Zbiór Orzeczeń

WYROK TRYBUNAŁU (wielka izba)

z dnia 2 marca 2021 r.*

Odesłanie prejudycjalne – Przetwarzanie danych osobowych w sektorze łączności elektronicznej – Dyrektywa 2002/58/WE – Dostawcy usług łączności elektronicznej – Poufność komunikacji – Ograniczenia – Artykuł 15 ust. 1 – Artykuły 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej – Ustawodawstwo przewidujące uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji przez dostawców usług łączności elektronicznej – Dostęp organów państwowych do zatrzymanych danych do celów dochodzenia – Zwalczanie ogółu przestępczości – Zezwolenie udzielone przez prokuraturę – Wykorzystanie danych w ramach postępowania karnego jako dowodów – Dopuszczalność

W sprawie C-746/18

mającej za przedmiot wniosek o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożony przez Riigikohus (sąd najwyższy, Estonia) postanowieniem z dnia 12 listopada 2018 r., które wpłynęło do Trybunału w dniu 29 listopada 2018 r., w postępowaniu karnym przeciwko

H.K.,

przy udziale:

Prokuratuur,

TRYBUNAŁ (wielka izba),

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

rzecznik generalny: G. Pitruzzella,

sekretarz: C. Strömholm, administratorka,

uwzględniając pisemny etap postępowania i po przeprowadzeniu rozprawy w dniu 15 października 2019 r.,

rozważywszy uwagi, które przedstawili:

– w imieniu H.K. – S. Reinsaar, vandeadvokaat,

– w imieniu Prokuratuur – T. Pern i M. Voogma, w charakterze pełnomocników,

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

* Język postępowania: estoński.

– w imieniu rządu duńskiego – J. Nymann-Lindegren i M.S. Wolff, w charakterze pełnomocników,

– w imieniu Irlandii – M. Browne, G. Hodge i J. Quaney oraz A. Joyce, w charakterze pełnomocników, których wspierał D. Fennelly, barrister,

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

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

– w imieniu rządu węgierskiego – M.Z. Fehér i A. Pokoraczki, w charakterze pełnomocników,

– w imieniu rządu polskiego – B. Majczyna, w charakterze pełnomocnika,

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

– w imieniu rządu fińskiego – J. Heliskoski, w charakterze pełnomocnika,

– w imieniu rządu Zjednoczonego Królestwa – S. Brandon i Z. Lavery, w charakterze pełnomocników, których wspierali G. Facenna, QC, i C. Knight, barrister,

– w imieniu Komisji Europejskiej – początkowo H. Kranenborg, M. Wasmeier, P. Costa de Oliveira i K. Toomus, a następnie H. Kranenborg, M. Wasmeier i E. Randvere, w charakterze pełnomocników,

po zapoznaniu się z opinią rzecznika generalnego na posiedzeniu w dniu 21 stycznia 2020 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 złożony w ramach postępowania karnego wszczętego przeciwko H.K. pod zarzutem kradzieży, wykorzystania karty bankowej osoby trzeciej oraz przemocy wobec osób uczestniczących w postępowaniu sądowym.

Ramy prawne

Prawo Unii

3 Motywy 2 i 11 dyrektywy 2002/58 stanowią:

„(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.

[…]

(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 w dniu 4 listopada 1950 r.], dla której wykładnię stanowi orzecznictwo Europejskiego Trybunału Praw Człowieka. Środki tego rodzaju muszą być właściwe, współmierne do zamierzonego celu i niezbędne w ramach społeczeństwa demokratycznego oraz powinny podlegać stosownym zabezpieczeniom zgodnie z Europejską Konwencją o Ochronie Praw Człowieka i Podstawowych Wolności”.

4 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 (dyrektyw[y] ramow[ej]) [(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;

[…]".

5 Zgodnie z art. 5 dyrektywy 2002/58, zatytułowanym „Poufność komunikacji":

„1. Państwa członkowskie zapewniają, poprzez ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. W szczególności zakazują słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników, z wyjątkiem upoważnienia zgodnego z art. 15 ust. 1. Niniejszy ustęp nie zabrania technicznego przechowywania, które jest niezbędne do przekazania komunikatu bez uszczerbku dla zasady poufności.

[…]

3. Państwa członkowskie zapewniają, aby przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym abonenta lub użytkownika było dozwolone wyłącznie pod warunkiem, że dany abonent lub użytkownik wyraził zgodę zgodnie z dyrektywą [95/46] po otrzymaniu jasnych i wyczerpujących informacji, między innymi o celach przetwarzania. Nie stanowi to przeszkody dla 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".

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

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

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

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

[…]

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

[…]”.

7 Artykuł 9 dyrektywy 2002/58, zatytułowany „Dane dotyczące lokalizacji inne niż dane o ruchu”, w ust. 1 przewiduje:

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

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

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

Prawo estońskie

Ustawa o łączności elektronicznej

9 Paragraf 111[1] elektroonilise side seadus (ustawy o łączności elektronicznej, RT I 2004, 87, 593; RT I, 22.05.2018, 3), w brzmieniu mającym zastosowanie do okoliczności faktycznych w postępowaniu głównym (zwanej dalej „ustawą o łączności elektronicznej”), zatytułowany „Obowiązek zatrzymywania danych”, przewiduje:

„[…]

2. Operatorzy usług telefonii stacjonarnej i komórkowej oraz usług sieci telefonii stacjonarnej i telefonii komórkowej są zobowiązani zatrzymywać następujące dane:

1) numer osoby wywołującej oraz nazwę i adres abonenta;

2) numer osoby wywoływanej oraz nazwę i adres abonenta;

3) w wypadku usług dodatkowych takich jak przekazywanie lub przekierowanie połączeń – wybrany numer oraz nazwę i adres abonenta;

4) datę i godzinę rozpoczęcia i zakończenia połączenia;

5) wykorzystaną usługę telefonii stacjonarnej lub komórkowej;

6) międzynarodowy numer tożsamości abonenta mobilnego (International Mobile Subscriber Identity – IMSI) osoby wywołującej i wywoływanej;

7) międzynarodowy identyfikator urządzenia ruchomego (International Mobile Equipment Identity – IMEI) osoby wywołującej i wywoływanej;

8) identyfikator komórki w chwili rozpoczęcia połączenia;

9) dane pozwalające ustalić położenie geograficzne komórki poprzez odniesienie się do identyfikatora komórki w czasie, przez który zatrzymywane są dane;

10) w przypadku anonimowych usług telefonii opłaconych z góry – datę i dokładną godzinę początkowej aktywacji usługi oraz identyfikator lokalizacji, z której dokonano aktywacji usługi.

[…]

4. Dane, o których mowa w ust. 2 i 3 niniejszego paragrafu, są zatrzymywane przez okres jednego roku od dnia połączenia, jeżeli zostały wygenerowane lub przetworzone podczas świadczenia usługi łączności. […]

[…]

11. Dane, o których mowa w ust. 2 i 3 niniejszego paragrafu, są przekazywane:

1) zgodnie z kriminaalmenetluse seadustik [(kodeksem postępowania karnego)] organowi dochodzeniowemu, organowi uprawnionemu do podejmowania środków nadzoru, prokuraturze, sądowi;

[…]”.

Kodeks postępowania karnego

10 Paragraf 17 kodeksu postępowania karnego (kriminaalmenetluse seadustik, RT I 2003, 27, 166; RT I, 31.05.2018, 22) stanowi:

„1. Stronami postępowania sądowego są: prokurator […].

[…]”.

11 Paragraf 30 tego kodeksu ma następujące brzmienie:

„1. Prokuratura kieruje postępowaniem przygotowawczym, zapewniając jego legalność i skuteczność, i pełni funkcję oskarżyciela publicznego przed sądem.

2. Kompetencje prokuratury w ramach postępowania karnego wykonuje w jej imieniu prokurator, który działa w sposób niezależny i związany jest jedynie ustawą”.

12 Paragraf 90^1 wspomnianego kodeksu przewiduje:

„[…]

2. Organ dochodzeniowy może za zgodą prokuratury w toku postępowania przygotowawczego lub za zgodą sądu w toku postępowania sądowego zażądać od przedsiębiorstwa łączności elektronicznej danych wymienionych w § 111^1 ust. 2 i 3 ustawy o łączności elektronicznej, które nie są wymienione w ust. 1 niniejszego paragrafu. Ta zgoda powinna dokładnie wskazywać okres, którego może dotyczyć żądanie danych.

3. Zgodnie z niniejszym paragrafem można żądać danych tylko wówczas, gdy jest to niezbędne do osiągnięcia celu postępowania karnego".

13 Paragraf 211 tego kodeksu stanowi:

„1. Celem postępowania przygotowawczego jest zgromadzenie dowodów i stworzenie pozostałych warunków do przeprowadzenia procesu.

2. W toku postępowania przygotowawczego organ dochodzeniowy i prokuratura ustalają okoliczności obciążające i odciążające podejrzanego lub oskarżonego".

Ustawa o prokuraturze

14 Paragraf 1 prokuratuuriseadus (ustawy o prokuraturze, RT I 1998, 41, 625; RT I, 06.07.2018, 20), w brzmieniu mającym zastosowanie do okoliczności faktycznych w postępowaniu głównym, stanowi:

„1. Prokuratura jest organem rządowym, podległym ministerstwu sprawiedliwości, który bierze udział w planowaniu działań monitorowania niezbędnych do wykrywania i zwalczania przestępstw, kieruje postępowaniem przygotowawczym, zapewniając jego legalność i skuteczność, pełni funkcję oskarżyciela publicznego przed sądem oraz wykonuje inne zadania spoczywające na niej na mocy ustawy.

1^1. Prokuratura wypełnia w sposób niezależny swoje zadania ustawowe i działa na podstawie niniejszej ustawy, innych ustaw i aktów prawnych wydanych na podstawie tych ustaw.

[…]".

15 Paragraf 2 ust. 2 tej ustawy stanowi:

„Prokurator jest niezależny przy wypełnianiu swoich zadań i działa wyłącznie zgodnie z ustawą i własnymi przekonaniami".

Postępowanie główne i pytania prejudycjalne

16 Wyrokiem z dnia 6 kwietnia 2017 r. Viru Maakohus (sąd pierwszej instancji, Viru, Estonia) skazał H.K. na karę dwóch lat pozbawienia wolności za popełnienie w okresie od dnia 17 stycznia 2015 r. do dnia 1 lutego 2016 r. szeregu kradzieży mienia (o wartości od 3 do 40 EUR) i gotówki (w wysokości od 5,20 do 2100 EUR), posługiwanie się kartą bankową osoby trzeciej, co wyrządziło tej osobie szkodę w wysokości 3941,82 EUR, oraz dopuszczenie się przemocy w stosunku do osób uczestniczących w toczącym się wobec niej postępowaniu sądowym.

17 Uznając H.K. za winną popełnienia tych przestępstw, Viru Maakohus (sąd pierwszej instancji, Viru) oparł się między innymi na szeregu protokołów sporządzonych na podstawie danych dotyczących łączności elektronicznej w rozumieniu § 111^1 ust. 2 ustawy o łączności elektronicznej, otrzymanych przez organ dochodzeniowy od dostawcy elektronicznych usług telekomunikacyjnych w toku postępowania przygotowawczego, po uzyskaniu na podstawie § 90^1 kodeksu postępowania karnego

szeregu zezwoleń udzielonych w tym celu przez Viru Ringkonnaprokuratuur (prokuraturę okręgową, Viru, Estonia). Zezwolenia te, udzielone w dniach 28 stycznia 2015 r., 2 lutego 2015 r., 2 listopada 2015 r. oraz 25 lutego 2016 r., odnosiły się do danych dotyczących szeregu numerów telefonów H.K. i różnych międzynarodowych identyfikatorów urządzenia mobilnego H.K. za okres od dnia 1 stycznia do dnia 2 lutego 2015 r., dzień 21 września 2015 r., a także za okres od dnia 1 marca 2015 r. do dnia 19 lutego 2016 r.

18 Od orzeczenia Viru Maakohus (sądu pierwszej instancji, Viru) H.K. wniosła apelację do Tartu Ringkonnakohus (sądu apelacyjnego w Tartu, Estonia), który oddalił tę apelację wyrokiem z dnia 17 listopada 2017 r.

19 Od wyroku tego H.K. wniosła skargę kasacyjną do Riigikohus (sądu najwyższego, Estonia), kwestionując między innymi dopuszczalność protokołów sporządzonych na podstawie danych otrzymanych od dostawcy usług łączności elektronicznej. Jej zdaniem z wyroku z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, zwanego dalej „wyrokiem Tele2", EU:C:2016:970), wynika, że przepisy § 111^1 ustawy o łączności elektronicznej przewidujące zobowiązanie dostawców usług do zatrzymywania danych dotyczących łączności oraz wykorzystanie tych danych do celów jej skazania są sprzeczne z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty.

20 Zdaniem sądu odsyłającego powstaje pytanie, czy protokoły sporządzane na podstawie danych, o których mowa w § 111^1 ust. 2 ustawy o łączności elektronicznej, można uznać za stanowiące dopuszczalne dowody. Sąd ten zauważa, że dopuszczalność protokołów rozpatrywanych w postępowaniu głównym jako dowodów zależy od tego, w jakim stopniu gromadzenie danych, na podstawie których sporządzono te protokoły, było zgodne z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty.

21 Wspomniany sąd uważa, że odpowiedź na to pytanie wymaga ustalenia, czy ów art. 15 ust. 1 w związku z kartą należy interpretować w ten sposób, że dostęp organów państwowych do danych, które pozwalają na ustalenie źródła i odbiorcy połączenia telefonicznego z telefonu stacjonarnego lub komórkowego osoby podejrzanej, ustalenie daty, godziny, czasu trwania i rodzaju tego połączenia oraz użytego urządzenia łączności i lokalizacji użytego urządzenia łączności ruchomej, stanowi na tyle poważną ingerencję w omawiane prawa podstawowe, że dostęp ten powinien być ograniczony do zwalczania poważnej przestępczości, niezależnie od okresu, w odniesieniu do którego organy państwowe zwróciły się o dostęp do zatrzymywanych danych.

22 Sąd odsyłający uważa jednak, że długość tego okresu jest istotnym elementem oceny wagi ingerencji, która polega na dostępie do danych o ruchu i danych o lokalizacji. Tak więc w sytuacji, gdy wspomniany okres jest bardzo krótki lub gdy ilość zebranych danych jest bardzo ograniczona, należałoby zastanowić się nad tym, czy cel polegający na zwalczaniu ogółu przestępczości, a nie tylko zwalczaniu poważnej przestępczości, może uzasadniać taką ingerencję.

23 Wreszcie, sąd odsyłający żywi wątpliwości co do możliwości uznania estońskiej prokuratury za niezależny organ administracyjny w rozumieniu pkt 120 wyroku z dnia 21 grudnia 2016 r., Tele2 (C-203/15 i C-698/15, EU:C:2016:970), który może upoważnić organ dochodzeniowy do dostępu do danych dotyczących łączności elektronicznej, takich jak te, o których mowa w § 111^1 ust. 2 ustawy o łączności elektronicznej.

24 Prokuratura kieruje postępowaniem przygotowawczym, zapewniając jego legalność i skuteczność. Ponieważ celem tego postępowania jest między innymi gromadzenie dowodów, organ dochodzeniowy i prokurator ustalają okoliczności obciążające i odciążające podejrzanego lub oskarżonego. Jeżeli prokuratura jest przekonana, że zostały zebrane wszystkie niezbędne dowody, wnosi ona przeciwko obwinionemu akt oskarżenia. Kompetencje prokuratury są wykonywane w jej imieniu przez prokuratora wykonującego swoje obowiązki w sposób niezależny, jak wynika z § 30 ust. 1 i 2 kodeksu postępowania karnego oraz z §§ 1 i 2 ustawy o prokuraturze.

25 W tym kontekście sąd odsyłający zauważa, że jego wątpliwości co do niezależności wymaganej przez prawo Unii wynikają przede wszystkim z faktu, że prokuratora nie tylko kieruje postępowaniem przygotowawczym, lecz również pełni funkcję oskarżyciela publicznego przed sądem, ponieważ organ ten na mocy prawa krajowego jest stroną postępowania karnego.

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

„1) 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 w postępowaniu karnym dostęp organów państwowych do danych, które pozwalają na ustalenie źródła i odbiorcy połączenia telefonicznego z telefonu stacjonarnego lub komórkowego osoby podejrzanej, ustalenie daty, godziny, czasu trwania i rodzaju tego połączenia oraz użytego urządzenia łączności i lokalizacji użytego urządzenia łączności ruchomej, stanowi na tyle poważną ingerencję w prawa podstawowe gwarantowane wspomnianymi artykułami karty, że dostęp ten musi być ograniczony do zapobiegania, dochodzenia, wykrywania i karania poważnych przestępstw kryminalnych, niezależnie od okresu, w odniesieniu do którego organy państwowe mają dostęp do zatrzymywanych danych?

2) Czy art. 15 ust. 1 dyrektywy [2002/58] należy interpretować w oparciu o zasadę proporcjonalności przywołaną w pkt 55–57 [wyroku z dnia 2 października 2018 r., Ministerio Fiscal (C-207/16, EU:C:2018:788),] w ten sposób, że jeżeli ilość wspomnianych w pytaniu pierwszym danych, do których organy państwowe mają dostęp, nie jest bardzo duża (zarówno pod względem ich rodzaju, jak i długości rzeczonego okresu), wynikająca z tego ingerencja w prawa podstawowe może być uzasadniona w sposób ogólny zapobieganiem, dochodzeniem, wykrywaniem i karaniem przestępstw kryminalnych, i że im większa jest ilość danych, do których mają dostęp organy państwowe, tym poważniejsze muszą być przestępstwa kryminalne, których zwalczaniu ma służyć ingerencja?

3) Czy określony w pkt 2 sentencji [wyroku z dnia 21 grudnia 2016 r., Tele2 (C-203/15 i C-698/15, EU:C:2016:970),] wymóg, by dostęp właściwych organów państwowych do danych był poddany uprzedniej kontroli przez sąd lub niezależny organ administracyjny, oznacza, że art. 15 ust. 1 dyrektywy [2002/58] należy interpretować w ten sposób, iż za niezależny organ administracyjny można uznać prokuraturę, która kieruje postępowaniem przygotowawczym i jest przy tym na mocy ustawy zobowiązana do działania niezależnego, podlegając tylko ustawie, a w ramach postępowania przygotowawczego bada zarówno okoliczności obciążające, jak i odciążające oskarżonego, ale w późniejszym postępowaniu sądowym pełni funkcję oskarżyciela publicznego?”.

W przedmiocie pytań prejudycjalnych

W przedmiocie pytań pierwszego i drugiego

27 Poprzez pytania pierwsze i drugie, które należy rozpatrzyć łącznie, sąd odsyłający dąży w istocie do ustalenia, czy 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, że sprzeciwia się on przepisom krajowym umożliwiającym dostęp organów władzy publicznej do zbioru danych o ruchu lub danych o lokalizacji, które mogą dostarczyć informacji o połączeniach wykonywanych przez użytkownika środka łączności elektronicznej lub o lokalizacji używanego przez niego urządzenia końcowego oraz umożliwić wyciągnięcie precyzyjnych wniosków na temat jego życia prywatnego, do celów zapobiegania, dochodzenia, wykrywania i karania przestępstw, bez ograniczania takiego dostępu do postępowań mających na celu zwalczanie poważnej przestępczości, niezależnie od długości okresu, na jaki wniesiono o dostęp do takich danych, oraz ilości i rodzaju danych dostępnych przez taki okres.

28 W tym względzie z wniosku o wydanie orzeczenia w trybie prejudycjalnym wynika, że – jak potwierdził rząd estoński na rozprawie – dane, do których krajowy organ dochodzeniowy miał dostęp w sprawie w postępowaniu głównym, to dane zatrzymywane na podstawie § 111^1 ust. 2 i 4 ustawy o łączności elektronicznej nakładającej na dostawców usług łączności elektronicznej obowiązek zatrzymywania przez okres jednego roku w sposób ogólny i niezróżnicowany danych o ruchu i danych o lokalizacji w odniesieniu do telefonii stacjonarnej i komórkowej. Dane te pozwalają w szczególności na ustalenie źródła i odbiorcy połączenia telefonicznego z telefonu stacjonarnego lub komórkowego osoby podejrzanej, ustalenie daty, godziny, czasu trwania i rodzaju tego połączenia, użytego urządzenia łączności i lokalizacji telefonu komórkowego bez konieczności przekazywania komunikatu. Co więcej, oferują one możliwość określenia częstotliwości połączeń użytkownika z pewnymi osobami w danym okresie. Ponadto, jak potwierdził rząd estoński na rozprawie, można żądać dostępu do tych danych w ramach zwalczania przestępczości w odniesieniu do wszystkich rodzajów przestępstw.

29 W odniesieniu do warunków, na jakich organy władzy publicznej mogą, do celów zapobiegania, dochodzenia, wykrywania i karania przestępstw, uzyskać dostęp do danych o ruchu i danych o lokalizacji zatrzymywanych przez dostawców usług łączności elektronicznej na podstawie środka podjętego zgodnie z art. 15 ust. 1 dyrektywy 2002/58, Trybunał orzekł, że taki dostęp może zostać przyznany tylko wtedy, gdy dane te są zatrzymywane przez tych dostawców w sposób zgodny ze wspomnianym art. 15 ust. 1 (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 167).

30 W tym względzie Trybunał orzekł również, że wspomniany art. 15 ust. 1 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty stoi na przeszkodzie środkom ustawodawczym przewidującym w tych celach prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji (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 168).

31 Odnośnie do celów mogących uzasadniać dostęp organów władzy publicznej do danych zatrzymywanych przez dostawców usług łączności elektronicznej na podstawie środka zgodnego z tymi przepisami z orzecznictwa Trybunału wynika, po pierwsze, że taki dostęp może być uzasadniony jedynie celem interesu ogólnego, dla którego ci dostawcy usług zostali zobowiązani do takiego zatrzymywania (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 166).

32 Po drugie, Trybunał orzekł, że możliwość uzasadnienia przez państwa członkowskie ograniczenia praw i obowiązków przewidzianych w szczególności w art. 5, 6 i 9 dyrektywy 2002/58 należy oceniać, badając wagę ingerencji, jaką stanowi takie ograniczenie, oraz sprawdzając, 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).

33 Jeśli chodzi o realizowany przez przepisy rozpatrywane w postępowaniu głównym cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu przestępstw, to zgodnie z zasadą proporcjonalności jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniom 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, niezależnie od tego, czy jest ono uogólnione, niezróżnicowane czy ukierunkowane. A zatem jedynie takie ingerencje w omawiane prawa podstawowe, które nie mają poważnego charakteru, mogą być uzasadnione celem polegającym na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu ogółu 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 140, 146).

34 W tym względzie orzeczono w szczególności, że środki ustawodawcze dotyczące przetwarzania danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej jako takich, w szczególności ich zatrzymywanie i dostęp do nich wyłącznie w celu identyfikacji danego użytkownika, bez możliwości powiązania wspomnianych danych z informacjami dotyczącymi wykonywanych połączeń, mogą być uzasadnione celem polegającym na zapobieganiu, dochodzeniu, wykrywaniu i karaniu ogółu przestępstw, do którego odwołuje się art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58. Dane te same w sobie nie pozwalają bowiem na poznanie daty, godziny, czasu trwania i odbiorców wykonywanych połączeń ani też miejsc, w których połączenia te się odbyły, lub ich częstotliwości z określonymi osobami w danym okresie, a więc nie dostarczają one, poza ich danymi kontaktowymi takimi jak adresy, żadnych informacji dotyczących danych połączeń, a w konsekwencji ich życia prywatnego. A zatem ingerencji, jaką pociąga za sobą środek dotyczący tych danych, nie można co do zasady uważać za poważną (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 157, 158 i przytoczone tam orzecznictwo).

35 W tych okolicznościach jedynie cele w postaci zwalczania poważnej przestępczości lub zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego mogą uzasadniać dostęp organów władzy publicznej do zbioru danych o ruchu lub danych o lokalizacji, które mogą dostarczyć informacji o połączeniach wykonywanych przez użytkownika środka łączności elektronicznej lub o lokalizacji używanych przez niego urządzeń końcowych i umożliwiają wyciągnięcie precyzyjnych wniosków na temat życia prywatnego osób, których dane dotyczą (zob. podobnie wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 54), przy czym inne czynniki związane z proporcjonalnością wniosku o udzielenie dostępu, takie jak długość okresu, na jaki wniesiono o dostęp do takich danych, nie mogą skutkować tym, by cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i karaniu ogółu przestępstw mógł uzasadniać taki dostęp.

36 Należy zauważyć, że dostęp do zbioru danych o ruchu lub danych o lokalizacji, takich jak dane zatrzymywane na podstawie § 111^1 ustawy o łączności elektronicznej, może rzeczywiście pozwolić na wyciągnięcie precyzyjnych, a nawet 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, podejmowane czynności, relacje towarzyskie i środowiska społeczne, w których osoby te się obracają (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 117).

37 Prawdą jest, jak sugeruje sąd odsyłający, że im dłuższy jest okres, na jaki wniesiono o dostęp, tym większa jest co do zasady ilość danych, które mogą być zatrzymywane przez dostawców usług łączności elektronicznej i które dotyczą zrealizowanych połączeń elektronicznych, miejsc pobytu oraz przemieszczania się użytkownika środka łączności elektronicznej, co pozwala na wyciągnięcie większej liczby wniosków z poznanych danych na temat życia prywatnego tego użytkownika. Analogiczne stwierdzenie można sformułować również w odniesieniu do kategorii żądanych danych.

38 Zatem w celu spełnienia wymogu proporcjonalności, zgodnie z którym odstępstwa od ochrony danych osobowych i jej ograniczenia muszą mieścić się w ramach tego, co ściśle niezbędne (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), do właściwych organów państwowych należy zapewnienie w każdym indywidualnym przypadku, aby zarówno dana kategoria lub kategorie danych, jak i okres, na jaki wniesiono o dostęp do nich, były, w zależności od okoliczności sprawy, ograniczone do tego, co jest ściśle niezbędne do celów danego dochodzenia.

39 Jednakże ingerencja w prawa podstawowe ustanowione w art. 7 i 8 karty, polegająca na dostępie organu władzy publicznej do zbioru danych o ruchu lub danych o lokalizacji, które mogą dostarczyć informacji na temat połączeń wykonywanych przez użytkownika środka łączności elektronicznej lub lokalizacji używanych przez niego urządzeń końcowych, ma w każdym wypadku poważny charakter, niezależnie od długości okresu, na jaki wnosi się o dostęp do wspomnianych danych, oraz od ilości lub rodzaju

danych dostępnych w takim okresie, jeżeli, tak jak ma to miejsce w sprawie w postępowaniu głównym, ten zbiór danych może pozwolić na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego osoby lub osób, których dane dotyczą.

40 W tym względzie nawet dostęp do ograniczonej ilości danych o ruchu lub danych o lokalizacji lub dostęp do danych na krótki okres może dostarczyć dokładnych informacji na temat życia prywatnego użytkownika środka łączności elektronicznej. Ponadto ilość dostępnych danych i wynikające z nich konkretne informacje na temat życia prywatnego osoby, której dane dotyczą, są okolicznościami, które można ocenić dopiero po zapoznaniu się ze wspomnianymi danymi. Tymczasem zezwolenie na dostęp udzielone przez sąd lub właściwy niezależny organ ma siłą rzeczy miejsce przed zapoznaniem się z danymi i wynikającymi z nich informacjami. Ocena wagi ingerencji, jaką stanowi dostęp, musi być zatem dokonywana w oparciu o ryzyko dla życia prywatnego zainteresowanych osób, które jest ogólnie związane z kategorią żądanych danych, przy czym nie ma ponadto znaczenia, czy wynikające z nich informacje dotyczące życia prywatnego mają, konkretnie rzecz biorąc, poufny charakter, czy też nie.

41 Wreszcie, biorąc pod uwagę fakt, że do sądu odsyłającego zwrócono się z wnioskiem o stwierdzenie niedopuszczalności protokołów sporządzonych na podstawie danych o ruchu i danych o lokalizacji, ze względu na to, że przepisy § 111^1 ustawy o łączności elektronicznej są sprzeczne z art. 15 ust. 1 dyrektywy 2002/58 zarówno w odniesieniu do zatrzymywania danych, jak i dostępu do nich, należy przypomnieć, że w obecnym stanie prawa Unii wyłącznie do prawa krajowego należy co do zasady określenie przepisów dotyczących dopuszczalności i oceny, w ramach postępowania karnego wszczętego przeciwko osobom podejrzanym o popełnienie przestępstw, informacji i dowodów uzyskanych w wyniku takiego uogólnionego i niezróżnicowanego zatrzymywania danych sprzecznego z prawem Unii (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 222), lub w wyniku sprzecznego z tym prawem dostępu organów państwowych do tych danych.

42 Z utrwalonego orzecznictwa wynika bowiem, że w braku uregulowań Unii w tej dziedzinie do wewnętrznego porządku prawnego każdego państwa członkowskiego należy, zgodnie z zasadą autonomii proceduralnej, określenie zasad proceduralnych dotyczących środków prawnych mających na celu zapewnienie ochrony uprawnień podmiotów prawa wynikających z prawa Unii, pod warunkiem jednak, że nie są one mniej korzystne niż przepisy regulujące podobne sytuacje podlegające prawu wewnętrznemu (zasada równoważności) i że nie czynią one w praktyce niemożliwym lub nadmiernie utrudnionym wykonywania uprawnień wynikających z prawa Unii (zasada skuteczności) (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 223 i przytoczone tam orzecznictwo).

43 Co się tyczy w szczególności zasady skuteczności, należy przypomnieć, że krajowe przepisy dotyczące dopuszczalności i wykorzystywania informacji i dowodów mają na celu, zgodnie z wyborem dokonanym w prawie krajowym, uniknięcie sytuacji, w której informacje i dowody uzyskane w sposób niezgodny z prawem wyrządzałyby nienależnie szkodę osobie podejrzanej o popełnienie przestępstw. Tymczasem cel ten można zgodnie z prawem krajowym osiągnąć nie tylko poprzez zakaz wykorzystywania takich informacji i dowodów, lecz również przez krajowe przepisy i praktyki regulujące ocenę i wyważenie informacji i dowodów, a nawet poprzez uwzględnienie ich bezprawnego charakteru w ramach ustalania kary (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 225).

44 Konieczność wykluczenia informacji i dowodów uzyskanych z naruszeniem przepisów prawa Unii należy oceniać w szczególności w świetle zagrożenia, jakie dopuszczalność takich informacji i dowodów stwarza dla poszanowania zasady kontradyktoryjności, a tym samym prawa do rzetelnego procesu. Sąd, który uważa, że strona nie jest w stanie skutecznie przedstawić stanowiska co do środka dowodowego, który należy do dziedziny niepodlegającej rozpoznaniu przez sąd i który może mieć decydujący wpływ na ocenę okoliczności faktycznych, powinien stwierdzić naruszenie prawa do rzetelnego procesu i wykluczyć ten środek dowodowy, aby uniknąć takiego naruszenia. W związku

z tym zasada skuteczności nakłada na krajowy sąd karny obowiązek nieuwzględniania informacji i dowodów uzyskanych w drodze uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji niezgodnego z prawem Unii lub też w drodze sprzecznego z tym prawem dostępu właściwego organu do tych danych, w ramach postępowania karnego wszczętego przeciwko osobom podejrzanym o popełnienie przestępstwa, jeżeli osoby te nie są w stanie skutecznie ustosunkować się do tych informacji i dowodów, należących do dziedziny niepodlegającej rozpoznaniu przez sąd i mogących mieć decydujący wpływ na ocenę okoliczności faktycznych (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 226, 227).

45 W świetle powyższych rozważań na pytania pierwsze i drugie 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, że sprzeciwia się on przepisom krajowym umożliwiającym dostęp organów władzy publicznej do zbioru danych o ruchu lub danych o lokalizacji, które mogą dostarczyć informacji o połączeniach wykonywanych przez użytkownika środka łączności elektronicznej lub o lokalizacji używanego przez niego urządzenia końcowego oraz umożliwić wyciągnięcie precyzyjnych wniosków na temat jego życia prywatnego, do celów zapobiegania, dochodzenia, wykrywania i karania przestępstw, bez ograniczania takiego dostępu do postępowań mających na celu zwalczanie poważnej przestępczości lub zapobieganie poważnym zagrożeniom bezpieczeństwa publicznego, niezależnie od długości okresu, na jaki wniesiono o dostęp do takich danych, oraz ilości lub rodzaju danych dostępnych przez taki okres.

W przedmiocie pytania trzeciego

46 Poprzez pytanie trzecie sąd odsyłający dąży w istocie do ustalenia, czy 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, że sprzeciwia się on przepisom krajowym przyznającym prokuraturze, której zadaniem jest kierowanie postępowaniem przygotowawczym oraz sprawowanie, w stosownych przypadkach, funkcji oskarżyciela publicznego w ramach późniejszego postępowania, kompetencję do udzielania zezwoleń na dostęp organu władzy publicznej do danych o ruchu i danych o lokalizacji do celów postępowania przygotowawczego.

47 Sąd odsyłający wyjaśnia w tym względzie, że o ile zgodnie z prawem krajowym estońska prokuratura jest zobowiązana do działania w sposób niezależny, podlega wyłącznie ustawie i ma obowiązek zbadania w toku postępowania przygotowawczego okoliczności obciążających i odciążających, to jednak celem tego postępowania pozostaje zgromadzenie dowodów, a także stworzenie pozostałych warunków niezbędnych do przeprowadzenia procesu. Ten sam organ pełni funkcję oskarżyciela publicznego przed sądem, a zatem jest on również stroną postępowania. Ponadto z akt sprawy, którymi dysponuje Trybunał, wynika – jak potwierdziły to również rząd estoński i Prokuratuur na rozprawie – że estońska prokuratura jest zorganizowana w sposób hierarchiczny oraz że wnioski o dostęp do danych o ruchu i danych o lokalizacji nie podlegają szczególnym wymogom formalnym i mogą zostać złożone przez samego prokuratora. Wreszcie, osobami, których dane mogą zostać udostępnione, nie są jedynie osoby podejrzane o udział w popełnieniu przestępstwa.

48 Prawdą jest, jak już orzekł Trybunał, że do prawa krajowego należy określenie warunków, na jakich dostawcy usług łączności elektronicznej powinni udzielać właściwym organom państwowym dostępu do danych będących w ich posiadaniu. Jednakże, aby spełnić wymóg proporcjonalności, takie uregulowanie musi zawierać jasne i precyzyjne przepisy regulujące zakres i sposób stosowania rozpatrywanego środka oraz ustanawiające minimalne wymogi służące temu, aby osoby, o których dane osobowe chodzi, miały wystarczające gwarancje pozwalające na skuteczną ochronę tych danych przed ryzykiem nadużyć. To uregulowanie musi być prawnie wiążące w prawie wewnętrznym i 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 (zob. podobnie wyroki: z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15,

EU:C:2016:970, pkt 117, 118; z dnia 6 października 2020 r., Privacy International, C-623/17, EU:C:2020:790, pkt 68; 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 132 i przytoczone tam orzecznictwo).

49 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 warunki materialne i proceduralne regulujące to wykorzystanie (wyroki z dnia 6 października 2020 r.: Privacy International, C-623/17, EU:C:2020:790, pkt 77; a także La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 176 i przytoczone tam orzecznictwo).

50 I tak, jeśli powszechnego dostępu do zatrzymanych danych, niezależnie od jakiegokolwiek związku, nawet pośredniego, z realizowanym celem, nie można uważać za ograniczony do tego, co absolutnie konieczne, rozpatrywane przepisy krajowe winny opierać się na obiektywnych kryteriach umożliwiających określenie okoliczności i warunków przyznania dostępu właściwym organom państwowym do omawianych danych. W tym względzie, biorąc pod uwagę 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 (zob. podobnie wyroki: z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 119; 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 188).

51 W celu zapewnienia w praktyce pełnej zgodności z tymi warunkami ważne jest, aby dostęp właściwych organów państwowych 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, wykrywanie lub karanie przestępstw. W pilnych i należycie uzasadnionych przypadkach kontrola powinna nastąpić w krótkim czasie (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 189 i przytoczone tam orzecznictwo).

52 Ta uprzednia kontrola wymaga między innymi, jak zauważył zasadniczo rzecznik generalny w pkt 105 opinii, aby sąd lub organ odpowiedzialny za przeprowadzenie wspomnianej uprzedniej kontroli dysponował wszelkimi uprawnieniami i gwarancjami niezbędnymi do pogodzenia poszczególnych wchodzących w grę interesów i praw. Jeśli chodzi w szczególności o dochodzenie karne, taka kontrola wymaga, aby ten sąd lub ten organ był w stanie zapewnić właściwą równowagę pomiędzy z jednej strony 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.

53 Jeżeli kontrola ta jest dokonywana nie przez sąd, lecz przez niezależny organ administracyjny, musi on posiadać status pozwalający mu działać przy wykonywaniu swoich obowiązków w sposób obiektywny i bezstronny i w tym celu powinien pozostawać poza jakimkolwiek wpływem z zewnątrz [zob. podobnie wyrok z dnia 9 marca 2010 r., Komisja/Niemcy, C-518/07, EU:C:2010:125, pkt 25; a także opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 229, 230].

54 Z powyższych rozważań wynika, że wymóg niezależności, który powinien spełnić organ odpowiedzialny za przeprowadzenie uprzedniej kontroli, o którym mowa w pkt 51 niniejszego wyroku, 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, jak zauważył zasadniczo rzecznik generalny w pkt 126 opinii, że organ odpowiedzialny za tę uprzednią kontrolę, po pierwsze, nie jest zaangażowany w prowadzenie omawianego dochodzenia karnego, a po drugie, zajmuje neutralną pozycję wobec stron postępowania karnego.

55 Nie jest tak w przypadku prokuratury, która kieruje dochodzeniem i w stosownych przypadkach sprawuje funkcję oskarżyciela publicznego. Prokuratura ma bowiem za zadanie nie rozstrzyganie sporu przy zachowaniu całkowitej niezależności, ale, ewentualnie, jako strona postępowania, która wnosi akt oskarżenia, skierowanie sporu do właściwego sądu.

56 Okoliczność, że prokuratura, zgodnie z przepisami regulującymi jej kompetencje i status, jest zobowiązana do weryfikacji okoliczności obciążających i odciążających, do zapewnienia zgodności z prawem postępowania przygotowawczego i działania wyłącznie zgodnie z ustawą i własnymi przekonaniami, nie może wystarczyć do przyznania jej statusu strony trzeciej w stosunku do spornych interesów w rozumieniu opisanym w pkt 52 niniejszego wyroku.

57 Wynika z tego, że prokuratora nie jest w stanie przeprowadzić uprzedniej kontroli, o której mowa w pkt 51 niniejszego wyroku.

58 Ponieważ sąd odsyłający podniósł ponadto kwestię, czy brak kontroli przeprowadzonej przez niezależny organ można uzupełnić w drodze późniejszej kontroli dokonanej przez sąd krajowy w zakresie zgodności z prawem dostępu organu państwowego do danych o ruchu i danych o lokalizacji, należy zauważyć, że – jak wymaga tego orzecznictwo przypomniane w pkt 51 niniejszego wyroku – niezależna kontrola powinna mieć miejsce przed uzyskaniem wszelkiego dostępu, z wyjątkiem pilnych i należycie uzasadnionych przypadków, w których powinna ona nastąpić w krótkim czasie. Jak zauważył rzecznik generalny w pkt 128 opinii, taka późniejsza kontrola nie pozwoliłaby na realizację celu uprzedniej kontroli, polegającego na uniemożliwieniu udzielania zezwoleń na dostęp do rozpatrywanych danych, który wykracza poza granice tego, co ściśle niezbędne.

59 W tych okolicznościach na pytanie trzecie 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, że sprzeciwia się on przepisom krajowym przyznającym prokuraturze, której zadaniem jest kierowanie postępowaniem przygotowawczym oraz sprawowanie, w stosownych przypadkach, funkcji oskarżyciela publicznego w ramach późniejszego postępowania, kompetencję do udzielania zezwoleń na dostęp organu władzy publicznej do danych o ruchu i danych o lokalizacji do celów postępowania przygotowawczego.

W przedmiocie kosztów

60 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 Parlamentu Europejskiego i Rady 2009/136/WE 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 sprzeciwia się on przepisom krajowym umożliwiającym dostęp organów władzy publicznej do zbioru danych o ruchu lub danych o lokalizacji, które mogą dostarczyć informacji o połączeniach wykonywanych przez użytkownika środka łączności elektronicznej lub o lokalizacji używanego przez niego urządzenia końcowego oraz umożliwić wyciągnięcie precyzyjnych wniosków na temat jego życia prywatnego, do celów zapobiegania, dochodzenia, wykrywania i karania przestępstw, bez ograniczania takiego dostępu do postępowań mających na celu zwalczanie poważnej przestępczości lub zapobieganie poważnym zagrożeniom bezpieczeństwa publicznego, niezależnie od długości okresu, na jaki wniesiono o dostęp do takich danych, oraz ilości lub rodzaju danych dostępnych przez taki okres.

2) **Artykuł 15 ust. 1 dyrektywy 2002/58, zmienionej dyrektywą 2009/136, w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty praw podstawowych należy interpretować w ten sposób, że sprzeciwia się on przepisom krajowym przyznającym prokuraturze, której zadaniem jest kierowanie postępowaniem przygotowawczym oraz sprawowanie, w stosownych przypadkach, funkcji oskarżyciela publicznego w ramach późniejszego postępowania, kompetencję do udzielania zezwoleń na dostęp organu władzy publicznej do danych o ruchu i danych o lokalizacji do celów postępowania przygotowawczego.**

Podpisy