności i skuteczności.

128 W świetle powyższych rozważań na pytania piąte i szóste należy odpowiedzieć, że prawo Unii należy interpretować w ten sposób, iż stoi ono na przeszkodzie temu, by sąd krajowy ograniczył w czasie skutki stwierdzenia nieważności, którego ma on dokonać na podstawie prawa krajowego w odniesieniu do uregulowania krajowego nakładającego na dostawców usług łączności elektronicznej obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji, a to ze względu na niezgodność tego uregulowania z art. 15 ust. 1 dyrektywy 2002/58 interpretowanego w związku z kartą. Kwestia dopuszczalności dowodów uzyskanych za pomocą takiego uogólnionego i niezróżnicowanego zatrzymywania należy, zgodnie z zasadą autonomii proceduralnej państw członkowskich, do prawa krajowego, z zastrzeżeniem poszanowania w szczególności zasad równoważności i skuteczności.

W przedmiocie kosztów

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

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

1) **Artykuł 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywy o prywatności i łączności elektronicznej), zmienionej dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r., w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że stoi on na przeszkodzie środkom ustawodawczym przewidującym, do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji. Natomiast wspomniany art. 15 ust. 1 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych nie stoi na przeszkodzie środkom ustawodawczym przewidującym, do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego:**

– **ukierunkowane zatrzymywanie danych o ruchu i danych o lokalizacji, którego granice zostają wyznaczone na podstawie obiektywnych i niedyskryminacyjnych przesłanek w zależności od kategorii osób, których dane dotyczą, lub za pomocą kryterium geograficznego, przez okres ograniczony do tego, co ściśle niezbędne, ale odnawialny;**

– **uogólnione i niezróżnicowane zatrzymywanie adresów IP przydzielonych źródłu połączenia, przez okres ograniczony do tego, co ściśle niezbędne;**

– **uogólnione i niezróżnicowane zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej; oraz**

– **posłużenie się skierowanym do dostawców usług łączności elektronicznej, w drodze decyzji właściwego organu poddanej skutecznej kontroli sądowej, nakazem szybkiego zatrzymania przez określony czas danych o ruchu i danych o lokalizacji, którymi dysponują ci dostawcy usług,**

o ile środki te, za pomocą jasnych i precyzyjnych przepisów, zapewniają, że odnośne zatrzymywanie danych jest uzależnione od spełnienia związanych z nim materialnych i proceduralnych przesłanek oraz że osoby, których dane dotyczą, dysponują skutecznymi gwarancjami chroniącymi przed ryzykiem nadużyć.

2) **Artykuł 15 ust. 1 dyrektywy 2002/58, zmienionej dyrektywą 2009/136, w związku z art. 7, 8, 11 oraz art. 52 ust. 1 Karty praw podstawowych należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu, na podstawie którego scentralizowane rozpatrywanie pochodzących od policji wniosków o udzielenie dostępu do danych zatrzymanych przez dostawców usług łączności elektronicznej, w ramach wykrywania i ścigania poważnych przestępstw, należy do funkcjonariusza policji, wspieranego przez jednostkę ustanowioną w obrębie policji, której przysługuje pewien stopień autonomii w wykonywaniu powierzonego jej zadania i której decyzje mogą być następnie przedmiotem kontroli sądowej.**

3) **Prawo Unii należy interpretować w ten sposób, że stoi ono na przeszkodzie temu, by sąd krajowy ograniczył w czasie skutki stwierdzenia nieważności, którego ma on dokonać na podstawie prawa krajowego w odniesieniu do uregulowania krajowego nakładającego na dostawców usług łączności elektronicznej obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji, a to ze względu na niezgodność tego uregulowania z art. 15 ust. 1 dyrektywy 2002/58, zmienionej dyrektywą 2009/136, w związku z Kartą praw podstawowych. Kwestia dopuszczalności dowodów uzyskanych za pomocą takiego uogólnionego i niezróżnicowanego zatrzymywania należy, zgodnie z zasadą autonomii proceduralnej państw członkowskich, do prawa krajowego, z zastrzeżeniem poszanowania w szczególności zasad równoważności i skuteczności.**

Podpisy