WYROK TRYBUNAŁU (wielka izba)

z dnia 6 października 2020 r.(*)

[Tekst sprostowany postanowieniem z dnia 16 listopada 2020 r.]

Spis treści

Odesłanie prejudycjalne – Przetwarzanie danych osobowych w sektorze łączności elektronicznej – Dostawcy usług łączności elektronicznej – Dostawcy usług hostingowych i dostawcy dostępu do Internetu – Uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji – Zautomatyzowana analiza danych – Dostęp do danych w czasie rzeczywistym – Ochrona bezpieczeństwa narodowego i walka z terroryzmem – Zwalczanie przestępczości – Dyrektywa 2002/58/WE – Zakres stosowania – Artykuł 1 ust. 3 i art. 3 – Poufność łączności elektronicznej – Ochrona – Artykuł 5 i art. 15 ust. 1 – Dyrektywa 2000/31/WE – Zakres stosowania – Karta praw podstawowych Unii Europejskiej – Artykuły 4, 6–8 i 11 oraz art. 52 ust. 1 – Artykuł 4 ust. 2 TUE

W sprawach połączonych C-511/18, C-512/18 i C-520/18,

mających za przedmiot wnioski o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożone przez Conseil d'État (radę stanu, Francja) postanowieniami z dnia 26 lipca 2018 r., które wpłynęły do Trybunału w dniu 3 sierpnia 2018 r. (C-511/18 i C-512/18), oraz przez Cour constitutionnelle (trybunał konstytucyjny, Belgia) postanowieniem z dnia 19 lipca 2018 r., które wpłynęło do Trybunału w dniu 2 sierpnia 2018 r. (C-520/18), w postępowaniach:

**La Quadrature du Net** (C-511/18 i C-512/18),

**French Data Network** (C-511/18 i C-512/18),

**Fédération des fournisseurs d'accès à Internet associatifs** (C-511/18 i C-512/18),

**Igwan.net** (C-511/18)

przeciwko

**Premier ministre** (C-511/18 i C-512/18),

**Garde des Sceaux, ministre de la Justice** (C-511/18 i C-512/18),

**Ministre de l'Intérieur** (C-511/18),

**Ministre des Armées** (C-511/18), przy udziale:

**Privacy International** (C-512/18),

**Center for Democracy and Technology** (C-512/18),

oraz

**Ordre des barreaux francophones et germanophone,**

**Académie Fiscale ASBL,**

**UA,**

**Liga voor Mensenrechten ASBL,**

**Ligue des Droits de l'Homme ASBL,**

**VZ,**

**WY,**

**XX**

przeciwko

**Conseil des ministres,**

przy udziale:

**Child Focus** (C-520/18),

TRYBUNAŁ (wielka izba),

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

rzecznik generalny: M. Campos Sánchez-Bordona,

sekretarz: C. Strömholm, administratorka,

uwzględniając pisemny etap postępowania i po przeprowadzeniu rozprawy w dniach 9 i 10 września 2019 r.,

rozważywszy uwagi, które przedstawili:

– w imieniu Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net i Center for Democracy and Technology – A. Fitzjean Ò Cobhthaigh, avocat,

– w imieniu French Data Network – Y. Padova, avocat,

– w imieniu Privacy International – H. Roy, avocat,

– w imieniu Ordre des barreaux francophones et Germanophone – E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart i J.-F. Henrotte, avocats,

– w imieniu Académie Fiscale ASBL i UA – J.-P. Riquet,

– w imieniu Liga voor Mensenrechten ASBL – J. Vander Velpen, avocat,

– w imieniu Ligue des Droits de l'Homme ASBL – R· Jespers i J. Fermon, avocats,

– w imieniu VZ, WY i XX – D. Pattyn, avocat,

– w imieniu Child Focus – N. Buisseret, K. De Meester i J. Van Cauter, avocats,

– w imieniu rządu francuskiego – początkowo D. Dubois, F. Alabrune i D. Colas oraz E. de

Moustier i A.-L. Desjonquères, następnie D. Dubois i F. Alabrune oraz E. de Moustier i A.-L. Desjonquères, w charakterze pełnomocników,

– w imieniu rządu belgijskiego – J.-C. Halleux i P. Cottin oraz C. Pochet, w charakterze pełnomocników, których wspierały J. Vanpraet, Y. Peeters, S. Depré i E. de Lophem, avocats,

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

– w imieniu rządu duńskiego – początkowo J. Nymann-Lindegren oraz M. Wolff i P. Ngo, następnie J. Nymann-Lindegren i M. Wolff, w charakterze pełnomocników,

– w imieniu rządu niemieckiego – początkowo J. Möller, M. Hellmann, E. Lankenau, R. Kanitz i T. Henze, następnie J. Möller, M. Hellmann, E. Lankenau i R. Kanitz, w charakterze pełnomocników,

– w imieniu rządu estońskiego – N. Grünberg i A. Kalbus, w charakterze pełnomocników,

– w imieniu rządu irlandzkiego – A. Joyce oraz M. Browne i G. Hodge, w charakterze pełnomocników, których wspierał D. Fennelly, BL,

– w imieniu rządu hiszpańskiego – początkowo L. Aguilera Ruiz i A. Rubio González, następnie L. Aguilera Ruiz, w charakterze pełnomocników,

– w imieniu rządu cypryjskiego – E. Neofytou, w charakterze pełnomocnika,

– w imieniu rządu łotewskiego – V. Soņeca, w charakterze pełnomocnika,

– w imieniu rządu węgierskiego – początkowo M.Z. Fehér i Z. Wagner, następnie M.Z. Fehér, w charakterze pełnomocnika,

– w imieniu rządu niderlandzkiego – M.K. Bulterman i A.M. de Ree, w charakterze pełnomocników,

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

– w imieniu rządu szwedzkiego – początkowo H. Shev, H. Eklinder, C. Meyer-Seitz oraz A. Falk, następnie H. Shev, H. Eklinder, C. Meyer-Seitz i J. Lundberg, w charakterze pełnomocników,

– w imieniu rządu Zjednoczonego Królestwa – S. Brandon, w charakterze pełnomocnika, którego wspierali G. Facenna, QC, i C. Knight, barrister,

– [tiret usunięte postanowieniem z dnia 16 listopada 2020 r.],

– w imieniu Komisji Europejskiej – początkowo H. Kranenborg i M. Wasmeier oraz P. Costa de Oliveira, następnie H. Kranenborg i M. Wasmeier, w charakterze pełnomocników,

– w imieniu Europejskiego Inspektora Ochrony Danych – T. Zerdick i A. Buchta, w charakterze pełnomocników,

po zapoznaniu się z opinią rzecznika generalnego na posiedzeniu w dniu 15 stycznia 2020 r.,

wydaje następujący

**Wyrok**

1 Wnioski o wydanie orzeczenia w trybie prejudycjalnym dotyczą wykładni z jednej strony art. 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. 2002, L 201, s. 37), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. (Dz.U. 2009, L 337, s. 11) (zwanej dalej „dyrektywą 2002/58"), i z drugiej strony art. 12–15 dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.U. 2000, L 178, s. 1), w związku z art. 4, 6–8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą") i art. 4 ust. 2 TUE.

2 Wniosek w sprawie C-511/18 złożono w ramach sporu pomiędzy Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs i Igwan.net a Premier ministre (premierem, Francja), Garde des Sceaux, ministre de la Justice (ministrem sprawiedliwości, Francja), ministre de l'Intérieur (ministrem spraw wewnętrznych, Francja) i ministre des Armées (ministrem obrony, Francja) dotyczącego zgodności z prawem décret nº 2015-1185, du 28 septembre 2015, portant désignation des services spécialisés de renseignement (dekretu nr 2015-1185 z dnia 28 września 2015 r. w sprawie powołania wyspecjalizowanych służb wywiadowczych, JORF z dnia 29 września 2015 r., tekst 1 z 97, zwanego dalej „dekretem nr 2015-1185"), décret nº 2015-1211, du 1er octobre 2015, relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (dekretu nr 2015-1211 z dnia 1 października 2015 r. w sprawie sporów dotyczących wdrażania technik wywiadowczych podlegających procedurze udzielania zezwoleń i plików dotyczących bezpieczeństwa narodowego, JORF z dnia 2 października 2015 r., tekst 7 z 108, zwanego dalej „dekretem nr 2015-1211"), décret nº 2015-1639, du 11 décembre 2015, relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure (dekretu nr 2015-1639 z dnia 11 grudnia 2015 r. w sprawie wyznaczenia służb innych niż wyspecjalizowane służby wywiadowcze, upoważnionych do stosowania technik określonych w tytule V księgi VIII kodeksu bezpieczeństwa wewnętrznego, wydanego na podstawie art. L. 811-4 kodeksu bezpieczeństwa wewnętrznego, JORF z dnia 12 grudnia 2015 r., tekst 28 z 127, zwanego dalej „dekretem nr 2015-1639"), oraz décret nº 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement (dekretu nr 2016-67 z dnia 29 stycznia 2016 r. w sprawie technik gromadzenia danych wywiadowczych, JORF z dnia 31 stycznia 2016 r., tekst 2 z 113, zwanego dalej „dekretem 2016-67").

3 Wniosek w sprawie C-512/18 złożono w ramach sporu pomiędzy French Data Network, Quadrature du Net i Fédération des fournisseurs d'accès à Internet associatifs a Premier ministre (premierem, Francja) i Garde des Sceaux, ministre de la justice (ministrem sprawiedliwości, Francja) dotyczącego zgodności z prawem art. R. 10-13 code des postes et des communications électroniques (kodeksu poczty i łączności elektronicznej, zwanego dalej „CPCE") i décret nº 2011-219, du 25 février 2011, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (dekretu nr 2011-219 z dnia 25 lutego 2011 r. w sprawie zatrzymywania i udostępniania danych umożliwiających identyfikację każdej osoby, która przyczyniła się do stworzenia treści umieszczonych w Internecie, JORF z dnia 1 marca 2011 r., tekst 32 z 170, zwanego dalej „dekretem nr 2011-219").

4 Wniosek w sprawie C-520/18 został złożony w ramach sporu pomiędzy Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY i XX a Conseil des ministres (radą ministrów, Belgia) dotyczącego zgodności z prawem loi du 29 mai 2016 relative à la collecte et à la

conservation des données dans le secteur des communications électroniques (ustawy z dnia 29 maja 2016 r. o zbieraniu i zatrzymywaniu danych w sektorze łączności elektronicznej, *Moniteur belge* z dnia 18 lipca 2016 r., s. 44717, zwanej dalej „ustawą z dnia 29 maja 2016 r.”).

## Ramy prawne

### *Prawo Unii*

*Dyrektywa 95/46*

5 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) została zastąpiona ze skutkiem od dnia 25 maja 2018 r. rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnym rozporządzeniem o ochronie danych) (Dz.U. 2016, L 119, s. 1; sprostowanie Dz.U. 2018, L 127, s. 2). Artykuł 3 ust. 2 dyrektywy 95/46 stanowił:

„Niniejsza dyrektywa nie ma zastosowania do przetwarzania danych osobowych:

– w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. dane, o których stanowi tytuł V i VI Traktatu o Unii Europejskiej, a w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarcza państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności państwa w obszarach prawa karnego,

– przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze”.

6 Artykuł 22 dyrektywy 95/46, zawarty w rozdziale III tej dyrektywy, zatytułowany „Środki sądowe”, miał następujące brzmienie:

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

*Dyrektywa 97/66*

7 Zgodnie z art. 5 dyrektywy 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze telekomunikacyjnym (Dz.U. 1997, L 24, s. 1), zatytułowanym „Poufność komunikacji”:

„1. Państwa członkowskie zapewniają, poprzez ustawodawstwo krajowe, poufność komunikacji prowadzonej za pomocą publicznej sieci telekomunikacyjnej i publicznie dostępnych usług telekomunikacyjnych. W szczególności zakazują słuchania, przechwytywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników, z art. 14 ust. 1.

2. Ustęp 1 nie ma wpływu na prawnie dozwolone rejestrowanie komunikatów w ramach zgodnego z prawem użytku zawodowego w celu dostarczenia dowodu na operacje handlowe lub innego rodzaju komunikacji handlowej” [tłumaczenie nieoficjalne].

*Dyrektywa 2000/31*

8 Motywy 14 i 15 dyrektywy 2000/31 przewidują:

„(14) Ochrona osób fizycznych w odniesieniu do przetwarzania danych osobowych regulowana jest wyłącznie dyrektywą [95/46] oraz dyrektywą [97/66], które mają pełne zastosowanie do usług społeczeństwa informacyjnego; dyrektywy te stanowią już wspólnotowe ramy prawne w dziedzinie danych osobowych, dlatego nie jest konieczne obejmowanie tego zagadnienia niniejszą dyrektywą w celu zapewnienia sprawnego funkcjonowania rynku wewnętrznego, w szczególności swobodnego przepływu danych osobowych między państwami członkowskimi; wykonanie i stosowanie niniejszej dyrektywy powinny być całkowicie zgodne z zasadami odnoszącymi się do ochrony danych osobowych, w szczególności w odniesieniu do niezamawianych informacji handlowych oraz odpowiedzialności pośredników; niniejsza dyrektywa nie może uniemożliwiać anonimowego korzystania z otwartych sieci, takich jak Internet.

(15) Poufność porozumiewania się zapewniona jest przez art. 5 dyrektywy [97/66]; zgodnie z tą dyrektywą państwa członkowskie muszą zakazać wszystkich rodzajów niedozwolonego podsłuchu lub nadzorowania takiego porozumiewania się przez osoby inne niż nadawcy i odbiorcy, z wyjątkiem przypadków, gdy taka działalność jest prawnie dozwolona”.

9 Artykuł 1 dyrektywy 2000/31 ma następujące brzmienie:

„1. Niniejsza dyrektywa dąży do przyczynienia się do właściwego funkcjonowania rynku wewnętrznego przez zapewnienie swobodnego przepływu usług społeczeństwa informacyjnego między państwami członkowskimi.

2. Niniejsza dyrektywa zbliża, w zakresie potrzebnym do osiągnięcia celu określonego w ust. 1, niektóre przepisy krajowe w sprawie usług społeczeństwa informacyjnego odnoszące się do rynku wewnętrznego, siedzib usługodawców, informacji handlowych, umów zawieranych drogą elektroniczną, odpowiedzialności pośredników, kodeksów postępowania, pozasądowych dróg rozstrzygania sporów, dochodzenia praw przed sądem oraz współpracy między państwami członkowskimi.

3. Niniejsza dyrektywa uzupełnia prawo wspólnotowe mające zastosowanie do usług społeczeństwa informacyjnego bez uszczerbku dla poziomu ochrony, w szczególności zdrowia publicznego oraz interesów konsumentów ustanowionego we wspólnotowych aktach prawnych oraz wykonujących je ustawodawstwach krajowych w zakresie, w jakim nie ogranicza to swobody świadczenia usług społeczeństwa informacyjnego.

[…]

5. Niniejsza dyrektywa nie ma zastosowania do:

[…]

b) zagadnień odnoszących się do usług społeczeństwa informacyjnego objętych dyrektywami [95/46] oraz [97/66];

[…]”.

10 Artykuł 2 dyrektywy 2000/31 ma następujące brzmienie:

„Do celów niniejszej dyrektywy następujące pojęcia oznaczają:

a) »usługi społeczeństwa informacyjnego«: usługi w rozumieniu art. 1 ust. 2 dyrektywy 98/34/WE [Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998 r. ustanawiającej procedurę udzielania informacji w zakresie norm i przepisów technicznych (Dz.U. 1998, L 204, s. 37)], zmienionej dyrektywą 98/48/WE [Parlamentu Europejskiego i Rady z dnia 20 lipca 1998 r.

(Dz.U. 1998, L 217, s. 18];

[…]”.

11 W art. 15 dyrektywy 2000/31 przewidziano:

„1. Państwa członkowskie nie nakładają na usługodawców świadczących usługi określone w art. 12, 13 i 14 ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują ani ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność.

2. Państwa członkowskie mogą ustanowić w stosunku do usługodawców świadczących usługi społeczeństwa informacyjnego obowiązek niezwłocznego powiadamiania właściwych władz publicznych o rzekomych bezprawnych działaniach podjętych przez ich usługobiorców lub przez nich przekazanych informacjach lub obowiązek przekazywania właściwym władzom, na ich żądanie, informacji pozwalających na ustalenie tożsamości ich usługobiorców, z którymi mają umowy o przechowywanie”.

*Dyrektywa 2002/21*

12 Zgodnie z motywem 10 dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywy ramowej) (Dz.U. 2002, L 108, s. 33):

„Definicja »społeczeństwa informacyjnego« zawarta w art. 1 dyrektywy [98/34], [zmienionej dyrektywą 98/48], odnosi się do szeroko pojętej działalności gospodarczej, która może być prowadzona on-line. Większa część takiej działalności nie jest objęta zakresem niniejszej dyrektywy, albowiem działalność ta nie polega w całości czy w przeważającej części na przekazywaniu sygnałów poprzez sieci łączności elektronicznej. Usługi w zakresie telefonii głosowej oraz przekazywania poczty elektronicznej są przedmiotem niniejszej dyrektywy. Jedno i to samo przedsiębiorstwo, np. podmiot świadczący usługi internetowe, może świadczyć usługi łączności elektronicznej w dwóch kategoriach, takich jak świadczenie dostępu do Internetu oraz usług nieobjętych zakresem niniejszej dyrektywy, w tym usług polegających na określaniu treści stron internetowych”.

13 W art. 2 dyrektywy 2002/21 przewidziano:

„Dla celów niniejszej dyrektywy:

[…]

c) »usługa łączności elektronicznej« oznacza usługę zazwyczaj świadczoną za wynagrodzeniem, polegającą całkowicie lub częściowo na przekazywaniu sygnałów w sieciach łączności elektronicznej, w tym usługi telekomunikacyjne i usługi transmisyjne świadczone poprzez sieci nadawcze; nie obejmuje jednak usług związanych z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci lub usług łączności elektronicznej. Spod zakresu niniejszej definicji wyłączone są usługi społeczeństwa informacyjnego w rozumieniu art. 1 dyrektywy [98/34], jeżeli nie polegają one całkowicie lub częściowo na przekazywaniu sygnałów w sieciach łączności elektronicznej;

[…]”.

*Dyrektywa 2002/58*

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

„(2) Niniejsza dyrektywa dąży do poszanowania fundamentalnych praw i jest zgodna z zasadami

uznanymi w szczególności przez [kartę]. 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], nie odnosi się do kwestii ochrony podstawowych praw i wolności związanych z działalnością, która nie jest regulowana prawem wspólnotowym. Dyrektywa nie zmienia zatem istniejącej równowagi między prawem do prywatności osoby fizycznej a możliwością państw członkowskich do podejmowania środków, określonych w art. 15 ust. 1 niniejszej dyrektywy, niezbędnych do ochrony bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając gospodarczy dobrobyt państwa, gdy działania dotyczą zagadnień bezpieczeństwa państwa) i wykonywania prawa karnego. Wskutek tego, niniejsza dyrektywa nie wpływa na 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.

[…]

(22) Zakaz przechowywania komunikatów oraz związanych z nimi danych dotyczących ruchu w sieci przez osoby inne niż użytkownicy lub bez ich zgody nie ma na celu zakazu automatycznego, pośredniego i przejściowego przechowywania takiej informacji wówczas, gdy odbywa się to wyłącznie do celu przeprowadzenia transmisji w sieci łączności elektronicznej, oraz pod warunkiem że informacja nie jest przechowywana przez okres dłuższy niż jest to konieczne w celu wykonania transmisji i zarządzania ruchem, oraz że w okresie przechowywania zagwarantowana zostaje poufność. […]

[…]

(26) Dane dotyczące abonentów przetwarzane w ramach sieci łączności elektronicznej w celu ustanowienia połączenia i przenoszenia informacji zawierają informacje dotyczące prywatnego życia osób fizycznych i dotyczą prawa do poszanowania tajemnicy korespondencji lub dotyczą uzasadnionych interesów osób prawnych. Takie dane mogą być przechowywane tylko przez określony czas i wyłącznie w zakresie umożliwiającym świadczenie usług związanych z naliczaniem opłat i rozliczeń międzyoperatorskich. Wszelkie dalsze przetwarzanie tego rodzaju danych […] może być dozwolone tylko w przypadkach, gdy abonent wyraził na to zgodę na podstawie udzielonej mu przez dostawcę usług dokładnej

i pełnej informacji o rodzajach zamierzonego dalszego przetwarzania oraz prawie abonenta do nieudzielenia zgody na przetwarzanie lub jej odwołania. Dane dotyczące ruchu wykorzystywane w marketingu usług komunikacyjnych […] powinny również zostać usunięte lub uczynione anonimowymi […].

[…]

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

15 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".

16 Zgodnie z art. 2 dyrektywy 2002/58, zatytułowanym „Definicje":

„Z zastrzeżeniem innych przepisów, stosuje się definicje z dyrektywy [95/46] i dyrektywy [2002/21].

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;

[…]".

17 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 we Wspólnocie, włącznie z publicznymi sieciami łączności służącymi do zbierania danych i obsługi urządzeń identyfikacyjnych”.

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

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

[…]

3. Państwa członkowskie zapewniają, aby przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym abonenta lub użytkownika było dozwolone wyłącznie pod warunkiem że dany abonent lub użytkownik wyraził zgodę zgodnie z dyrektywą [95/46] po otrzymaniu jasnych i wyczerpujących informacji, między innymi o celach przetwarzania. Nie stanowi to przeszkody dla każdego technicznego przechowywania danych ani dostępu do nich jedynie w celu wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej, lub gdy jest to ściśle niezbędne w celu świadczenia usługi przez dostawcę usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika”.

19 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”.

20 W art. 9 tej dyrektywy, zatytułowanym „Dane dotyczące lokalizacji inne niż dane o ruchu”,

przewidziano 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 […]”.

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

„1. Państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4 i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (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.

[…]

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

[…]”.

*Rozporządzenie 2016/679*

22 Motyw 10 rozporządzenia 2016/679 stanowi:

„Aby zapewnić wysoki i spójny stopień ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii, należy zapewnić równorzędny we wszystkich państwach członkowskich stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych. Należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych […]”.

23 Artykuł 2 tego rozporządzenia stanowi:

„1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

2. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:

a) w ramach działalności nieobjętej zakresem prawa Unii;

b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;

[…]

d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

[…]

4. Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy [2000/31], w szczególności dla zasad odpowiedzialności usługodawców będących pośrednikami, o których to zasadach mowa w art. 12–15 tej dyrektywy".

24 W art. 4 omawianego rozporządzenia przewidziano:

„Na użytek niniejszego rozporządzenia:

1) »dane osobowe« oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (»osobie, której dane dotyczą«); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

2) »przetwarzanie« oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

[…]".

25 Artykuł 5 rozporządzenia 2016/679 stanowi:

„1. Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (»zgodność z prawem, rzetelność i przejrzystość«);

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami (»ograniczenie celu«);

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (»minimalizacja danych«);

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (»prawidłowość«);

e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez

okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą (»ograniczenie przechowywania«);

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (»integralność i poufność«);

[…]”.

26 Artykuł 6 tego rozporządzenia ma następujące brzmienie:

„1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

[…]

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

[…]

3. Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona:

a) w prawie Unii; lub

b) w prawie państwa członkowskiego, któremu podlega administrator.

Cel przetwarzania musi być określony w tej podstawie prawnej […]. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

[…]”.

27 W art. 23 omawianego rozporządzenia przewidziano:

„1. Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:

a) bezpieczeństwu narodowemu;

b) obronie;

c) bezpieczeństwu publicznemu;

d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;

e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu;

f) ochronie niezależności sądów i postępowania sądowego;

g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu;

h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a)–e) oraz g);

i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób;

j) egzekucji roszczeń cywilnoprawnych.

2. W szczególności akt prawny, o którym mowa w ust. 1, musi zawierać szczegółowe przepisy przynajmniej – w stosownym przypadku – o:

a) celach przetwarzania lub kategorii przetwarzania;

b) kategoriach danych osobowych;

c) zakresie wprowadzonych ograniczeń;

d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu;

e) określeniu administratora lub kategorii administratorów;

f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania;

g) ryzykach naruszenia praw lub wolności osoby, której dane dotyczą; oraz

h) prawie osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia”.

28 Zgodnie z art. 79 ust. 1 omawianego rozporządzenia:

„Bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego zgodnie z art. 77, każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia”.

29 Zgodnie z art. 94 rozporządzenia 2016/679:

„1. Dyrektywa [95/46] zostaje uchylona ze skutkiem od dnia 25 maja 2018 r.

2. Odesłania do uchylonej dyrektywy należy traktować jako odesłania do niniejszego rozporządzenia. Odesłania do Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, ustanowionej w art. 29 dyrektywy [95/46], należy traktować jako odesłania do Europejskiej Rady Ochrony Danych, ustanowionej niniejszym rozporządzeniem".

30 Artykuł 95 tego rozporządzenia stanowi:

„Niniejsze rozporządzenie nie nakłada dodatkowych obowiązków na osoby fizyczne ani prawne co do przetwarzania w związku ze świadczeniem ogólnodostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii w sprawach, w których podmioty te podlegają szczegółowym obowiązkom mającym ten sam cel określonym w dyrektywie [2002/58]".

***Prawo francuskie***

*Kodeks bezpieczeństwa wewnętrznego*

31 Księga VIII ustawodawczej części kodeksu bezpieczeństwa wewnętrznego (zwanego dalej „CSI") zawiera w art. L. 801-1-L. 898-1 przepisy dotyczące informacji wywiadowczych.

32 L. 811-3 CSI stanowi:

„Wyłącznie w celu wykonywania swoich odpowiednich zadań wyspecjalizowane służby wywiadowcze mogą posługiwać się technikami wymienionymi w tytule V niniejszej księgi dla gromadzenia danych wywiadowczych mających znaczenie dla obronności i wspierania następujących podstawowych interesów narodowych:

1) niepodległość narodowa, integralność terytorialna i obrona narodowa;

2) główne interesy polityki zagranicznej, wypełnianie zobowiązań europejskich i międzynarodowych Francji i zapobieganie wszelkim formom zagranicznej ingerencji;

3) główne interesy gospodarcze, przemysłowe i naukowe Francji;

4) zapobieganie terroryzmowi;

5) zapobieganie:

a) naruszeniom republikańskiej formy instytucji;

b) działaniom zmierzającym do utrzymania lub ponownego utworzenia ugrupowań rozwiązanych w zastosowaniu art. L. 212-1;

c) zbiorowym formom przemocy, które mogłyby poważnie naruszyć spokój publiczny;

6) zapobieganie przestępczości i przestępczości zorganizowanej;

7) zapobieganie rozprzestrzenianiu broni masowego rażenia".

33 Artykuł L. 811-4 CSI stanowi:

„Dekret Conseil d'État (rady stanu, Francja), przyjęty po uzyskaniu opinii krajowej komisji ds. kontroli technik wywiadowczych, wskaże służby, inne niż wyspecjalizowane służby wywiadowcze, podlegające ministrom obrony, spraw wewnętrznych i sprawiedliwości oraz ministrom właściwym w dziedzinie gospodarki, budżetu lub ceł, które mogą uzyskać zezwolenie na posłużenie się technikami wymienionymi w tytule V niniejszej księgi w warunkach przewidzianych w tej księdze. Dla każdej służby dekret wskaże cele wymienione w art. L. 811-3 i techniki, na jakie można udzielić zezwolenia".

34 Artykuł L. 821-1 akapit pierwszy CSI przewiduje, co następuje:

„Stosowanie na terytorium krajowym technik gromadzenia danych wywiadowczych, o których mowa w rozdziałach I-IV tytułu V niniejszej księgi, podlega uprzedniemu zezwoleniu wydanemu przez premiera po uzyskaniu opinii krajowej komisji ds. kontroli technik wywiadowczych”.

35 Artykuł L. 821-2 CSI przewiduje:

„Zezwolenie, o którym mowa w art. L. 821-1, wydaje się na pisemny i uzasadniony wniosek ministra obrony, ministra spraw wewnętrznych, ministra sprawiedliwości lub ministrów właściwych w dziedzinie gospodarki, budżetu lub ceł. Każdy minister może przekazać to uprawnienie indywidualnie tylko bezpośrednim współpracownikom posiadającym klauzulę tajności w dziedzinie obrony narodowej.

We wniosku określa się:

1) technikę lub techniki, które mają być wdrożone;

2) służbę, na rzecz której jest on składany;

3) zamierzony cel lub zamierzone cele;

4) powód lub powody podjęcia środków;

5) okres ważności zezwolenia;

6) osobę lub osoby, miejsce lub miejsca, lub pojazdy, których to dotyczy.

Do celów stosowania pkt 6 osoby, których tożsamość nie jest znana, mogą być oznaczone poprzez ich identyfikatory lub ich cechę, a miejsca lub pojazdy mogą zostać określone poprzez odniesienie do osób, których dotyczy wniosek.

[…]”.

36 Zgodnie z art. L. 821-3 akapit pierwszy CSI:

„Wniosek jest przekazywany prezesowi lub, w razie jego braku, jednemu z członków krajowej komisji ds. kontroli technik wywiadowczych spośród tych, o których mowa w art. L. 831-1 pkt 2 i 3, który przekazuje premierowi opinię w terminie 24 godzin. Jeżeli wniosek jest rozpatrywany przez ograniczony skład lub pełny skład komisji, premier zostaje o tym bezzwłocznie poinformowany i opinię wydaje się w terminie 72 godzin”.

37 Artykuł L. 821-4 CSI stanowi:

„Zezwolenie na stosowanie technik wymienionych w rozdziałach I-IV tytułu V niniejszej księgi wydaje premier na okres nieprzekraczający czterech miesięcy. […] Zezwolenie zawiera uzasadnienie i informacje przewidziane w art. L. 821-2 pkt 1–6. Zezwolenie może zostać odnowione na tych samych warunkach co określone w niniejszym rozdziale.

W przypadku gdy zezwolenie jest wydawane po negatywnej opinii krajowej komisji ds. kontroli technik wywiadowczych, wskazuje się w nim przyczyny, dla których nie oparto się na tej opinii.

[…]”.

38 Artykuł L. 833-4 CSI zawarty w rozdziale III tego tytułu stanowi:

„Komisja z własnej inicjatywy lub w przypadku, gdy jakakolwiek osoba pragnąca sprawdzić, czy

jakaś technika wywiadowcza została wdrożona wobec niej w sposób niezgodny z prawem, złoży zażalenie, przeprowadza kontrolę wskazanej techniki lub technik w celu sprawdzenia, czy są one lub były wdrażane zgodnie z niniejszą księgą. Informuje ona składającego zażalenie o przeprowadzeniu niezbędnych weryfikacji, nie potwierdzając ich wdrażania ani nie zaprzeczając mu".

39 Artykuł L. 841-1 akapity pierwszy i drugi CSI ma następujące brzmienie:

„Z zastrzeżeniem przepisów szczególnych, o których mowa w art. L. 854-9 niniejszego kodeksu, rada stanu jest właściwa do rozpoznawania, na warunkach przewidzianych w rozdziale III bis tytułu VII księgi VII kodeksu postępowania przed sądami administracyjnymi, skarg dotyczących wdrażania technik wywiadowczych wymienionych w tytule V niniejszej księgi.

Skargę może wnieść:

1) każda osoba, która chce sprawdzić, czy jakaś technika wywiadowcza została wdrożona wobec niej w sposób nieprawidłowy i uzasadniający uprzednie przeprowadzenie postępowania przewidzianego w art. L. 833-4;

2) krajowa komisja ds. kontroli technik wywiadowczych w warunkach przewidzianych w art. L. 833-8".

40 Tytuł V księgi VIII części legislacyjnej CSI, dotyczący „technik gromadzenia danych wywiadowczych podlegających obowiązkowi uzyskania zezwolenia", zawiera w szczególności rozdział I, zatytułowany „Dostęp administracyjny do danych o połączeniach", obejmujący art. L. 851-1-L. 851-7 CSI.

41 Artykuł L. 851-1 CSI przewiduje:

„Na warunkach określonych w rozdziale 1 tytułu II niniejszej księgi może być dopuszczone zbieranie od operatorów łączności elektronicznej i osób wymienionych w art. L. 34-1 [CPCE] oraz osób, o których mowa w art. 6 ust. I pkt 1 i 2 loi n.º 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [ustawy nr 2004-575 z dnia 21 czerwca 2004 r. o zaufaniu w gospodarce cyfrowej (JORF z dnia 22 czerwca 2004 r., s. 11168)], informacji lub dokumentów przetwarzanych lub zatrzymywanych w ich sieciach lub w ramach usług łączności elektronicznej, w tym danych technicznych dotyczących identyfikacji numerów abonamentowych lub dostępu do usług łączności elektronicznej, wyliczenia wszystkich numerów abonamentowych lub dostępu do usług łączności elektronicznej wskazanej osoby, lokalizacji wykorzystanych urządzeń końcowych oraz połączeń abonenta odnoszących się do listy numerów przychodzących i wychodzących, czasu trwania i daty połączeń.

W drodze odstępstwa od art. L. 821-2 indywidualnie wyznaczeni i uprawnieni agenci służb wywiadowczych, o których mowa w art. L. 811-2 i L. 811-4, przekazują uzasadnione pisemne wnioski odnoszące się do danych technicznych dotyczących identyfikacji numerów abonamentowych lub połączenia z usługami łączności elektronicznej lub spisu wszystkich numerów abonamentowych lub połączeń oznaczonej osoby bezpośrednio do krajowej komisji ds. kontroli technik wywiadowczych. Komisja wydaje opinię na warunkach określonych w art. L. 821-3.

Służby premiera mają za zadanie gromadzenie informacji lub dokumentów od operatorów i osób, o których mowa w akapicie pierwszym niniejszego artykułu. Krajowa komisja ds. kontroli technik wywiadowczych ma stały, pełny, bezpośredni i natychmiastowy dostęp do zgromadzonych informacji lub dokumentów.

Szczegółowe zasady stosowania niniejszego artykułu określa dekret rady stanu, wydany po zasięgnięciu opinii krajowej komisji ds. informatyki i swobód oraz krajowej komisji ds. kontroli technik wywiadowczych".

42 Artykuł L. 851-2 CSI stanowi:

„I. W okolicznościach przewidzianych w rozdziale I tytułu II niniejszej księgi i wyłącznie na potrzeby zapobiegania terroryzmowi można wydać indywidualne zezwolenie na gromadzenie w czasie rzeczywistym, w sieciach operatorów i osób, o których mowa w art. L. 851-1, informacji lub dokumentów, o których mowa w art. L. 851-1, dotyczących uprzednio zidentyfikowanej osoby, która może mieć związek z zagrożeniem. Jeżeli istnieją poważne podstawy, by sądzić, że jedna lub więcej osób należących do otoczenia osoby, której dotyczy zezwolenie, może dostarczyć informacji związanych z celem uzasadniającym zezwolenie, zezwolenie to może być również udzielone indywidualnie dla każdej z tych osób.

I bis. Maksymalną liczbę jednocześnie obowiązujących zezwoleń wydanych na podstawie niniejszego artykułu określa premier, po zasięgnięciu opinii krajowej komisji ds. kontroli technik wywiadowczych. O decyzji określającej tę maksymalną liczbę i jej podział między ministrów wymienionych w art. L. 821-2 akapit pierwszy, a także o liczbie wydanych zezwoleń na przechwytywanie informuje się komisję.

[…]”.

43 Artykuł L. 851-3 CSI przewiduje:

„I. Na warunkach przewidzianych w rozdziale I tytułu II niniejszej księgi i wyłącznie dla potrzeb zapobiegania terroryzmowi można zobowiązać operatorów i osoby wymienione w art. L. 851-1 do wdrożenia w swoich sieciach operacji automatycznego przetwarzania, na podstawie parametrów określonych w zezwoleniu, zmierzających do wykrycia połączeń, które mogą wskazywać na zagrożenie terrorystyczne.

Takie automatyczne przetwarzanie wykorzystuje wyłącznie informacje lub dokumenty, o których mowa w art. L. 851-1, bez gromadzenia innych danych niż te, które odpowiadają ich parametrom projektowym, i bez umożliwienia identyfikacji osób, do których odnoszą się informacje lub dokumenty.

W zgodzie z zasadą proporcjonalności zezwolenie premiera określa zakres techniczny przeprowadzania tego przetwarzania.

II. Krajowa komisja ds. kontroli technik wywiadowczych wydaje opinię w przedmiocie wniosku o wydanie zezwolenia na automatyczne przetwarzanie i przyjęte parametry wykrywania. Posiada stały, kompletny i bezpośredni dostęp do takiego przetwarzania, jak również do zgromadzonych informacji i danych. Komisja jest informowana o wszelkich zmianach w sposobie przetwarzania i parametrach oraz może wydawać zalecenia.

Pierwsze zezwolenie na wdrożenie automatycznego przetwarzania przewidzianego w pkt I niniejszego artykułu wydaje się na okres dwóch miesięcy. Zezwolenie może zostać przedłużone zgodnie z warunkami określonymi w rozdziale I tytułu II niniejszej księgi. Wniosek o przedłużenie zawiera ilościowy wykaz identyfikatorów wykrytych przez automatyczne przetwarzanie i analizę istotności tych ostrzeżeń.

III. Warunki przewidziane w art. L. 871-6 mają zastosowanie do czynności materialnych dokonywanych w ramach tego wdrożenia przez operatorów i osoby wymienione w art. L. 851-1.

IV. W przypadku gdy operacje przetwarzania, o których mowa w pkt I niniejszego artykułu, ujawniają dane mogące wskazywać na istnienie zagrożenia o charakterze terrorystycznym, premier lub jedna z osób przez niego delegowanych może zezwolić, po zasięgnięciu opinii krajowej komisji ds. kontroli technik wywiadowczych wydanej na warunkach przewidzianych w rozdziale I tytułu II niniejszej księgi, na identyfikację osoby lub osób, których dane dotyczą, oraz zgromadzenie związanych z tym danych. Dane te są wykorzystywane w ciągu 60 dni od tego zgromadzenia

i zostają zniszczone po upływie tego terminu, chyba że występują ważne okoliczności potwierdzające istnienie zagrożenia terrorystycznego związanego z jedną lub wieloma osobami, których dane dotyczą.

[…]”.

44 Artykuł L. 851-4 CSI ma następujące brzmienie:

„W warunkach przewidzianych w rozdziale I tytułu II niniejszej księgi dane techniczne o lokalizacji używanych urządzeń końcowych, o których mowa w art. L. 851-1, mogą zostać zgromadzone w sieci na żądanie i przekazane w czasie rzeczywistym przez operatorów służbom premiera”.

45 Artykuł R. 851-5 CSI, zawarty w części regulacyjnej tego kodeksu, przewiduje:

„I. Z wyłączeniem treści wymienionej korespondencji lub konsultowanych informacji, informacjami lub dokumentami, o których mowa w art. L. 851-1, są:

1) informacje lub dokumenty wymienione w art. R. 10-13 i R. 10-14 [CPCE] oraz w art. 1 dekretu [nr 2011-219];

2) dane techniczne inne niż wymienione w pkt 1:

a) pozwalające na zlokalizowanie urządzeń końcowych;

b) dotyczące dostępu do urządzeń końcowych sieci lub usług internetowej komunikacji publicznej;

c) dotyczące przekazywania komunikatów elektronicznych przez sieci;

d) dotyczące identyfikacji i uwierzytelnienia użytkownika, połączenia, sieci lub usługi internetowej komunikacji publicznej;

e) dotyczące cech urządzeń końcowych i danych konfiguracji ich oprogramowania.

II. Jedynie informacje i dokumenty, o których mowa w ust. I pkt 1, mogą zostać zgromadzone na podstawie art. L. 851-1. Gromadzenie to ma miejsce z opóźnieniem.

Informacje wymienione w ust. I pkt 2 mogą być gromadzone wyłącznie na podstawie art. L. 851-2 i L. 851-3 na warunkach i w granicach określonych w tych artykułach i z zastrzeżeniem stosowania art. R. 851-9”.

*CPCE*

46 Artykuł L. 34-1 CPCE stanowi:

„I. Niniejszy artykuł ma zastosowanie do przetwarzania danych osobowych w związku z publicznym świadczeniem usług łączności elektronicznej; ma on zastosowanie w szczególności do sieci obejmujących urządzenia do zbierania danych i urządzenia do identyfikacji.

II. Operatorzy łączności elektronicznej i, w szczególności, osoby, których działalność polega na oferowaniu dostępu do usług internetowej komunikacji publicznej, są zobowiązani do usunięcia lub zanonimizowania wszystkich danych o ruchu, z zastrzeżeniem przepisów ust. III, IV, V i VI.

Osoby świadczące publicznie usługi łączności elektronicznej są zobowiązane ustanowić, z uwzględnieniem przepisów poprzedniego ustępu, procedury wewnętrzne umożliwiające ustosunkowanie się do żądań właściwych organów.

Osoby, które w ramach głównej lub dodatkowej działalności zawodowej oferują publicznie

połączenie umożliwiające komunikację internetową za pośrednictwem dostępu do sieci, nawet bezpłatnie, są zobowiązane do przestrzegania przepisów mających zastosowanie do operatorów łączności elektronicznej na mocy niniejszego artykułu.

III. Do celów wykrywania, stwierdzania i ścigania przestępstw lub uchybienia obowiązkowi określonemu w art. L. 336-3 code de la propriété intellectuelle [francuskiego kodeksu własności intelektualnej] lub do celów zapobiegania naruszeniom systemów zautomatyzowanego przetwarzania danych, które są przewidziane i karane na mocy art. 323-1-323-3-1 code pénal [kodeksu karnego], i jedynie w celu umożliwienia, w razie konieczności, udostępnienia sądowi lub wysokiej władzy, o której mowa w art. 331-12 kodeksu własności intelektualnej, lub krajowemu organowi ds. bezpieczeństwa systemów informatycznych określonemu w art. L. 2321-1 code de la défense [kodeksu obronnego], działania zmierzające do usunięcia lub anonimizacji określonych kategorii danych technicznych mogą zostać odroczone na okres maksymalnie jednego roku. Wydany po zasięgnięciu opinii Commission nationale de l'informatique et des libertés [krajowej komisji ds. informatyki i wolności] konsultowany z Conseil d'État (radą stanu, Francja) dekret określa, w granicach ustanowionych w ust. VI, te kategorie danych i okres ich zatrzymywania, w zależności od działalności operatorów i charakteru połączeń oraz warunków rekompensaty, w stosownych przypadkach, możliwych do ustalenia i wyszczególnionych kosztów dodatkowych świadczeń gwarantowanych z tego tytułu przez operatorów na żądanie państwa.

[…]

VI. Dane zatrzymywane i przetwarzane zgodnie z warunkami określonymi w ust. III, IV i V dotyczą wyłącznie identyfikacji użytkowników usług świadczonych przez operatorów, cech technicznych komunikacji dostarczanej przez operatorów oraz lokalizacji urządzeń końcowych.

W żadnym wypadku nie mogą one odnosić się do treści wymienianej korespondencji lub do informacji, z którymi się zapoznano, w jakiejkolwiek formie, w ramach tej komunikacji.

Zatrzymywanie i przetwarzanie tych danych musi się odbywać zgodnie z przepisami ustawy nr 78-17 z dnia 6 stycznia 1978 r. dotyczącej informatyki, plików i swobód.

Operatorzy są zobowiązani do podjęcia wszelkich środków, aby zapobiec wykorzystaniu tych danych do celów innych niż przewidziane w niniejszym artykule".

47 Artykuł R. 10-13 CPCE ma następujące brzmienie:

„I. Na podstawie art. L. 34-1 ust. III operatorzy łączności elektronicznej zatrzymują do celów wykrywania, stwierdzania i ścigania przestępstw:

a) informacje umożliwiające identyfikację użytkownika;

b) dane dotyczące używanych końcowych urządzeń komunikacyjnych;

c) cechy techniczne oraz datę, godzinę i czas trwania każdego połączenia;

d) dane dotyczące żądanych lub używanych usług dodatkowych i ich dostawców;

e) dane umożliwiające identyfikację odbiorcy lub odbiorców połączenia.

II. W przypadku działalności w zakresie telefonii operator zatrzymuje dane, o których mowa w ust. II, a ponadto dane, które pozwalają na identyfikację pochodzenia i lokalizacji połączenia.

III. Okres zatrzymywania danych, o których mowa w niniejszym artykule, wynosi jeden rok, licząc od dnia ich zarejestrowania.

IV. Możliwe do ustalenia i wyszczególnione koszty dodatkowe ponoszone przez operatorów

przyjęte przez organy sądowe w odniesieniu do dostarczania danych należących do kategorii określonych w niniejszym artykule są rekompensowane zgodnie z zasadami przewidzianymi w art. R. 213-1 kodeksu postępowania karnego".

48 Artykuł R. 10-14 CPCE przewiduje:

„I. Na podstawie art. L. 34-1 ust. IV operatorzy łączności elektronicznej są uprawnieni do zatrzymywania, na potrzeby swoich czynności fakturowania i płatności, danych technicznych umożliwiających identyfikację użytkownika, a także danych wymienionych w art. R. 10-13 ust. I lit. b), c) i d).

II. W przypadku działalności w zakresie telefonii operatorzy mogą zatrzymywać, oprócz danych określonych w ust. I, dane techniczne o lokalizacji połączenia, identyfikujące odbiorcę lub odbiorców komunikatu oraz dane umożliwiające wystawienie rachunku.

III. Dane, o których mowa w ust. I i II niniejszego artykułu, mogą być zatrzymywane tylko wtedy, gdy są konieczne do naliczania i uiszczenia opłat za świadczone usługi. Ich zatrzymywanie powinno być ograniczone do czasu ściśle koniecznego dla tego celu i nie może przekraczać jednego roku.

IV. W celu zapewnienia bezpieczeństwa sieci i instalacji operatorzy mogą zatrzymać na okres nieprzekraczający trzech miesięcy:

a) dane umożliwiające ustalenie źródła połączenia;

b) cechy techniczne oraz datę, godzinę i czas trwania każdego połączenia;

c) dane techniczne umożliwiające identyfikację odbiorcy lub odbiorców połączenia;

d) dane dotyczące żądanych lub używanych usług dodatkowych i ich dostawców".

*Ustawa nr 2004-575 z dnia 21 czerwca 2004 r. o zaufaniu w gospodarce cyfrowej*

49 Artykuł 6 ustawy nr 2004-575 z dnia 21 czerwca 2004 r. o zaufaniu w gospodarce cyfrowej (JORF z dnia 22 czerwca 2004 r., s. 11168, zwanej dalej „LCEN") stanowi:

„I. - 1. Osoby, których działalność polega na oferowaniu dostępu do usług internetowej komunikacji publicznej, informują swoich abonentów o istnieniu środków technicznych umożliwiających ograniczenie dostępu do niektórych usług lub ich wybór i proponują im co najmniej jeden z tych środków.

[…].

2. Osoby fizyczne lub prawne oferujące, nawet nieodpłatnie, do publicznego udostępniania za pomocą usług internetowej komunikacji publicznej, przechowywanie sygnałów, tekstów, obrazów, dźwięków lub wszelkiego rodzaju wiadomości dostarczonych przez odbiorców tych usług nie mogą ponosić odpowiedzialności cywilnej za działania lub informacje przechowywane na żądanie odbiorcy tych usług, jeżeli nie miały one rzeczywistej wiedzy na temat ich bezprawnego charakteru lub na temat faktów i okoliczności wskazujących na taki charakter, lub gdy z chwilą, w której osoby te zyskały taką wiedzę, zadziałały one niezwłocznie w celu wycofania tych danych lub uniemożliwienia dostępu do nich.

[…]

II. Osoby, o których mowa w ust. I pkt 1 i 2, mają obowiązek posiadać i zatrzymywać dane umożliwiające identyfikację każdego, kto przyczynił się do stworzenia treści lub części treści usług, których są usługodawcami.

Zapewniają one osobom, które redagują usługę internetowej komunikacji publicznej, środki techniczne umożliwiające im spełnienie warunków identyfikacji przewidzianych w ust. III.

Organ sądowy może zażądać od usługodawców, o których mowa w ust. I pkt 1 i 2, przekazania danych wskazanych w akapicie pierwszym.

Przepisy art. 226-17, 226-21 i 226-22 kodeksu karnego mają zastosowanie do przetwarzania tych danych.

Dekret Conseil d'État (rady stanu, Francja), wydany po zasięgnięciu opinii krajowej komisji ds. informatyki i swobód, określa dane, o których mowa w akapicie pierwszym, oraz określa czas trwania i szczegółowe zasady ich zatrzymywania.

[…]".

*Dekret nr 2011-219*

50 Rozdział I dekretu nr 2011-219, przyjęty na podstawie art. 6 ust. II akapit ostatni LCEN, obejmuje art. 1–4 tego dekretu.

51 Artykuł 1 dekretu nr 2011-219 stanowi:

„Danymi, o których mowa w art. 6 ust. II [LCEN], a które osoby są zobowiązane zatrzymywać na podstawie tego przepisu, są następujące dane:

1. w przypadku osób wymienionych w ust. I pkt 1 tego artykułu dla każdego połączenia ich abonentów:

a) identyfikator połączenia;

b) identyfikator przydzielony przez te osoby abonentowi;

c) identyfikator urządzenia końcowego wykorzystanego do połączenia, jeżeli mają do niego dostęp;

d) daty i godzina rozpoczęcia i zakończenia połączenia;

e) cechy linii abonenta;

2. w przypadku osób, o których mowa w ust. I pkt 2 tego artykułu, dla każdej czynności utworzenia:

a) identyfikator połączenia, z którego pochodzi komunikat;

b) identyfikator przydzielony przez system informatyczny treści będącej przedmiotem czynności;

c) rodzaje protokołów wykorzystywanych do połączenia z usługą i przekazywania treści;

d) charakter czynności;

e) data i godzina czynności;

f) identyfikator użyty przez autora czynności w przypadku, gdy podmiot ten dostarczył tę informację;

3. w przypadku osób, o których mowa w ust. I pkt 1 i 2 tego artykułu, informacje dostarczone w trakcie zawierania umowy przez użytkownika lub w trakcie tworzenia konta:

a) identyfikator tego połączenia w momencie utworzenia konta;

b) imię i nazwisko lub firma;

c) powiązane adresy pocztowe;

d) używane pseudonimy;

e) powiązane adresy poczty elektronicznej lub konta;

f) numery telefonu;

g) hasło oraz dane umożliwiające jego weryfikację lub zmianę, w ostatniej zaktualizowanej wersji;

4. w przypadku osób, o których mowa w ust. I pkt 1 i 2 tego artykułu, gdy zawarcie umowy lub utworzenie konta jest płatne, następujące informacje dotyczące płatności dla każdej transakcji płatniczej:

a) użyta forma płatności;

b) numer referencyjny płatności;

c) kwota;

d) data i godzina transakcji.

Dane, o których mowa w pkt 3 i 4, powinny być zatrzymywane tylko w zakresie, w jakim osoby te zwykle je gromadzą".

52 Artykuł 2 tego dekretu brzmi następująco:

„Wkład w tworzenie treści obejmuje czynności dotyczące:

a) pierwotnego tworzenia treści;

b) modyfikacji treści i danych związanych z treściami;

c) usuwania treści".

53 Artykuł 3 wspomnianego dekretu przewiduje:

„Okres zatrzymywania danych, wymieniony w art. 1, wynosi jeden rok:

a) w przypadku danych, o których mowa w pkt 1 i 2, począwszy od dnia utworzenia treści – dla każdej czynności stanowiącej wkład w tworzenie treści określonej w art. 2;

b) w przypadku danych, o których mowa w pkt 3, począwszy od dnia rozwiązania umowy lub likwidacji konta;

c) w przypadku danych, o których mowa w pkt 4, począwszy od daty wystawienia faktury lub transakcji płatniczej, dla każdej faktury lub transakcji płatniczej".

***Prawo belgijskie***

54 Ustawa z dnia 29 maja 2016 r. zmieniła w szczególności loi du 13 juin 2005 relative aux communications electroniques (ustawę z dnia 13 czerwca 2005 r. o łączności elektronicznej, *Moniteur belge* z dnia 20 czerwca 2005 r., s. 28070, zwaną dalej „ustawą z dnia 13 czerwca 2005 r."), code d'instruction criminelle (kodeks postępowania karnego), a także loi du 30 novembre 1998 organique des services de renseignement et de securité (ustawę organiczną z dnia 30 listopada 1998 r. o służbie wywiadowczej i służbie bezpieczeństwa, *Moniteur belge* z dnia 18 grudnia 1998 r.,

s. 40312, zwaną dalej „ustawą z dnia 30 listopada 1998 r.”).

55 Artykuł 126 ustawy z dnia 13 czerwca 2005 r. w brzmieniu zmienionym ustawą z dnia 29 maja 2016 r. przewiduje:

„§ 1. Bez uszczerbku dla przepisów loi du 8 décembre 1992 relative à la protection de la vie privée à l’égard des traitements de données à caractère personnel (ustawy z dnia 8 grudnia 1992 r. o ochronie życia prywatnego w odniesieniu do przetwarzania danych osobowych), dostawcy publicznych usług telefonicznych, w tym świadczonych za pośrednictwem Internetu, dostępu do Internetu, internetowej poczty elektronicznej, podmioty udostępniające publiczne sieci łączności elektronicznej oraz operatorzy świadczący którąkolwiek z tych usług zatrzymują dane, o których mowa w ust. 3, uzyskiwane lub przetwarzane przez nich w ramach świadczenia usług w zakresie łączności.

Niniejszy artykuł nie odnosi się do treści połączeń.

Obowiązek zatrzymywania danych, o którym mowa w § 3, stosuje się również do nieodebranych połączeń w zakresie, w jakim dane te są dostępne w ramach świadczenia odnośnych usług łączności:

1. w przypadku danych telefonicznych, generowanych lub przetwarzanych przez operatorów publicznie dostępnych usług łączności elektronicznej lub publicznej sieci łączności elektronicznej, lub

2. w przypadku danych internetowych aktualizowanych przez tych dostawców.

§ 2. Dane zatrzymywane w rozumieniu niniejszego artykułu mogą być udostępniane przez dostawców i operatorów wymienionych w § 1 akapit pierwszy wyłącznie na żądanie wskazanych poniżej organów, dla celów i na warunkach określonych poniżej:

1. organy sądowe w celu badania, dochodzenia i ścigania przestępstw, w wykonaniu środków, o których mowa w art. 46 bis i 88 bis code d’instruction criminelle (kodeksu postępowania karnego) i zgodnie z warunkami określonymi w tych artykułach;

2. służby wywiadowcze i służby bezpieczeństwa w celu wypełniania misji wywiadowczych podjętych z wykorzystaniem metod zbierania danych, o których mowa w art. 16/2, 18/7 i 18/8 loi du 30 novembre 1998 organique des services de renseignement et de Sécurité (ustawy organicznej z dnia 30 listopada 1998 r. o służbie wywiadowczej i służbie bezpieczeństwa) na określonych w tej ustawie warunkach;

3. każdy oficer policji sądowej [Institut belge des services postaux et des telecomunications (belgijskiego instytutu ds. usług pocztowych i telekomunikacji)] w celu badania, dochodzenia i ścigania naruszeń art. 114, 124 i niniejszego artykułu;

4. służby ratownicze udzielające pomocy na miejscu, jeżeli w następstwie zgłoszenia alarmowego nie uzyskają one od dostawcy lub danego operatora danych identyfikacyjnych osoby dzwoniącej za pomocą bazy danych, o której mowa w art. 107 § 2 akapit trzeci, lub otrzymały niepełne lub nieprawidłowe dane. Żądanie to może dotyczyć wyłącznie danych identyfikacyjnych zgłaszającego i może być skierowane wyłącznie w ciągu 24 godzin od dokonania zgłoszenia;

5. funkcjonariusze policji z Cellule des personnes disparues de la Police Fédérale (prowadzonej przez policję federalną komórki ds. osób zaginionych) w ramach pomocy osobie zagrożonej, poszukiwania osób, których zaginięcie budzi podejrzenia, oraz jeżeli istnieją uzasadnione poszlaki lub przesłanki wskazujące na fakt bezpośredniego zagrożenia integralności fizycznej osoby zaginionej. Do danego operatora lub dostawcy można zwrócić się, za pośrednictwem służby policji wyznaczonej przez króla, o udostępnienie wyłącznie danych, o których mowa w § 3 akapity

pierwszy i drugi, dotyczących osoby zaginionej i zatrzymywanych przez 48 godzin poprzedzających złożenie żądania udostępnienia danych;

6. service de mediation pour les telecommunications (służba mediacji w telekomunikacji) w celu ustalenia tożsamości osoby, która w sposób niedozwolony wykorzystała sieć lub usługę łączności elektronicznej – zgodnie z warunkami określonymi w art. 43a § 3 pkt 7 loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (ustawy z dnia 21 marca 1991 r. w sprawie reformy niektórych publicznych przedsiębiorstw gospodarczych). Żądanie to może obejmować wyłącznie dane identyfikacyjne.

Dostawcy i operatorzy, o których mowa w § 1 akapit pierwszy, udostępniają dane wymienione w ust. 3 w taki sposób, aby były one dostępne bez ograniczeń z terytorium Belgii oraz aby dane te i inne niezbędne informacje dotyczące tych danych mogły być przekazywane bezzwłocznie wyłącznie organom wymienionym w niniejszym paragrafie.

Bez uszczerbku dla innych przepisów dostawcy i operatorzy, o których mowa w ust. 1 akapit pierwszy, nie mogą wykorzystywać danych zatrzymywanych na podstawie ust. 3 do jakichkolwiek innych celów.

§ 3. Dane umożliwiające identyfikację użytkownika lub abonenta oraz środków łączności, z wyjątkiem danych przewidzianych w szczególności w akapitach drugim i trzecim, są zatrzymywane przez okres dwunastu miesięcy od daty, w której łączność za pomocą określonej usługi była po raz ostatni możliwa.

Dane dotyczące dostępu i podłączenia urządzeń końcowych do sieci i do usługi oraz lokalizacji urządzeń, w tym punktu zakończenia sieci, są zatrzymywane przez okres dwunastu miesięcy od daty połączenia.

Dane komunikacyjne, z wyjątkiem treści, w tym dotyczące ich pochodzenia i przeznaczenia, są zatrzymywane przez okres dwunastu miesięcy od daty połączenia.

Król, w drodze dekretu konsultowanego z radą ministrów, na wniosek ministra sprawiedliwości i ministra [właściwego w dziedzinie łączności elektronicznej] oraz po zasięgnięciu opinii Commission de la protection de la vie privée (komisji ochrony życia prywatnego) i instytutu, ustala rodzaje danych podlegających zatrzymaniu z podziałem na typy kategorii określonych w akapitach od pierwszego do trzeciego, jak również wymogi, które dane te muszą spełniać.

[…]”.

## Spory w postępowaniach głównych i pytania prejudycjalne

### *Sprawa C-511/18*

56 W skargach złożonych w dniach 30 listopada 2015 r. i 16 marca 2016 r., które zostały połączone w postępowaniu głównym, Quadrature du Net, French Data Network i Fédération des opératives d’Internet associatifs, a także Igwan.net wniosły do Conseil d’État (rady stanu, Francja) o stwierdzenie nieważności dekretów nr 2015-1185, nr 2015-1211, nr 2015-1639 i nr 2016-67, w szczególności z tego powodu, że są one sprzeczne z francuską konstytucją, europejską Konwencją o ochronie praw człowieka i podstawowych wolności (zwaną dalej „EKPC”) oraz dyrektywami 2000/31 i 2002/58 w związku z art. 7, 8 i 47 karty.

57 Co się tyczy w szczególności zarzutów dotyczących naruszenia dyrektywy 2000/31, sąd odsyłający wskazuje, że przepisy art. L. 851-3 CSI zobowiązują operatorów łączności elektronicznej oraz dostawców technologii do „wdrożenia w swoich sieciach operacji automatycznego przetwarzania, na podstawie parametrów określonych w zezwoleniu, zmierzających do wykrycia połączeń, które

mogą wskazywać na zagrożenie terrorystyczne". Technika ta miała na celu jedynie gromadzenie przez określony czas, spośród wszystkich danych o połączeniach przetwarzanych przez tych operatorów i tych dostawców, danych, które mogłyby mieć związek z takim poważnym przestępstwem. W tych okolicznościach wspomniane przepisy, które nie nakładają ogólnego obowiązku aktywnego nadzoru, nie naruszają zdaniem tego sądu art. 15 dyrektywy 2000/31.

58 Co się tyczy zarzutów dotyczących naruszenia dyrektywy 2002/58, sąd odsyłający uważa, że w szczególności z przepisów tej dyrektywy, a także 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, iż przepisy krajowe nakładające obowiązki na dostawców usług łączności elektronicznej, takie jak uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji ich użytkowników i ich abonentów, do celów określonych w art. 15 ust. 1 wspomnianej dyrektywy, do których należą ochrona bezpieczeństwa narodowego, obronność i bezpieczeństwo publiczne, są objęte zakresem stosowania tej dyrektywy w zakresie, w jakim przepisy te regulują działalność wspomnianych dostawców. To samo dotyczy przepisów regulujących dostęp organów krajowych do danych oraz ich wykorzystywanie.

59 Sąd odsyłający wnioskuje z tego, że zakresem stosowania dyrektywy 2002/58 objęty jest zarówno obowiązek zatrzymywania wynikający z art. L. 851-1 CSI, jak i dostęp administracyjny do wspomnianych danych, w tym również dostęp w czasie rzeczywistym, przewidziany w art. L. 851-1, L. 851-2 i L. 851-4 wspomnianego kodeksu. Dotyczy to także zdaniem tego sądu przepisów zawartych w art. L. 851-3 tego kodeksu, które jakkolwiek nie nakładają na zainteresowanych operatorów ogólnego obowiązku zatrzymywania danych, to jednak wymagają od nich wdrożenia w ich sieciach operacji automatycznego przetwarzania w celu wykrywania połączeń mogących wskazywać na zagrożenie terrorystyczne.

60 Sąd ten uważa natomiast, że zakresem stosowania dyrektywy 2002/58 nie są objęte przepisy CSI, do których odnoszą się żądania stwierdzenia nieważności, dotyczące technik gromadzenia informacji stosowanych bezpośrednio przez państwo, a które nie regulują działalności dostawców usług łączności elektronicznej poprzez nałożenie na nich szczególnych obowiązków. Nie można zatem uznać, że przepisy te wdrażają prawo Unii, w związku z czym nie można skutecznie podnosić zarzutów opartych na naruszeniu przez nie dyrektywy 2002/58.

61 Zatem w perspektywie rozstrzygnięcia sporów dotyczących zgodności z prawem dekretów nr 2015-1185, nr 2015-1211, nr 2015-1639 i nr 2016-67 z punktu widzenia dyrektywy 2002/58 - jako że zostały one wydane w celu wykonania art. L. 851-1-L. 851-4 CSI – pojawiają się trzy kwestie dotyczące wykładni prawa Unii.

62 Co się tyczy wykładni art. 15 ust. 1 dyrektywy 2002/58, sąd odsyłający zastanawia się w pierwszej kolejności nad tym, czy obowiązek uogólnionego i niezróżnicowanego zatrzymywania nałożony na dostawców usług łączności elektronicznej na podstawie art. L. 851-1 i R. 851-5 CSI należy postrzegać – w szczególności w świetle gwarancji i kontroli, którym podlegają dostęp administracyjny do danych dotyczących połączeń i wykorzystanie tych danych – jako ingerencję uzasadnioną prawem do bezpieczeństwa osobistego gwarantowanym w art. 6 karty oraz wymogami bezpieczeństwa narodowego, które leżą w zakresie wyłącznej odpowiedzialności państw członkowskich zgodnie z art. 4 TUE.

63 Co się tyczy w drugiej kolejności innych obowiązków, jakie mogą zostać nałożone na dostawców usług łączności elektronicznej, sąd odsyłający wskazuje, że przepisy art. L. 851-2 CSI zezwalają, wyłącznie na potrzeby zapobiegania terroryzmowi, na zbieranie od tych osób informacji lub dokumentów przewidzianych w art. L. 851-1 tego kodeksu. Takie zbieranie, które dotyczy tylko jednej osoby lub wielu indywidualnych osób wcześniej zidentyfikowanych jako mogące mieć związek z zagrożeniem terroryzmem, odbywa się w czasie rzeczywistym. To samo dotyczy przepisów art. L. 851-4 wspomnianego kodeksu, zezwalających na transmitowanie w czasie rzeczywistym przez operatorów wyłącznie danych technicznych dotyczących lokalizacji urządzeń

końcowych. Techniki te regulują w różnych celach i na różne sposoby dostęp administracyjny w czasie rzeczywistym do danych zatrzymywanych na podstawie CPCE i LCEN, nie nakładając jednak na dostawców, których to dotyczy, wymogu dodatkowego zatrzymywania w stosunku do tego, co jest konieczne do fakturowania i świadczenia ich usług. Podobnie przepisy art. L. 851-3 CSI, które nakładają na dostawców usług obowiązek wdrożenia w ich sieciach zautomatyzowanej analizy połączeń, również nie wymagają uogólnionego i niezróżnicowanego zatrzymywania.

64 Tymczasem, po pierwsze, sąd odsyłający uważa, że zarówno uogólnione i niezróżnicowane zatrzymywanie, jak i dostęp w czasie rzeczywistym do danych dotyczących połączeń wykazują, w kontekście charakteryzującym się poważnym i trwałym zagrożeniem dla bezpieczeństwa narodowego, związanym w szczególności z ryzykiem terrorystycznym, niezrównaną przydatność operacyjną. Uogólnione i niezróżnicowane zatrzymywanie umożliwia bowiem służbom wywiadowczym dostęp do danych dotyczących połączeń przed wykryciem podstaw do tego, aby sądzić, że osoba, której dane dotyczą, stanowi zagrożenie dla bezpieczeństwa publicznego, obronności lub bezpieczeństwa państwa. Ponadto dostęp w czasie rzeczywistym do danych dotyczących połączeń pozwala na śledzenie, z dużą możliwością reakcji, zachowań osób mogących stanowić bezpośrednie zagrożenie dla porządku publicznego.

65 Po drugie, technika przewidziana w art. L. 851-3 CSI pozwala na wykrycie, na podstawie kryteriów jasno określonych w tym celu, osób, których zachowanie, z uwagi na ich kanały komunikacji, może wskazywać na zagrożenie terrorystyczne.

66 W trzeciej kolejności, co się tyczy dostępu właściwych organów do zatrzymywanych danych, sąd odsyłający zastanawia się, czy dyrektywę 2002/58, odczytywaną w świetle karty, należy interpretować w ten sposób, że uzależnia ona we wszystkich przypadkach prawidłowość procedur gromadzenia danych dotyczących połączeń od wymogu informowania osób, których dane dotyczą, kiedy taka informacja nie może już zagrozić dochodzeniom prowadzonym przez właściwe organy, lub czy takie procedury mogą zostać uznane za prawidłowe w świetle wszystkich innych istniejących gwarancji proceduralnych, skoro gwarancje te zapewniają skuteczność prawa do środka odwoławczego.

67 Co się tyczy tych innych gwarancji proceduralnych, sąd odsyłający wyjaśnia w szczególności, że każda osoba pragnąca sprawdzić, czy jakaś technika wywiadowcza nie została w stosunku do niej nieprawidłowo wdrożona, może zwrócić się do wyspecjalizowanego składu Conseil d'État (rady stanu, Francja), do którego należy zbadanie w świetle przekazanych jej informacji w postępowaniu niespornym, czy wobec skarżącego wdrożono technikę i czy została ona wdrożona zgodnie z księgą VIII CSI. Przysługujące temu składowi uprawnienia do rozpoznawania skarg gwarantują skuteczność sprawowanej przez niego kontroli sądowej. Tak więc ma on uprawnienia do rozpoznawania skarg, uwzględniania z urzędu wszystkich stwierdzonych przez niego przypadków bezprawności oraz nakazywania administracji podjęcia wszelkich właściwych środków w celu wyeliminowania stwierdzonych naruszeń. Ponadto do krajowej komisji ds. kontroli technik wywiadowczych należy sprawdzenie, czy techniki gromadzenia informacji są na terytorium krajowym wdrażane zgodnie z wymogami wynikającymi z CSI. Zatem okoliczność, że przepisy ustawowe rozpatrywane w postępowaniu głównym nie przewidują powiadomienia osób, których dane dotyczą, o środkach nadzoru stosowanych wobec nich, nie stanowi sama w sobie nadmiernego naruszenia prawa do poszanowania życia prywatnego.

68 W tych okolicznościach Conseil d'État (rada stanu, Francja) postanowiła zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami:

„1) Czy obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych nałożony na dostawców usług w oparciu o przepisy upoważniające zawarte w art. 15 ust. 1 dyrektywy [2002/58/WE] należy uważać, w kontekście poważnych i trwałych zagrożeń dla bezpieczeństwa narodowego, a zwłaszcza zagrożenia terrorystycznego, za ingerencję uzasadnioną prawem do bezpieczeństwa osobistego zagwarantowanym w art. 6 [karty]

i wymogami bezpieczeństwa narodowego, które leżą w zakresie wyłącznej odpowiedzialności państw członkowskich zgodnie z art. 4 [TUE]?

2) Czy dyrektywę [2002/58] odczytywaną w świetle [karty] należy interpretować w ten sposób, że dopuszcza ona środki ustawodawcze takie jak środki gromadzenia w czasie rzeczywistym danych dotyczących ruchu i lokalizacji określonych osób, które choć wpływają na prawa i obowiązki dostawców usług łączności elektronicznej, to jednak nie nakładają na nich szczególnego obowiązku [zatrzymywania] danych tych osób?

3) Czy dyrektywę [2002/58] odczytywaną w świetle [karty] należy interpretować w ten sposób, że uzależnia ona we wszystkich przypadkach prawidłowość procedur gromadzenia danych dotyczących połączeń od wymogu informowania osób, których dane dotyczą, kiedy taka informacja nie może już zagrozić dochodzeniom prowadzonym przez właściwe organy, lub czy takie procedury mogą zostać uznane za prawidłowe w świetle wszystkich innych istniejących gwarancji proceduralnych, skoro gwarancje te zapewniają skuteczność prawa do środka odwoławczego?".

***Sprawa C-512/18***

69 Pismem z dnia 1 września 2015 r. French Data Network, Quadrature du Net i Fédération des opératives d'Internet associatifs wniosły do Conseil d'État (rady stanu, Francja) skargę o stwierdzenie nieważności dorozumianej decyzji odmownej wynikającej z bezczynności premiera w przedmiocie ich wniosku o uchylenie art. R. 10-13 CPCE oraz dekretu nr 2011-219, w szczególności ze względu na to, że przepisy te są sprzeczne z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 karty. Privacy International oraz Center for Democracy and Technology zostały dopuszczone do udziału w postępowaniu głównym w charakterze interwenientów.

70 Co się tyczy art. R. 10-13 CPCE i obowiązku uogólnionego i niezróżnicowanego zatrzymywania danych dotyczących połączeń, który jest w nim przewidziany, sąd odsyłający, przedstawiając rozważania podobne do tych przedstawionych w ramach sprawy C-511/18, zauważa, że takie zatrzymywanie umożliwia organowi sądowemu dostęp do danych dotyczących połączeń, które dana osoba wykonała, zanim stała się podejrzana o popełnienie przestępstwa, w związku z czym to zatrzymywanie wykazuje niezrównaną przydatność dla celów wykrywania, stwierdzania i ścigania przestępstw.

71 Co się tyczy dekretu nr 2011-219, sąd odsyłający uważa, że art. 6 ust. II LCEN, który nakłada obowiązek posiadania i zatrzymywania jedynie danych dotyczących tworzenia treści, nie jest objęty zakresem stosowania dyrektywy 2002/58, ponieważ zgodnie z jej art. 3 ust. 1 jest ona ograniczona do dostarczania publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii, lecz zakresem stosowania dyrektywy 2000/31.

72 Sąd ten uważa jednak, że z art. 15 ust. 1 i 2 dyrektywy 2000/31 wynika, iż nie wprowadza ona zasadniczego zakazu zatrzymywania danych dotyczących tworzenia treści, od którego można jedynie odstąpić w drodze wyjątku. Powstaje zatem pytanie, czy art. 12, 14 i 15 wspomnianej dyrektywy, w związku z art. 6–8 i 11 oraz art. 52 ust. 1 karty, należy interpretować w ten sposób, że pozwalają one państwu członkowskiemu na przyjęcie przepisu krajowego, takiego jak art. 6 ust. II LCEN, nakładającego na zainteresowane osoby obowiązek zatrzymywania danych umożliwiających identyfikację każdego, kto przyczynił się do stworzenia treści lub części treści usług, których są usługodawcami, aby organ sądowy mógł, w razie potrzeby, zażądać ich przekazania w celu egzekwowania przepisów dotyczących odpowiedzialności cywilnej lub karnej.

73 W tych okolicznościach Conseil d'État (rada stanu, Francja) postanowiła zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„1) Czy obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych nałożony na dostawców usług na podstawie przepisów upoważniających zawartych w art. 15 ust. 1

dyrektywy [2002/58] należy uważać, biorąc pod uwagę gwarancje i kontrole towarzyszące następnie gromadzeniu i wykorzystaniu tych danych o połączeniach, za ingerencję uzasadnioną prawem do bezpieczeństwa osobistego zagwarantowanym w art. 6 [karty] i wymogami bezpieczeństwa narodowego, które leżą w zakresie wyłącznej odpowiedzialności państw członkowskich zgodnie z art. 4 [TUE]?

2) Czy przepisy dyrektywy [2000/31], w związku z art. 6, 7, 8 i 11 oraz art. 52 ust. 1 [karty], należy interpretować w ten sposób, że pozwalają one państwu na wprowadzenie przepisów krajowych nakładających na osoby, których działalność polega na oferowaniu dostępu do usług internetowej komunikacji publicznej oraz na osoby fizyczne lub prawne oferujące, nawet nieodpłatnie, do publicznego udostępniania za pomocą usługi internetowej komunikacji publicznej, przechowywanie sygnałów, tekstów, obrazów, dźwięków lub wszelkiego rodzaju wiadomości dostarczonych przez odbiorców tych usług obowiązek zatrzymywania danych umożliwiających identyfikację każdego, kto przyczynił się do stworzenia treści lub części treści usług, których są usługodawcami, aby organ sądowy mógł, w razie potrzeby, zażądać ich przekazania w celu egzekwowania przepisów dotyczących odpowiedzialności cywilnej lub karnej?”.

***Sprawa C-520/18***

74 W skargach wniesionych w dniach 10, 16, 17 i 18 stycznia 2017 r., które zostały połączone w ramach postępowania głównego, Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL i UA, Liga voor Mensenrechten ASBL i Ligue des Droits de l’Homme ASBL oraz VZ, WY i XX wniosły do Cour constitutionnelle (trybunału konstytucyjnego, Belgia) o stwierdzenie nieważności ustawy z dnia 29 maja 2016 r. z powodu jej sprzeczności z art. 10 i 11 belgijskiej konstytucji w związku z art. 5, 6–11, 14, 15, 17 i 18 EKPC, art. 7, 8, 11 i 47 oraz art. 52 ust. 1 karty, art. 17 Międzynarodowego paktu praw obywatelskich i politycznych, przyjętego przez Zgromadzenie Ogólne Narodów Zjednoczonych w dniu 16 grudnia 1966 r., który wszedł w życie w dniu 23 marca 1976 r., ogólnymi zasadami pewności prawa, proporcjonalności i samostanowienia w dziedzinie informacji, a także art. 5 ust. 4 TUE.

75 Na poparcie swoich skarg skarżący w postępowaniu głównym podnoszą zasadniczo, że niezgodność z prawem ustawy z dnia 29 maja 2016 r. wynika w szczególności z faktu, iż ustawa ta wykracza poza granice tego, co ściśle niezbędne, i nie przewiduje wystarczających gwarancji ochrony. W szczególności ani jej przepisy dotyczące zatrzymywania danych, ani te regulujące dostęp organów do zatrzymanych danych nie odpowiadają wymogom wynikającym z wyroku z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in. (C-293/12 i C-594/12, zwanego dalej „wyrokiem Digital Rights”, EU:C:2014:238), oraz z wyroku z dnia 21 grudnia 2016 r., Tele2 (C-203/15 i C-698/15, EU:C:2016:970). Przepisy te niosą bowiem ze sobą ryzyko stworzenia profili osobowości, wraz z wynikającymi z tego możliwymi nadużyciami ze strony właściwych organów, oraz nie przewidują odpowiedniego poziomu zabezpieczenia i ochrony zatrzymanych danych. Wreszcie ustawa ta dotyczy osób objętych tajemnicą zawodową oraz osób, na których ciąży obowiązek zachowania poufności, i odnosi się do szczególnie chronionych danych osobowych dotyczących połączeń, nie zawierając przy tym szczególnych gwarancji w celu ochrony tych ostatnich danych.

76 Sąd odsyłający wskazuje, że dane, które zgodnie z ustawą z dnia 29 maja 2016 r. powinni zatrzymywać dostawcy usług telefonicznych, w tym przez Internet, dostępu do Internetu i poczty elektronicznej, a także dostawcy publicznych sieci łączności elektronicznej, są identyczne z danymi wymienionymi w dyrektywie Parlamentu Europejskiego i Rady 2006/24/WE z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE (Dz.U. 2006, L 105, s. 54), jednak bez wprowadzenia rozróżnienia w zależności od osób, których dane dotyczą, ani zamierzonych celów. W tym ostatnim względzie sąd ów wyjaśnia, że celem, do którego ustawodawca zmierza w tej

ustawie, jest nie tylko zwalczanie terroryzmu i pornografii dziecięcej, ale także możliwość wykorzystania zatrzymanych danych w wielu różnych sytuacjach w ramach postępowania karnego. Ponadto sąd odsyłający stwierdza, że z uzasadnienia wspomnianej ustawy wnika, iż ustawodawca krajowy uznał, że nie było możliwości, w świetle zamierzonego celu, ustanowienia obowiązku ukierunkowanego i zróżnicowanego zatrzymywania, i zdecydował się opatrzyć obowiązek uogólnionego i niezróżnicowanego zatrzymywania rygorystycznymi gwarancjami zarówno w odniesieniu do zatrzymywanych danych, jak i dostępu do nich, aby ograniczyć do minimum ingerencję w prawo do poszanowania życia prywatnego.

77 Sąd odsyłający dodaje, że art. 126 ust. 2 pkt 1 i 2 ustawy z dnia 13 czerwca 2005 r., zmieniony ustawą z dnia 29 maja 2016 r., określa warunki, na jakich, odpowiednio, organy sądowe oraz służby wywiadowcze i bezpieczeństwa mogą uzyskać dostęp do zatrzymanych danych, a więc badanie zgodności z prawem tej ustawy w świetle wymogów prawa Unii należy wstrzymać do czasu wydania przez Trybunał orzeczenia w dwóch zawisłych przed nim postępowaniach prejudycjalnych dotyczących takiego dostępu.

78 Wreszcie sąd odsyłający wskazuje, że ustawa z dnia 29 maja 2016 r. ma na celu umożliwienie skutecznego dochodzenia karnego i zastosowania skutecznej sankcji w przypadku wykorzystywania seksualnego małoletnich oraz umożliwienie zidentyfikowania sprawcy takiego przestępstwa, nawet w przypadku korzystania ze środków łączności elektronicznej. W toku postępowania przed tym sądem zwrócono uwagę w tym względzie na pozytywne obowiązki wynikające z art. 3 i 8 EKPC. Obowiązki te mogą wynikać również z odpowiednich postanowień karty, mogących mieć wpływ na wykładnię art. 15 ust. 1 dyrektywy 2002/58.

79 W tych okolicznościach Cour constitutionnelle (trybunał konstytucyjny, Belgia) postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„1) Czy art. 15 ust. 1 dyrektywy [2002/58] w związku z prawem do bezpieczeństwa zagwarantowanym w art. 6 [karty] oraz prawem do ochrony danych osobowych zagwarantowanym w art. 7, 8 i art. 52 ust. 1 [karty] należy interpretować w ten sposób, że sprzeciwia się on uregulowaniu krajowemu takiemu jak rozpatrywane w postępowaniu głównym, przewidującemu dla operatorów i dostawców usług łączności elektronicznej powszechny obowiązek zatrzymywania wszystkich danych o ruchu i lokalizacji w rozumieniu dyrektywy [2002/58], generowanych lub przetwarzanych w ramach świadczenia tych usług, które to uregulowanie ma na celu nie tylko dochodzenie, wykrywanie i karanie poważnych przestępstw, ale także zapewnienie bezpieczeństwa narodowego, obrony terytorium i bezpieczeństwa publicznego oraz zapobieganie, dochodzenie, wykrywanie i karanie przestępstw innych niż poważne lub zapobieganie niedozwolonemu używaniu systemów łączności elektronicznej lub realizuje inny cel, który jest wymieniony w art. 23 ust. 1 rozporządzenia [2016/679] i który ponadto jest objęty gwarancjami określonymi w tym uregulowaniu w zakresie zatrzymywania danych i dostępu do nich?

2) Czy art. 15 ust. 1 dyrektywy [2002/58] w związku z art. 4, 7, 8, 11 i art. 52 ust. 1 [karty] należy interpretować w ten sposób, że sprzeciwia się on uregulowaniu krajowemu takiemu jak rozpatrywane w postępowaniu głównym, które przewiduje spoczywający na operatorach i dostawcach usług łączności elektronicznej powszechny obowiązek zatrzymywania danych o ruchu i lokalizacji w rozumieniu dyrektywy [2002/58], generowanych lub przetwarzanych przez nich w związku ze świadczeniem tych usług, jeżeli uregulowanie to ma na celu wypełnienie pozytywnych obowiązków nałożonych na organy zgodnie z art. 4 i [7] karty, polegających na ustanowieniu ram prawnych, które umożliwiają skuteczne prowadzenie dochodzenia w sprawach karnych oraz skuteczne zwalczanie wykorzystywania seksualnego małoletnich, a także skuteczne zidentyfikowanie sprawcy czynu karalnego nawet w przypadku korzystania ze środków łączności elektronicznej?

3) Jeżeli na podstawie odpowiedzi udzielonych na pierwsze lub drugie pytanie prejudycjalne

Cour constitutionnelle (trybunał konstytucyjny, Belgia) miałby dojść do wniosku, że zaskarżona ustawa narusza jeden lub więcej z obowiązków wynikających z przepisów wskazanych w tych pytaniach, czy mógłby tymczasowo utrzymać w mocy skutki ustawy [z dnia 29 maja 2016 r.], aby uniknąć niepewności prawa i zapewnić możliwość dalszego wykorzystywania uprzednio zebranych i zatrzymywanych danych do celów określonych w [ustawie]?".

**W przedmiocie postępowania przed Trybunałem**

80 Postanowieniem prezesa Trybunału z dnia 25 września 2018 r. sprawy C-511/18 i C-512/18 zostały połączone do celów przeprowadzenia pisemnego i ustnego etapu postępowania oraz wydania wyroku. Postanowieniem prezesa Trybunału z dnia 9 lipca 2020 r. sprawa C-520/18 została połączona z tymi sprawami do celów wydania wyroku.

**W przedmiocie pytań prejudycjalnych**

***W przedmiocie pytań pierwszych w sprawach C-511/18 i C-512/18 oraz w przedmiocie pytań pierwszego i drugiego w sprawie C-520/18***

81 Poprzez pytania pierwsze w sprawach C-511/18 i C-512/18, a także pytania pierwsze i drugie w sprawie C-520/18, które należy zbadać łącznie, sądy odsyłające dążą w istocie do ustalenia, czy art. 15 ust. 1 dyrektywy 2002/58 należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu nakładającemu na dostawców usług łączności elektronicznej, w celach określonych w tym art. 15 ust. 1, obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji.

*Uwagi wstępne*

82 Z akt sprawy, którymi dysponuje Trybunał, wynika, że uregulowania rozpatrywane w postępowaniu głównym odnoszą się do wszystkich środków łączności elektronicznej i obejmują wszystkich użytkowników tych środków, bez zróżnicowania ani wyjątku w tym względzie. Ponadto uregulowania te zobowiązują dostawców usług łączności elektronicznej do zatrzymywania w szczególności danych niezbędnych do ustalenia pochodzenia i przeznaczenia połączenia, określenia daty, godziny, czasu trwania i rodzaju połączenia, wskazania wykorzystanego urządzenia komunikacyjnego, a także ustalenia położenia urządzeń końcowych i połączeń, danych, wśród których znajdują się w szczególności nazwisko i adres użytkownika, numery telefonu przychodzące i wychodzące oraz adres IP w przypadku usług internetowych. Natomiast omawiane dane nie obejmują treści rozpatrywanych komunikatów.

83 A zatem dane, które zgodnie z uregulowaniami krajowymi rozpatrywanymi w postępowaniu głównym powinny być zatrzymywane przez okres jednego roku, pozwalają w szczególności na ustalenie osoby, z którą użytkownik środka komunikacji elektronicznej nawiązał połączenie, i tego, za pomocą jakiego środka doszło do tego połączenia, na określenie daty, godziny i czasu trwania połączeń i połączeń internetowych, a także miejsca, w którym połączenia te się odbyły, oraz na poznanie lokalizacji urządzeń końcowych, przy czym komunikat niekoniecznie musi być przekazywany. Ponadto oferują one możliwość określenia częstotliwości kontaktów użytkownika z niektórymi osobami w danym okresie. Wreszcie, co się tyczy przepisów krajowych rozpatrywanych w sprawach C-511/18 i C-512/18, wydaje się, że w zakresie, w jakim obejmują one również dane dotyczące przesyłania komunikatów elektronicznych przez sieci, pozwalają także na określenie charakteru informacji konsultowanych w Internecie.

84 Co się tyczy realizowanych celów, należy zauważyć, że uregulowania rozpatrywane w sprawach C-511/18 i C-512/18 mają na celu między innymi wykrywanie, stwierdzanie i ściganie przestępstw w ogólności, niepodległość narodową, integralność terytorium i obronę narodową, podstawowe

interesy polityki zagranicznej, wykonywanie zobowiązań europejskich i międzynarodowych Francji, najważniejsze interesy gospodarcze, przemysłowe i naukowe Francji, a także zapobieganie terroryzmowi, naruszeniom republikańskiej formy instytucji i przemocy zbiorowej, która mogłaby poważnie naruszyć spokój publiczny. Co się tyczy przepisów będących przedmiotem sprawy C-520/18, mają one na celu między innymi dochodzenie, wykrywanie i ściganie przestępstw, jak również ochronę bezpieczeństwa narodowego, ochronę terytorium i bezpieczeństwa publicznego.

85 Sądy odsyłające zastanawiają się w szczególności nad ewentualnym wpływem na wykładnię art. 15 ust. 1 dyrektywy 2002/58 prawa do bezpieczeństwa ustanowionego w art. 6 karty. Podobnie zastanawiają się, czy ingerencja w prawa podstawowe ustanowione w art. 7 i 8 karty, jaką pociąga za sobą zatrzymywanie danych przewidziane w przepisach rozpatrywanych w postępowaniu głównym, może, w świetle istnienia przepisów ograniczających dostęp organów krajowych do zatrzymanych danych, zostać uznana za uzasadnioną. Ponadto zdaniem Conseil d'État (rady stanu, Francja), skoro pytanie to powstaje w kontekście poważnego i trwałego zagrożenia dla bezpieczeństwa narodowego, należy je również oceniać w świetle art. 4 ust. 2 TUE. Cour constitutionnelle (trybunał konstytucyjny, Belgia) natomiast podkreśla, że uregulowanie krajowe rozpatrywane w sprawie C-520/18 wprowadza również w życie pozytywne obowiązki wynikające z art. 4 i 7 karty, polegające na ustanowieniu ram prawnych pozwalających na skuteczne zwalczanie wykorzystywania seksualnego małoletnich.

86 Jakkolwiek zarówno Conseil d'État (rada stanu, Francja), jak i Cour constitutionnelle (trybunał konstytucyjny, Belgia) wychodzą z założenia, że uregulowania krajowe rozpatrywane w postępowaniu głównym, które regulują zatrzymywanie danych o ruchu i danych o lokalizacji, a także dostęp organów krajowych do tych danych w celach przewidzianych w art. 15 ust. 1 dyrektywy 2002/58, takich jak ochrona bezpieczeństwa narodowego, są objęte zakresem stosowania tej dyrektywy, niektóre strony postępowania głównego i niektóre państwa członkowskie, które przedstawiły Trybunałowi uwagi na piśmie, wyrażają odmienną opinię w tym względzie, w szczególności w odniesieniu do wykładni art. 1 ust. 3 omawianej dyrektywy. Należy zatem najpierw zbadać, czy rzeczone przepisy wchodzą w zakres stosowania tej dyrektywy.

*W przedmiocie zakresu stosowania dyrektywy 2002/58*

87 Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International i Center for Democracy and Technology podnoszą zasadniczo, powołując się w tym względzie na orzecznictwo Trybunału dotyczące zakresu stosowania dyrektywy 2002/58, że zarówno zatrzymywanie danych, jak i dostęp do zatrzymanych danych są objęte tym zakresem stosowania, niezależnie od tego, czy dostęp ten miał miejsce w czasie późniejszym, czy też w czasie rzeczywistym. Skoro bowiem cel ochrony bezpieczeństwa narodowego został wyraźnie wymieniony w art. 15 ust. 1 tej dyrektywy, dążenie do tego celu nie pociąga za sobą niemożności stosowania wspomnianej dyrektywy. Artykuł 4 ust. 2 TUE, do którego odnoszą się sądy odsyłające, nie ma wpływu na tę ocenę.

88 Co się tyczy środków wywiadowczych, które właściwe organy francuskie wdrażają bezpośrednio, nie regulując działalności dostawców usług łączności elektronicznej poprzez nałożenie na nich szczególnych obowiązków, Center for Democracy and Technology zauważa, że środki te są w sposób nieunikniony objęte zakresem stosowania dyrektywy 2002/58 oraz zakresem karty, ponieważ stanowią odstępstwa od zasady poufności zagwarantowanej w art. 5 tej dyrektywy. Wspomniane środki powinny zatem być zgodne z wymogami wynikającymi z art. 15 ust. 1 tej dyrektywy.

89 Natomiast rządy francuski, czeski i estoński, Irlandia, rządy cypryjski, węgierski, polski, szwedzki i Zjednoczonego Królestwa podnoszą zasadniczo, że dyrektywa 2002/58 nie ma zastosowania do przepisów krajowych takich jak rozpatrywane w postępowaniu głównym, ponieważ mają one na celu ochronę bezpieczeństwa narodowego. Działalność służb wywiadowczych w zakresie, w jakim polega na utrzymaniu porządku publicznego oraz ochronie bezpieczeństwa wewnętrznego

i integralności terytorialnej, należy do podstawowych funkcji państw członkowskich i w konsekwencji należy do ich wyłącznej właściwości, o czym świadczy w szczególności art. 4 ust. 2 zdanie trzecie TUE.

90 Rządy te oraz Irlandia powołują się ponadto na art. 1 ust. 3 dyrektywy 2002/58, który wyłącza z zakresu stosowania tej dyrektywy, podobnie jak przewidywał to już art. 3 ust. 2 tiret pierwsze dyrektywy 95/46, działania dotyczące bezpieczeństwa publicznego, obronności i bezpieczeństwa państwa. Powołują się one w tym względzie na wykładnię tego ostatniego przepisu zawartą w wyroku z dnia 30 maja 2006 r., Parlament/Rada i Komisja (C-317/04 i C-318/04, EU:C:2006:346).

91 W tym względzie należy wskazać, że zgodnie z art. 1 ust. 1 dyrektywy 2002/58 dyrektywa ta przewiduje między innymi harmonizację przepisów krajowych wymaganych do zapewnienia równoważnego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do ochrony życia prywatnego i poufności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej.

92 Artykuł 1 ust. 3 tej dyrektywy wyłącza z zakresu jej stosowania „działalność" państwa w obszarach, które zostały tam wymienione, a w szczególności działalność państwa w dziedzinie prawa karnego oraz działalność dotyczącą bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa, włączając w to dobrobyt gospodarczy państwa, gdy działalność odnosi się do spraw bezpieczeństwa państwa. Rodzaje działalności, które zostały w ten sposób wymienione tytułem przykładu, stanowią w każdym wypadku działalność właściwą państwom i organom państwowym, odmienną od dziedzin działalności podmiotów indywidualnych (wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 32 i przytoczone tam orzecznictwo).

93 Ponadto art. 3 dyrektywy 2002/58 stanowi, że dyrektywa ta 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 obsługującymi urządzenia służące do gromadzenia danych i identyfikacji (zwanych dalej „usługami łączności elektronicznej"). W konsekwencji należy uznać, że omawiana dyrektywa reguluje działalność dostawców tych usług (wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 33 i przytoczone tam orzecznictwo).

94 W tych ramach art. 15 ust. 1 dyrektywy 2002/58 pozwala państwom członkowskim uchwalić, z poszanowaniem przewidzianych w nim warunków, „środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4 i art. 9 tej dyrektywy" (wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 71).

95 Tymczasem art. 15 ust. 1 dyrektywy 2002/58 stosuje się siłą rzeczy przy założeniu, że krajowe środki ustawodawcze, które są w nim wymienione, wchodzą w zakres stosowania tej dyrektywy, ponieważ ta ostatnia upoważnia wyraźnie państwa członkowskie do ich przyjmowania wyłącznie z poszanowaniem ustanowionych w niej warunków. Ponadto takie środki regulują, do celów, o których mowa w tym przepisie, działalność dostawców usług łączności elektronicznej (wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 34 i przytoczone tam orzecznictwo).

96 To w szczególności w świetle tych rozważań Trybunał orzekł, że art. 15 ust. 1 w związku z art. 3 dyrektywy 2002/58 należy interpretować w ten sposób, iż do zakresu stosowania tej dyrektywy należy nie tylko środek ustawodawczy, który nakłada na dostawców usług łączności elektronicznej obowiązek zatrzymywania danych o ruchu i danych o lokalizacji, lecz również środek ustawodawczy zobowiązujący ich do udzielenia dostępu właściwym organom krajowym do tych danych. Takie środki ustawodawcze wymagają bowiem bezwzględnie przetwarzania wspomnianych danych przez omawianych dostawców i nie mogą zatem, w zakresie, w jakim regulują działalność tych dostawców, być traktowane jako działalność właściwa państwom, o której mowa w art. 1 ust. 3 omawianej dyrektywy (zob. podobnie wyrok z dnia 2 października 2018 r., Ministerio Fiscal,

C-207/16, EU:C:2018:788, pkt 35, 37 i przytoczone tam orzecznictwo).

97 Ponadto, biorąc pod uwagę rozważania zawarte w pkt 95 niniejszego wyroku oraz ogólną systematykę dyrektywy 2002/58, wykładnia tej dyrektywy, zgodnie z którą środki ustawodawcze, o których mowa w jej art. 15 ust. 1, są wyłączone z zakresu stosowania wspomnianej dyrektywy z tego względu, że cele, do których środki te muszą prowadzić, pokrywają się zasadniczo z celami działalności, o których mowa w art. 1 ust. 3 tej dyrektywy, pozbawiałaby ten art. 15 ust. 1 wszelkiej skuteczności (effet utile) (zob. podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 72, 73).

98 Pojęcie „działalności", o którym mowa w art. 1 ust. 3 dyrektywy 2002/58, nie może zatem – jak zasadniczo zauważył rzecznik generalny w pkt 75 opinii w sprawach połączonych La Quadrature du Net i in. (C-511/18 i C-512/18, EU:C:2020:6) - być interpretowane jako obejmujące środki ustawodawcze, o których mowa w art. 15 ust. 1 tej dyrektywy.

99 Postanowienia art. 4 ust. 2 TUE, na które powołały się rządy wymienione w pkt 89 niniejszego wyroku, nie mogą podważyć tego wniosku. Zgodnie bowiem z utrwalonym orzecznictwem Trybunału, chociaż to do państw członkowskich należy określenie ich podstawowych interesów bezpieczeństwa i podjęcie środków zmierzających do zapewnienia ich bezpieczeństwa zewnętrznego i wewnętrznego, sam fakt, że środek krajowy został przyjęty w celu ochrony bezpieczeństwa narodowego, nie może prowadzić do niemożności stosowania prawa Unii i zwalniać państw członkowskich z konieczności przestrzegania tego prawa [zob. podobnie wyroki: z dnia 4 czerwca 2013 r., ZZ, C-300/11, EU:C:2013:363, pkt 38; z dnia 20 marca 2018 r., Komisja/ Austria (Drukarnia państwowa), C-187/16, EU:C:2018:194, pkt 75, 76; a także z dnia 2 kwietnia 2020 r., Komisja/Polska, Węgry i Republika Czeska (Tymczasowy mechanizm relokacji osób ubiegających się o udzielenie ochrony międzynarodowej), C-715/17, C-718/17 i C-719/17, EU:C:2020:257, pkt 143, 170].

100 Prawdą jest, że w wyroku z dnia 30 maja 2006 r., Parlament/Rada i Komisja (C-317/04 i C-318/04, EU:C:2006:346, pkt 56–59), Trybunał orzekł, iż przekazywanie danych osobowych przez linie lotnicze organom publicznym państwa trzeciego w celu zapobiegania terroryzmowi i innym poważnym przestępstwom oraz zwalczania ich nie było zgodnie z art. 3 ust. 2 tiret pierwsze dyrektywy 95/46 objęte zakresem stosowania tej dyrektywy, ponieważ takie przekazywanie następuje w ramach ustanowionych przez organy publiczne, mających na celu ochronę bezpieczeństwa publicznego.

101 Niemniej jednak, biorąc pod uwagę rozważania zawarte w pkt 93, 95 i 96 niniejszego wyroku, orzecznictwo to nie znajduje odpowiedniego zastosowania do wykładni art. 1 ust. 3 dyrektywy 2002/58. Jak bowiem rzecznik generalny wskazał w istocie w pkt 70–72 swojej opinii w sprawach połączonych La Quadrature du Net i in. (C-511/18 i C-512/18, EU:C:2020:6), art. 3 ust. 2 tiret pierwsze dyrektywy 95/46, do którego odnosi się wspomniane orzecznictwo, wyłączył z zakresu stosowania tej ostatniej dyrektywy w sposób ogólny „działalność na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa" bez rozróżnienia w zależności od rozpatrywanego podmiotu przetwarzającego dane. Natomiast w ramach wykładni art. 1 ust. 3 dyrektywy 2002/58 takie rozróżnienie okazuje się niezbędne. Jak bowiem wynika z pkt 94–97 niniejszego wyroku, wszelkie przetwarzanie danych osobowych przez dostawców usług łączności elektronicznej objęte jest zakresem stosowania omawianej dyrektywy, w tym przetwarzanie wynikające z obowiązków nałożonych na nich przez organy publiczne, podczas gdy to ostatnie przetwarzanie mogło ewentualnie być objęte zakresem stosowania odstępstwa przewidzianego w art. 3 ust. 2 tiret pierwsze dyrektywy 95/46, biorąc pod uwagę bardziej ogólne sformułowanie tego przepisu, odnoszące się do wszelkiego przetwarzania, bez względu na podmiot przetwarzający, na rzecz bezpieczeństwa publicznego, obronności lub bezpieczeństwa państwa.

102 Co więcej, należy wskazać, że dyrektywa 95/46, rozpatrywana w sprawie, w której zapadł wyrok z dnia 30 maja 2006 r., Parlament/Rada i Komisja (C-317/04 i C-318/04, EU:C:2006:346), została

na mocy art. 94 ust. 1 rozporządzenia 2016/679 uchylona i zastąpiona przez to rozporządzenie ze skutkiem od dnia 25 maja 2018 r. Tymczasem, jakkolwiek w art. 2 ust. 2 lit. d) omawianego rozporządzenia sprecyzowano, że nie ma ono zastosowania do przetwarzania „przez właściwe organy" do celów w szczególności wykrywania i ścigania czynów zabronionych, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, to jednak z art. 23 ust. 1 lit. d) i h) tego rozporządzenia wynika, że przetwarzanie danych osobowych w tych samych celach przez osoby prywatne jest objęte zakresem stosowania tego rozporządzenia. Wynika z tego, że powyższa wykładnia art. 1 ust. 3, art. 3 i art. 15 ust. 1 dyrektywy 2002/58 jest spójna z wyznaczeniem zakresu stosowania rozporządzenia 2016/679, które ta dyrektywa uzupełnia i doprecyzowuje.

103 Natomiast kiedy państwa członkowskie wprowadzają bezpośrednio środki stanowiące odstępstwo od poufności łączności elektronicznej, bez nakładania obowiązków przetwarzania na dostawców usług łączności elektronicznej, ochrona danych osób, których dane dotyczą, jest objęta nie dyrektywą 2002/58, ale jedynie prawem krajowym, z zastrzeżeniem stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz.U. 2016, L 119, s. 89), a więc rozpatrywane środki muszą respektować w szczególności prawo krajowe rangi konstytucyjnej i wymogi EKPC.

104 Z powyższych rozważań wynika, że uregulowanie krajowe nakładające na dostawców usług łączności elektronicznej obowiązek zatrzymywania danych o ruchu i danych o lokalizacji w celu ochrony bezpieczeństwa narodowego i zwalczania przestępczości, takie jak rozpatrywane w postępowaniu głównym, jest objęte zakresem stosowania dyrektywy 2002/58.

*W przedmiocie wykładni art. 15 ust. 1 dyrektywy 2002/58*

105 Na wstępie 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 (zob. podobnie wyrok z dnia 17 kwietnia 2018 r., Egenberger, C-414/16, EU:C:2018:257, pkt 44).

106 Dyrektywa 2002/58 ma 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 zatrzymywania i przetwarzania danych. W szczególności omawiana dyrektywa zmierza, jak wynika z jej motywu 2, do zapewnienia pełnego poszanowania praw określonych w art. 7 i 8 karty. W tym względzie z uzasadnienia wniosku 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, 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".

107 W tym celu 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 – zatrzymywania tych komunikatów i tych danych bez ich zgody.

108 Co się tyczy w szczególności przetwarzania i przechowywania danych o ruchu przez dostawców usług łączności elektronicznej, z art. 6 oraz z motywów 22 i 26 dyrektywy 2002/58 wynika, że takie przetwarzanie jest dozwolone jedynie w zakresie i przez okres niezbędny do sprzedaży usług,

naliczania opłat za te usługi oraz świadczenia usług tworzących wartość dodaną. Po upływie tego okresu dane, które podlegały przetwarzaniu i przechowywaniu, powinny zostać usunięte lub zanonimizowane. W odniesieniu do danych o lokalizacji innych niż dane o ruchu art. 9 ust. 1 wspomnianej dyrektywy przewiduje, że dane te mogą być przetwarzane wyłącznie po spełnieniu pewnych warunków i po ich anonimizacji lub za zgodą użytkowników lub abonentów (zob. podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 86 i przytoczone tam orzecznictwo).

109 Tak więc przyjmując tę dyrektywę, prawodawca Unii skonkretyzował prawa ustanowione w art. 7 i 8 karty 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.

110 Jednakże art. 15 ust. 1 dyrektywy 2002/58 pozwala państwom członkowskim na wprowadzenie wyjątków od ustanowionego w art. 5 ust. 1 tej dyrektywy zasadniczego obowiązku zapewnienia poufności danych osobowych, a także od odpowiadających im obowiązków wymienionych w szczególności w art. 6 i 9 omawianej dyrektywy, kiedy takie ograniczenie jest niezbędne, właściwe i proporcjonalne w społeczeństwie demokratycznym do ochrony bezpieczeństwa narodowego, obronności i bezpieczeństwa publicznego lub do zapobiegania, dochodzenia, wykrywania i ścigania przestępstw lub niedozwolonego używania systemu łączności elektronicznej. W tym celu państwa członkowskie mogą między innymi przyjmować środki ustawodawcze przewidujące zatrzymywanie danych przez określony czas, jeśli jest to uzasadnione jednym z tych względów.

111 Jednakże ta możliwość wprowadzenia odstępstwa od praw i obowiązków przewidzianych w art. 5, 6 i 9 dyrektywy 2002/58 nie może uzasadniać tego, że odstępstwo od zasadniczego obowiązku zapewnienia poufności łączności elektronicznej i danych z nią związanych, a w szczególności zakazu przechowywania tych danych, wyraźnie przewidzianego w art. 5 tej dyrektywy, stanie się regułą (zob. podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 89, 104).

112 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 (zob. podobnie wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 52 i przytoczone tam orzecznictwo).

113 Ponadto z art. 15 ust. 1 zdanie trzecie dyrektywy 2002/58 wynika, że państwa członkowskie są upoważnione do przyjmowania środków ustawodawczych zmierzających do ograniczenia zakresu praw i obowiązków, o których mowa w art. 5, 6 i 9 tej dyrektywy, jedynie z poszanowaniem zasad ogólnych prawa Unii, do których należy zasada proporcjonalności, i 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 (zob. podobnie wyroki: z dnia 8 kwietnia 2014 r., Digital Rights, C-293/12 i C-594/12, EU:C:2014:238, pkt 25, 70; a także z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 91, 92 i przytoczone tam orzecznictwo).

114 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 pluralistycznego i demokratycznego społeczeństwa, stanowiąc część wartości, na jakich zgodnie z art. 2 TUE opiera się Unia (zob. podobnie wyroki: z dnia 6 marca 2001 r., Connolly/Komisja, C-274/99 P, EU:C:2001:127, pkt 39; a także z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 93 i przytoczone tam orzecznictwo).

115 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 [zob. podobnie opinia 1/15 (Umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 124, 126 i przytoczone tam orzecznictwo; zob. analogicznie, w odniesieniu do art. 8 EKPC, wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom, CE:ECHR:2020:0130JUD005000112, § 81].

116 Nie ma również znaczenia, czy zatrzymane dane są następnie wykorzystywane, czy też nie (zob. analogicznie, w odniesieniu do art. 8 EKPC, wyrok ETPC z dnia 16 lutego 2000 r. w sprawie Amann przeciwko Szwajcarii, CE:ECHR:2000:0216JUD002779895, § 69; a także z dnia 13 lutego 2020 r., Trjakovski i Chipovski przeciwko Macedonii Północnej, CE:ECHR:2020:0213JUD005320513, § 51), ponieważ dostęp do takich danych stanowi, niezależnie od sposobu ich późniejszego wykorzystania, odrębną ingerencję w prawa podstawowe, o których mowa w poprzednim punkcie [zob. podobnie opinia 1/15 (Umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 124, 126].

117 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, podejmowane czynności, relacje towarzyskie i środowiska społeczne, w których osoby te się obracają. W szczególności dane te dają możność ustalenia profilu osób, których dane dotyczą, zaś informacja ta jest z punktu widzenia prawa do poszanowania życia prywatnego równie newralgiczna co sama treść komunikatów (zob. podobnie wyroki: z dnia 8 kwietnia 2014 r., Digital Rights, C-293/12 i C-594/12, EU:C:2014:238, pkt 27; a także z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 99).

118 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 (zob. podobnie wyroki: z dnia 8 kwietnia 2014 r., Digital Rights, C-293/12 i C-594/12, EU:C:2014:238, pkt 28; a także z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 101). Taki zniechęcający wpływ może zostać wywarty w szczególności na osoby, których komunikowanie się podlega zgodnie z prawem krajowym tajemnicy zawodowej, oraz na sygnalistów, których działalność chroni dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (UE) (Dz.U. 2019, L 305, s. 17). Ponadto skutki te są tym dotkliwsze, że zatrzymywane dane są bardzo liczne i zróżnicowane.

119 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.

120 Niemniej jednak w zakresie, w jakim art. 15 ust. 1 dyrektywy 2002/58 umożliwia państwom członkowskim wprowadzenie odstępstw, o których mowa w pkt 110 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 (zob. podobnie wyrok z dnia 16 lipca 2020 r., Facebook Ireland i Schrems, C-311/18, EU:C:2020:559, pkt 172 i przytoczone tam orzecznictwo).

121 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.

122 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.

123 W tym względzie art. 6 karty, do którego odwołują się Conseil d'État (rada stanu, Francja) i Cour constitutionnelle (trybunał konstytucyjny, Belgia), ustanawia prawo każdego nie tylko do wolności, ale również do bezpieczeństwa osobistego oraz gwarantuje prawa odpowiadające prawom gwarantowanym w art. 5 EKPC (zob. podobnie wyroki: z dnia 15 lutego 2016 r., N., C-601/15 PPU, EU:C:2016:84, pkt 47; z dnia 28 lipca 2016 r., JZ, C-294/16 PPU, EU:C:2016:610, pkt 48; a także z dnia 19 września 2019 r., Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, pkt 42 i przytoczone tam orzecznictwo).

124 Ponadto należy przypomnieć, że art. 52 ust. 3 karty ma na celu zapewnienie niezbędnej spójności między prawami zawartymi w karcie a odpowiadającymi im prawami zagwarantowanymi w EKPC, bez naruszania autonomii prawa Unii i Trybunału Sprawiedliwości Unii Europejskiej. Do celów wykładni karty należy zatem uwzględnić odpowiednie prawa EKPC jako próg minimalnej ochrony [zob. podobnie wyroki: z dnia 12 lutego 2019 r., TC, C-492/18 PPU, EU:C:2019:108, pkt 57; a także z dnia 21 maja 2019 r., Komisja/Węgry (Użytki z gruntów rolnych), C-235/17, EU:C:2019:432, pkt 72 i przytoczone tam orzecznictwo].

125 Co się tyczy art. 5 EKPC, który ustanawia „prawo do wolności" i „prawo do bezpieczeństwa osobistego", zgodnie z orzecznictwem Europejskiego Trybunału Praw Człowieka ma on na celu ochronę jednostki przed arbitralnym lub nieuzasadnionym pozbawieniem wolności (zob. podobnie wyroki ETPC: z dnia 18 marca 2008 r. w sprawie Ladent przeciwko Polsce, CE:ECHR:2008:0318JUD001103603, §§ 45, 46; z dnia 29 marca 2010 r., Medvedyev i in. przeciwko Francji, CE:ECHR:2010:0329JUD000339403, §§ 76, 77; a także z dnia 13 grudnia 2012 r. w sprawie El-Masri przeciwko „The former Yugoslav Republic of Macedonia", CE:ECHR:2012:1213JUD003963009, § 239). Jednakże skoro przepis ten dotyczy pozbawienia wolności przez organ publiczny, art. 6 karty nie może być interpretowany w ten sposób, że nakłada on na organy publiczne obowiązek przyjęcia szczególnych środków w celu ukarania za określone przestępstwa.

126 Natomiast jeśli chodzi w szczególności o skuteczną walkę z przestępstwami, których ofiarą są zwłaszcza małoletni i inne osoby podatne na zagrożenia, na którą powołuje się Cour constitutionnelle (trybunał konstytucyjny, Belgia), należy podkreślić, że z art. 7 karty mogą wynikać ciążące na organach publicznych pozytywne obowiązki przyjęcia środków prawnych w celu ochrony życia prywatnego i rodzinnego [zob. podobnie wyrok z dnia 18 czerwca 2020 r., Komisja/ Węgry (Przejrzystość stowarzyszeń), C-78/18, EU:C:2020:476, pkt 123 i przytoczone tam

orzecznictwo Europejskiego Trybunału Praw Człowieka]. 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.

127 Tymczasem w obliczu tych różnych pozytywnych obowiązków należy w sposób niezbędny pogodzić ze sobą różne rozpatrywane interesy i prawa.

128 Europejski Trybunał Praw Człowieka orzekł bowiem, że pozytywne obowiązki wynikające z art. 3 i 8 EKPC, 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 dochodzenia i skutecznego 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 ze środkami prawnymi 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 interesy i prawa podlegające ochronie (wyroki ETPC: z dnia 28 października 1998 r. w sprawie Osman przeciwko Zjednoczonemu Królestwu, CE:ECHR:1998:1028JUD002345294, §§ 115, 116; z dnia 4 marca 2004 r., M.C. przeciwko Bułgarii, CE:ECHR:2003:1204JUD003927298, § 151; z dnia 24 czerwca 2004 r., Von Hannover przeciwko Niemcom, CE:ECHR:2004:0624JUD005932000, §§ 57, 58; a także z dnia 2 grudnia 2008 r. w sprawie K.U. przeciwko Finlandii, CE:ECHR:2008:1202JUD 000287202, §§ 46, 48, 49).

129 Co się tyczy poszanowania zasady proporcjonalności, w art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 przewidziano, że państwa członkowskie mogą uchwalić środek stanowiący odstępstwo od zasady poufności komunikacji i związanych z nią danych o ruchu, gdy taki środek jest „niezbędny, właściwy i proporcjonalny w ramach społeczeństwa demokratycznego” z punktu widzenia celów wymienionych w tym przepisie. W motywie 11 tej dyrektywy wyjaśniono, że środek tego rodzaju musi być „[ściśle]” proporcjonalny do zamierzonego celu.

130 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 [zob. podobnie wyroki: z dnia 16 grudnia 2008 r., Satakunnan Markkinapörssi i Satamedia, C-73/07, EU:C:2008:727, pkt 56; z dnia 9 listopada 2010 r., Volker und Markus Schecke i Eifert, C-92/09 i C-93/09, EU:C:2010:662, pkt 76, 77, 86; a także z dnia 8 kwietnia 2014 r., Digital Rights, C-293/12 i C-594/12, EU:C:2014:238, pkt 52; opinia 1/15 (Umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 140].

131 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, 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 (zob. podobnie wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 55 i przytoczone tam orzecznictwo).

132 Aby spełnić wymóg proporcjonalności, 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. 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 tym 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, jaką są dane szczególnie chronione (zob. podobnie wyroki: z dnia 8 kwietnia 2014 r., Digital Rights, C-293/12 i C-594/12, EU:C:2014:238, pkt 54, 55; a także z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 117; opinia 1/15 (Umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 141].

133 Zatem uregulowanie przewidujące zatrzymywanie danych osobowych powinno zawsze spełniać obiektywne kryteria wykazujące związek między danymi podlegającymi zatrzymaniu a zamierzonym celem [zob. podobnie opinia 1/15 (Umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 191 i przytoczone tam orzecznictwo; a także wyrok z dnia 3 października 2019 r., A i in., C-70/18, EU:C:2019:823, pkt 63].

– *W przedmiocie środków ustawodawczych przewidujących prewencyjne zatrzymywanie danych o ruchu i danych o lokalizacji w celu ochrony bezpieczeństwa narodowego*

134 Należy zauważyć, że cel ochrony bezpieczeństwa narodowego, na który powołują się sądy odsyłające i rządy, które przedstawiły uwagi, nie został jeszcze w sposób szczególny zbadany przez Trybunał w wyrokach dokonujących wykładni dyrektywy 2002/58.

135 W tym względzie należy na wstępie zauważyć, że art. 4 ust. 2 TUE stanowi, iż bezpieczeństwo narodowe państw członkowskich pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego. Odpowiedzialność ta obejmuje pierwszorzędny interes w ochronie podstawowych funkcji państwa i podstawowych interesów społeczeństwa, a także zapobieganie i ściganie działalności mogącej poważnie zdestabilizować podstawowe struktury konstytucyjne, polityczne lub społeczne kraju, w szczególności bezpośrednio zagrozić społeczeństwu, ludności lub państwu jako takiemu, zwłaszcza takiej jak działalność terrorystyczna.

136 Znaczenie celu ochrony bezpieczeństwa narodowego, w świetle art. 4 ust. 2 TUE, wykracza poza 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. Zagrożenia takie jak te, o których mowa w poprzednim punkcie, różnią się bowiem ze względu na swój charakter i szczególną wagą od ogólnych zagrożeń powstania napięć i problemów, choćby poważnych, dla bezpieczeństwa publicznego. Z zastrzeżeniem poszanowania innych wymogów przewidzianych w art. 52 ust. 1 karty cel ochrony bezpieczeństwa narodowego może więc uzasadnić środki związane z dalej idącą ingerencją w prawa podstawowe niż środki, które mogłyby być uzasadnione tymi innymi celami.

137 Tak więc w sytuacjach takich jak te opisane w pkt 135 i 136 niniejszego wyroku art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty nie stoi co do zasady na przeszkodzie środkowi ustawodawczemu, który zezwala właściwym organom na nakazanie dostawcom usług łączności elektronicznej zatrzymywania danych o ruchu i danych o lokalizacji wszystkich użytkowników środków łączności elektronicznej w ograniczonym okresie, o ile występują wystarczająco konkretne okoliczności, które pozwalają na uznanie, że w danym państwie członkowskim istnieje poważne zagrożenie, takie jak opisane w pkt 135 i 136 niniejszego wyroku, dla bezpieczeństwa narodowego, które jest rzeczywiste i aktualne lub przewidywalne. Nawet jeśli taki środek dotyczy, bez rozróżnienia, wszystkich użytkowników środków łączności elektronicznej, którzy na pierwszy rzut oka nie wydają się wykazywać związku, w rozumieniu orzecznictwa wskazanego w pkt 133 niniejszego wyroku, z zagrożeniem dla bezpieczeństwa narodowego tego państwa członkowskiego, to należy jednak uznać, że istnienie takiego zagrożenia może samo w sobie wskazywać na taki związek.

138 Nakaz przewidujący prewencyjne zatrzymywanie danych wszystkich użytkowników środków łączności elektronicznej musi jednak być ograniczony w czasie do tego, co absolutnie niezbędne. O ile nie można wykluczyć, że skierowany do dostawców usług łączności elektronicznej nakaz zatrzymywania danych może ze względu na utrzymywanie się takiego zagrożenia zostać odnowiony, o tyle czas obowiązywania każdego nakazu nie może przekraczać dającego się przewidzieć okresu. Ponadto takie zatrzymywanie danych powinno być ograniczone i powinny mu towarzyszyć ścisłe gwarancje umożliwiające skuteczną ochronę danych osobowych osób, których dane dotyczą, przed ryzykiem nadużyć. Zatrzymywanie to nie może zatem mieć charakteru systemowego.

139 Uwzględniając wagę ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty, wynikającej z takiego uogólnionego i niezróżnicowanego środka zatrzymywania danych, należy zapewnić, by korzystanie z niego było rzeczywiście ograniczone do sytuacji, w których istnieje poważne zagrożenie dla bezpieczeństwa narodowego, takich jak sytuacje, o których mowa w pkt 135 i 136 niniejszego wyroku. W tym celu istotne jest, aby decyzja nakazująca dostawcom usług łączności elektronicznej takie zatrzymywanie danych mogła być przedmiotem skutecznej kontroli albo przez sąd, albo przez niezależny organ administracyjny, którego decyzja jest wiążąca, zmierzającej do zweryfikowania, czy zaistniała jedna z tych sytuacji, a także czy zostały spełnione warunki i gwarancje, które powinny zostać przewidziane.

– *W przedmiocie środków ustawodawczych przewidujących prewencyjne zatrzymywanie danych o ruchu i danych o lokalizacji do celów zwalczania przestępczości i ochrony bezpieczeństwa publicznego*

140 Jeśli chodzi o cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu przestępstw, 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 w omawiane prawa podstawowe, które nie mają poważnego charakteru, mogą być uzasadnione celem polegającym na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu ogółu przestępstw [zob. podobnie wyroki: z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 102; a także z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 56, 57; opinia 1/15 (Umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 149].

141 Uregulowanie krajowe przewidujące uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji w celu zwalczania poważnej przestępczości wykracza poza granice tego, co absolutnie niezbędne, i nie może być uważane za uzasadnione w społeczeństwie demokratycznym, jak tego wymaga art. 15 ust. 1 dyrektywy 2002/58, w związku z art. 7, 8 i 11 oraz 52 ust. 1 karty (zob. podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 107).

142 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, biorąc pod uwagę, po pierwsze, zniechęcający wpływ na wykonywanie praw podstawowych ustanowionych w art. 7 i 11 karty, o którym mowa w pkt 118 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 z uwzględnieniem celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego oraz wagi, jaką należy im nadać.

143 Ponadto Trybunał podkreślił, że uregulowanie 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. Takie uregulowanie, wbrew wymogowi przypomnianemu w pkt 133 niniejszego wyroku, obejmuje 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 dowodów 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 (zob. podobnie wyroki: z dnia 8 kwietnia 2014 r., Digital Rights, C-293/12 i C-594/12, EU:C:2014:238, pkt 57, 58; a także z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 105).

144 W szczególności, jak orzekł już Trybunał, takie uregulowanie nie jest ograniczone do zatrzymywania danych w określonym czasie lub obszarze geograficznym czy też danych kręgu osób, które mogłyby być powiązane w taki czy inny sposób z poważnym przestępstwem lub osób, które mogłyby w inny sposób przyczynić się, poprzez zatrzymywanie ich danych, do walki z poważną przestępczością (zob. podobnie wyroki: z dnia 8 kwietnia 2014 r., Digital Rights, C-293/12 i C-594/12, EU:C:2014:238, pkt 59; z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 106).

145 Tymczasem 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 126 i 128 niniejszego wyroku, dotyczą ustanowienia przepisów umożliwiających skuteczne zwalczanie przestępstw, nie mogą uzasadniać tak poważnych ingerencji jak te wynikające z przepisów przewidujących zatrzymywanie danych o ruchu i danych o lokalizacji w prawa podstawowe ustanowione w art. 7 i 8 karty prawie całej ludności, gdy dane rozpatrywanych osób nie wykazują związku, choćby pośredniego, z zamierzonym celem.

146 Natomiast zgodnie z tym, co zostało wskazane w pkt 142–144 niniejszego wyroku, oraz mając na uwadze konieczność pogodzenia rozpatrywanych praw i interesów, cele w postaci zwalczania poważnej przestępczości, zapobiegania poważnym naruszeniom bezpieczeństwa publicznego oraz, a fortiori, ochrony bezpieczeństwa narodowego mogą uzasadniać, biorąc pod uwagę ich znaczenie w świetle pozytywnych obowiązków przypomnianych w poprzednim punkcie, do których odniósł się w szczególności Cour constitutionnelle (trybunał konstytucyjny, Belgia), szczególnie poważną ingerencję polegającą na ukierunkowanym zatrzymywaniu danych o ruchu i danych o lokalizacji.

147 I tak, jak Trybunał już orzekł, 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 przyjęciu przez państwo członkowskie przepisów krajowych dopuszczających w ramach prewencji ukierunkowane zatrzymywanie danych o ruchu i danych o lokalizacji w celu zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, jak również dla celów ochrony bezpieczeństwa narodowego, pod warunkiem że takie zatrzymywanie – w odniesieniu do kategorii danych podlegających zatrzymywaniu, stosowanych środków łączności, osób, których dane dotyczą, oraz przyjętego okresu zatrzymywania – nie będzie wykraczać poza to, co jest ściśle niezbędne (zob. podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 108).

148 Jeśli chodzi o ograniczenia, jakim powinien podlegać taki środek polegający na zatrzymywaniu danych, mogą one w szczególności zostać ustalone na podstawie kręgu osób, których dane dotyczą, ponieważ art. 15 ust. 1 dyrektywy 2002/58 nie stoi na przeszkodzie uregulowaniu opartemu na obiektywnych elementach, umożliwiającemu objęcie osób, których dane o ruchu i dane o lokalizacji mogą mieć związek, przynajmniej pośredni, z poważną przestępczością, przyczyniać się w taki lub inny sposób do walki z ową przestępczością lub też zapobiegać powstawaniu poważnych zagrożeń dla bezpieczeństwa publicznego czy zagrożeń dla bezpieczeństwa narodowego (zob. podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 111).

149 W tym względzie należy uściślić, że taki środek mógłby obejmować w szczególności te osoby,

które zostały wcześniej zidentyfikowane w ramach właściwych procedur krajowych na podstawie obiektywnych przesłanek jako stwarzające zagrożenie dla bezpieczeństwa publicznego lub bezpieczeństwa narodowego danego państwa członkowskiego.

150 Wyznaczenie granic środka przewidującego zatrzymywanie danych o ruchu i danych o lokalizacji może być również oparte na kryterium geograficznym, jeżeli właściwe organy krajowe uznają, na podstawie obiektywnych i niedyskryminujących przesłanek, że na jednym lub większej liczbie obszarów geograficznych istnieje wysokie ryzyko przygotowania lub popełnienia poważnych przestępstw (zob. podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 111). 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 lub strefy poboru opłat za przejazd.

151 W celu zapewnienia, by ingerencja związana ze środkami ukierunkowanego zatrzymywania opisanymi w pkt 147–150 niniejszego wyroku była zgodna z zasadą proporcjonalności, czas ich obowiązywania 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.

– *W przedmiocie środków ustawodawczych przewidujących prewencyjne zatrzymywanie adresów IP i danych dotyczących tożsamości cywilnej do celów walki z przestępczością i ochrony bezpieczeństwa publicznego*

152 Należy zauważyć, że adresy IP, jakkolwiek należą do danych o ruchu, są generowane bez związku z określonym komunikatem i służą przede wszystkim identyfikowaniu przez dostawców usług łączności elektronicznej osoby fizycznej będącej właścicielem urządzenia końcowego, poprzez które odbywa się komunikacja za pośrednictwem Internetu. I tak, w dziedzinie poczty elektronicznej oraz telefonii internetowej, skoro zatrzymywane są jedynie adresy IP nadawcy komunikatu, a nie adresy jego odbiorcy, adresy te same w sobie nie ujawniają żadnej informacji na temat osób trzecich, które kontaktowały się z osobą, od której pochodzi komunikat. Ta kategoria danych wykazuje zatem mniejszy stopień wrażliwości niż inne dane o ruchu.

153 Jednakże skoro adresy IP mogą być wykorzystywane w szczególności do wyczerpującego prześledzenia poruszania się internauty w sieci, a w konsekwencji jego działalności on-line, dane te pozwalają na ustalenie jego szczegółowego profilu. Tak więc zatrzymywanie i analizowanie wspomnianych adresów IP, jakiego wymaga takie śledzenie, stanowi poważną ingerencję w prawa podstawowe internauty ustanowione w art. 7 i 8 karty, mogącą wywierać zniechęcające skutki, takie jak te, o których mowa w pkt 118 niniejszego wyroku.

154 Tymczasem do celów koniecznego pogodzenia rozpatrywanych praw i interesów, wymaganego przez orzecznictwo przytoczone w pkt 130 niniejszego wyroku, należy uwzględnić okoliczność, że w przypadku przestępstwa popełnionego w Internecie adres IP może stanowić jedyny środek dochodzeniowy umożliwiający ustalenie tożsamości osoby, której adres ten został przypisany w chwili popełnienia tego przestępstwa. Do tego dochodzi fakt, że zatrzymywanie adresów IP przez dostawców usług łączności elektronicznej na czas dłuższy niż czas, na który zostały one przydzielone, nie wydaje się co do zasady konieczne do celów naliczania opłat za rozpatrywane usługi, w związku z czym wykrywanie przestępstw popełnionych w Internecie może z tego względu, jak wskazało kilka rządów w uwagach przedstawionych Trybunałowi, okazać się niemożliwe bez posłużenia się środkiem ustawodawczym na podstawie art. 15 ust. 1 dyrektywy 2002/58. Może tak być zwłaszcza, jak podniosły te rządy, w przypadku szczególnie poważnych przestępstw w dziedzinie pornografii dziecięcej, takich jak nabywanie, rozpowszechnianie, przekazywanie lub udostępnianie 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).

155 W tych okolicznościach, o ile prawdą jest, że środek ustawodawczy przewidujący zatrzymywanie adresów IP wszystkich osób fizycznych będących właścicielami urządzeń końcowych, przy pomocy których można uzyskać dostęp do Internetu, dotyczy osób, które na pierwszy rzut oka nie wykazują związku, w rozumieniu orzecznictwa przytoczonego w pkt 133 niniejszego wyroku, z realizowanymi celami i że internauci mają, zgodnie z tym, co zostało stwierdzone w pkt 109 niniejszego wyroku, prawo oczekiwać, na mocy art. 7 i 8 karty, że ich tożsamość nie będzie co do zasady ujawniana, środek ustawodawczy przewidujący uogólnione i niezróżnicowane zatrzymywanie jedynie adresów IP przypisanych do źródła połączenia nie wydaje się co do zasady sprzeczny z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, pod warunkiem że możliwość ta zostanie uzależniona od drobiazgowego spełnienia warunków materialnych i proceduralnych, które winny regulować wykorzystywanie tych danych.

156 Z uwagi na poważny charakter ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty, jaką pociąga za sobą to zatrzymywanie, jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniom dla bezpieczeństwa publicznego mogą, podobnie jak ochrona bezpieczeństwa narodowego, uzasadniać tę ingerencję. Ponadto okres zatrzymywania nie może przekraczać okresu ściśle niezbędnego w świetle zamierzonego celu. Wreszcie środek tego rodzaju powinien przewidywać ścisłe warunki i gwarancje dotyczące wykorzystywania tych danych, w szczególności do śledzenia komunikacji i działalności w Internecie prowadzonej przez osoby, których dane dotyczą.

157 Wreszcie, jeśli chodzi o dane dotyczące tożsamości cywilnej użytkowników środków łączności elektronicznej, dane te same w sobie nie pozwalają 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 ich adresy, żadnych informacji dotyczących rozpatrywanych połączeń, a w konsekwencji ich życia prywatnego. A zatem ingerencji, jaką pociąga za sobą zatrzymywanie tych danych, nie można co do zasady uważać za poważną (zob. podobnie wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 59, 60).

158 Z powyższego wynika, że zgodnie z tym, co zostało wskazane w pkt 140 niniejszego wyroku, środki ustawodawcze dotyczące przetwarzania tych danych 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 (zob. podobnie wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 62).

159 W tych okolicznościach, biorąc pod uwagę konieczność pogodzenia rozpatrywanych praw i interesów oraz ze względów wskazanych w pkt 131 i 158 niniejszego wyroku, należy uznać, że nawet w braku związku między wszystkimi użytkownikami środków łączności elektronicznej a realizowanymi celami art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11, a także art. 52 ust. 1 karty nie stoi na przeszkodzie środkowi ustawodawczemu zobowiązującemu dostawców usług łączności elektronicznej do zatrzymywania bez szczególnego terminu danych dotyczących tożsamości cywilnej wszystkich użytkowników środków łączności elektronicznej w celu zapobiegania, dochodzenia, wykrywania i karania przestępstw oraz ochrony bezpieczeństwa publicznego, przy czym nie jest konieczne, aby te przestępstwa lub zagrożenia czy naruszenia bezpieczeństwa publicznego były poważne.

– *W przedmiocie środków ustawodawczych przewidujących szybkie zatrzymywanie danych o ruchu i danych o lokalizacji do celów walki z poważną przestępczością*

160 W odniesieniu do 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 legislacyjnych przyjętych na podstawie art. 15 ust. 1 tej dyrektywy, takich jak opisane w pkt 134–159 niniejszego wyroku, należy zauważyć, że dane te powinny co do zasady zostać, w zależności od przypadku, usunięte lub zanonimizowane po upływie ustawowych terminów, w których zgodnie z krajowymi przepisami transponującymi tę dyrektywę powinno nastąpić ich przetwarzanie i przechowywanie.

161 Jednakże podczas tego przetwarzania i tego przechowywania danych mogą występować sytuacje, w których występuje 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 wykryte, jak i w sytuacji, w której ich istnienie po przeprowadzeniu obiektywnego badania wszystkich istotnych okoliczności może być racjonalnie podejrzewane.

162 W tym względzie należy zauważyć, że konwencja Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r. (seria traktatów europejskich – nr 185), która została podpisana przez 27 państw członkowskich i ratyfikowana przez 25 z nich, mająca na celu ułatwienie walki z przestępstwami popełnionymi za pośrednictwem sieci informatycznych, przewiduje w art. 14, że umawiające się strony przyjmą dla celów przeprowadzenia specjalnych dochodzeń i postępowań karnych pewne środki w odniesieniu do już zatrzymywanych danych o ruchu, takie jak dalsze zatrzymywanie tych danych. W szczególności art. 16 ust. 1 tej konwencji stanowi, że umawiające się strony przyjmują środki ustawodawcze, które są niezbędne do tego, by umożliwić ich właściwym organom nakazanie lub uzyskanie w inny sposób szybkiego zatrzymywania danych o ruchu przechowywanych przy pomocy systemu informatycznego, w szczególności gdy istnieją podstawy do tego, by sądzić, że dane te mogą zostać utracone lub zmodyfikowane.

163 W sytuacji takiej jak ta, o której mowa w pkt 161 niniejszego wyroku, z uwagi na konieczność pogodzenia rozpatrywanych praw i interesów, o której mowa w pkt 130 niniejszego wyroku, państwa członkowskie mogą przewidzieć w ustawodawstwie 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 oni dysponują.

164 Skoro 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. Ponadto w celu zapewnienia, by ingerencja, jaką niesie ze sobą środek tego rodzaju, była ograniczona do tego, co ściśle niezbędne, po pierwsze, obowiązek zatrzymywania powinien dotyczyć wyłącznie danych o ruchu i danych o lokalizacji, które mogą przyczynić się do wyjaśnienia rozpatrywanego poważnego przestępstwa lub naruszenia bezpieczeństwa narodowego. Po drugie, okres zatrzymywania danych powinien być ograniczony do tego, co ściśle niezbędne, przy czym może on jednak zostać przedłużony, jeżeli uzasadniają to okoliczności i cel wspomnianego środka.

165 W tym względzie należy uściślić, że takie szybkie zatrzymywanie nie musi być ograniczone do danych osób konkretnie podejrzanych o popełnienie przestępstwa lub naruszenie bezpieczeństwa narodowego. Środek taki, 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, a także biorąc pod uwagę rozważania zawarte w pkt 133 niniejszego wyroku, może, zgodnie z wyborem ustawodawcy i przy poszanowaniu ograniczenia do 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 i zawodowego lub określonych obszarów geograficznych, takich jak miejsce popełnienia i przygotowania rozpatrywanego przestępstwa lub naruszenia bezpieczeństwa narodowego. Ponadto dostęp właściwych organów do zatrzymanych w ten sposób danych musi być zapewniony z poszanowaniem warunków wynikających z orzecznictwa dokonującego wykładni dyrektywy 2002/58 (zob. podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 118–121 i przytoczone tam orzecznictwo).

166 Należy jeszcze dodać, że jak wynika w szczególności z pkt 115 i 133 niniejszego wyroku, 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 może co do zasady być uzasadniony jedynie celem interesu ogólnego, dla którego dostawcy ci zostali zobowiązani do takiego zatrzymywania. Wynika z tego w szczególności, że nie można w żadnym wypadku udzielić dostępu do takich danych do celów ścigania i ukarania zwykłego przestępstwa, jeżeli ich zatrzymywanie było uzasadnione celem walki z poważną przestępczością lub, a fortiori, celem ochrony bezpieczeństwa narodowego. Natomiast zgodnie z zasadą proporcjonalności, o której mowa w pkt 131 niniejszego wyroku, dostęp do danych zatrzymanych w celu walki z poważną przestępczością może – o ile zostaną spełnione materialne i proceduralne warunki towarzyszące takiemu dostępowi, o których mowa w poprzednim punkcie – być uzasadniony celem ochrony bezpieczeństwa narodowego.

167 W tym względzie państwa członkowskie mogą przewidzieć w swoim ustawodawstwie, że dostęp do danych o ruchu i do danych o lokalizacji może nastąpić, przy spełnieniu tych samych warunków materialnych i proceduralnych, w celu zwalczania poważnej przestępczości lub ochrony bezpieczeństwa narodowego, jeżeli wspomniane dane są zatrzymywane przez dostawcę w sposób zgodny z art. 5, 6 i 9 lub art. 15 ust. 1 dyrektywy 2002/58.

168 W świetle całości powyższych rozważań na pytania pierwsze w sprawach C-511/18 i C-512/18, a także na pytania pierwsze i drugie w sprawie C-520/18 należy udzielić odpowiedzi, 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, w celach, o których mowa w tym art. 15 ust. 1, 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 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;

– przewidującym w celu ochrony bezpieczeństwa narodowego, 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;

– przewidującym w celu ochrony bezpieczeństwa narodowego, zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego uogólnione i niezróżnicowane zatrzymywanie adresów IP przydzielonych źródłu połączenia, w okresie ograniczonym do tego, co ściśle niezbędne;

– przewidującym w celu ochrony bezpieczeństwa narodowego, zwalczania przestępczości i ochrony bezpieczeństwa publicznego, uogólnione i niezróżnicowane zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej; oraz

– umożliwiającym, w celu zwalczania poważnej przestępczości oraz, a fortiori, ochrony bezpieczeństwa narodowego, posłużenie się nakazem skierowanym do dostawców 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 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 warunków oraz że osoby, których dane dotyczą, dysponują skutecznymi gwarancjami chroniącymi przed ryzykiem nadużyć.

***W przedmiocie pytań drugiego i trzeciego w sprawie C-511/18***

169 Poprzez pytania drugie i trzecie w sprawie C-511/18 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 stoi on na przeszkodzie uregulowaniu krajowemu zobowiązującemu dostawców usług łączności elektronicznej do wdrożenia w ich sieciach środków umożliwiających, po pierwsze, zautomatyzowaną analizę oraz gromadzenie w czasie rzeczywistym danych o ruchu i danych o lokalizacji, a po drugie, gromadzenie w czasie rzeczywistym danych technicznych dotyczących położenia wykorzystywanych urządzeń końcowych, bez przewidzenia obowiązku informowania osób, których dane są w ten sposób przetwarzane i gromadzone.

170 Sąd odsyłający wyjaśnia, że techniki gromadzenia informacji przewidziane w art. L. 851-2-L. 851-4 CSI nie oznaczają dla dostawców usług łączności elektronicznej szczególnego wymogu zatrzymywania danych o ruchu i danych o lokalizacji. Co się tyczy w szczególności zautomatyzowanej analizy, o której mowa w art. L. 851-3 CSI, sąd ten zauważa, że przetwarzanie to ma na celu wykrycie, na podstawie określonych w tym celu kryteriów, połączeń mogących wskazywać na zagrożenie terrorystyczne. Co się tyczy gromadzenia w czasie rzeczywistym, o którym mowa w art. L. 851-2 CSI, wspomniany sąd stwierdza, że dotyczy ono tylko jednej lub wielu osób uprzednio zidentyfikowanych jako mogące mieć związek z zagrożeniem terrorystycznym. Zdaniem tego sądu te dwie techniki mogą zostać wdrożone wyłącznie w celu zapobiegania terroryzmowi i dotyczą danych, o których mowa w art. L. 851-1 i R. 851-5 CSI.

171 Na wstępie należy wyjaśnić, że okoliczność, iż zgodnie z art. L. 851-3 CSI przewidziana w nim zautomatyzowana analiza nie pozwala sama w sobie na zidentyfikowanie użytkowników, których dane są poddane tej analizie, nie stoi na przeszkodzie zakwalifikowaniu takich danych jako „danych osobowych”. Skoro bowiem procedura przewidziana w ust. IV tego przepisu umożliwia na późniejszym etapie identyfikację osoby lub osób, których dotyczą dane, których zautomatyzowana analiza wykazała, że mogą one wskazywać na istnienie zagrożenia terrorystyczne, to wszystkie osoby, których dane są przedmiotem zautomatyzowanej analizy, pozostają na podstawie tych danych możliwe do zidentyfikowania. Tymczasem zgodnie z definicją danych osobowych zawartą w art. 4 pkt 1 rozporządzenia 2016/679 takimi danymi są informacje dotyczące w szczególności możliwej do zidentyfikowania osoby.

*W przedmiocie zautomatyzowanej analizy danych o ruchu i danych o lokalizacji*

172 Z art. L. 851-3 CSI wynika, że przewidziana w nim zautomatyzowana analiza polega zasadniczo na

filtrowaniu wszystkich danych o ruchu i danych o lokalizacji zatrzymywanych przez dostawców usług łączności elektronicznej, dokonywanym przez nich na wniosek właściwych organów krajowych i na podstawie określonych przez nie parametrów. Wynika z tego, że wszystkie dane użytkowników środków łączności elektronicznej są weryfikowane co do tego, czy odpowiadają tym parametrom. W związku z tym należy uznać, że taka zautomatyzowana analiza oznacza dla rozpatrywanych dostawców usług łączności elektronicznej stosowanie w imieniu właściwego organu uogólnionego i niezróżnicowanego przetwarzania w formie wykorzystywania za pomocą zautomatyzowanego procesu w rozumieniu art. 4 pkt 2 rozporządzenia 2016/679 obejmującego wszystkie dane o ruchu i dane o lokalizacji wszystkich użytkowników środków łączności elektronicznej. Przetwarzanie to jest niezależne od późniejszego zbierania danych dotyczących osób zidentyfikowanych w następstwie zautomatyzowanej analizy, które jest dozwolone na podstawie art. L. 851-3 ust. IV CSI.

173 Tymczasem uregulowanie krajowe, które dopuszcza taką zautomatyzowaną analizę danych o ruchu i danych o lokalizacji, stanowi odstępstwo od ustanowionego w art. 5 dyrektywy 2002/58 zasadniczego obowiązku zapewnienia poufności łączności elektronicznej i danych z nią związanych. Takie uregulowanie stanowi również ingerencję w prawa podstawowe ustanowione w art. 7 i 8 karty, niezależnie od późniejszego wykorzystania tych danych. Wreszcie wspomniane uregulowanie, zgodnie z orzecznictwem przytoczonym w pkt 118 niniejszego wyroku, może wywierać zniechęcający wpływ na korzystanie z wolności wypowiedzi ustanowionej w art. 11 karty.

174 Ponadto ingerencja wynikająca ze zautomatyzowanej analizy danych o ruchu i danych o lokalizacji, takiej jak rozpatrywana w postępowaniu głównym, jest szczególnie poważna, ponieważ obejmuje ona w sposób uogólniony i niezróżnicowany dane osób korzystających ze środków łączności elektronicznej. Stwierdzenie to narzuca się tym bardziej z tego względu, że – jak wynika z przepisów krajowych rozpatrywanych w postępowaniu głównym – dane będące przedmiotem zautomatyzowanej analizy mogą ujawnić charakter informacji konsultowanych w Internecie. Co więcej, taka zautomatyzowana analiza ma zastosowanie w sposób ogólny do wszystkich osób korzystających ze środków łączności elektronicznej, a w konsekwencji również do tych, w odniesieniu do których nie istnieje żadna przesłanka mogąca sugerować, że ich zachowanie może mieć związek, choćby pośredni lub daleki, z działaniami terrorystycznymi.

175 Co się tyczy uzasadnienia takiej ingerencji, należy wyjaśnić, że ustanowiony w art. 52 ust. 1 karty wymóg, zgodnie z którym wszelkie ograniczenia korzystania z praw podstawowych muszą być przewidziane ustawą, oznacza, iż podstawa prawna, która pozwala na tę ingerencję, musi sama określać zakres ograniczenia wykonywania danego prawa (zob. podobnie wyrok z dnia 16 lipca 2020 r., Facebook Ireland i Schrems, C-311/18, EU:C:2020:559, pkt 175 i przytoczone tam orzecznictwo).

176 Ponadto, aby spełnić przypomniany w pkt 130 i 131 niniejszego wyroku wymóg proporcjonalności, zgodnie z którym odstępstwa od ochrony danych osobowych i jej ograniczenia muszą ograniczać się do tego, co ściśle niezbędne, przepisy krajowe regulujące dostęp właściwych organów do zatrzymanych danych o ruchu i danych o lokalizacji muszą spełniać wymogi wynikające z orzecznictwa przytoczonego w pkt 132 niniejszego wyroku. W szczególności takie uregulowanie nie może ograniczać się do wymogu, aby dostęp organów do danych odpowiadał celowi realizowanemu przez te uregulowania, lecz musi ono również ustanawiać materialne i proceduralne warunki regulujące to wykorzystanie [zob. analogicznie opinia 1/15 (umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 192 i przytoczone tam orzecznictwo].

177 W tym względzie należy przypomnieć, że szczególnie poważna ingerencja polegająca na uogólnionym i niezróżnicowanym zatrzymywaniu danych o ruchu i danych o lokalizacji, której dotyczą rozważania przedstawione w pkt 134–139 niniejszego wyroku, a także szczególnie poważna ingerencja, jaką stanowi ich zautomatyzowana analiza, mogą spełniać wymóg proporcjonalności jedynie w sytuacjach, w których państwo członkowskie stoi w obliczu poważnego zagrożenia dla bezpieczeństwa narodowego, które jest rzeczywiste i aktualne lub

przewidywalne, oraz pod warunkiem, że okres ich zatrzymywania jest ograniczony do tego, co ściśle niezbędne.

178 W sytuacjach takich jak te, o których mowa w poprzednim punkcie, przeprowadzenie zautomatyzowanej analizy danych o ruchu i danych o lokalizacji wszystkich użytkowników środków łączności elektronicznej przez ściśle ograniczony okres można uznać za uzasadnione w świetle wymogów wynikających z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty.

179 Niemniej jednak, aby zagwarantować, że korzystanie z takiego środka rzeczywiście ogranicza się do tego, co jest ściśle niezbędne do ochrony bezpieczeństwa narodowego, a bardziej konkretnie - do zapobiegania terroryzmowi, zgodnie z tym, co zostało stwierdzone w pkt 139 niniejszego wyroku, istotne jest, aby decyzja zezwalająca na przeprowadzenie zautomatyzowanej analizy mogła być przedmiotem skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja ma skutek wiążący, mającej na celu sprawdzenie, czy wystąpiła sytuacja uzasadniająca wspomniany środek, oraz weryfikację spełnienia warunków i gwarancji, które winny zostać przewidziane.

180 W tym względzie należy uściślić, że ustalone wcześniej modele i kryteria, na których opiera się ten rodzaj przetwarzania danych, powinny być, po pierwsze, konkretne i wiarygodne, pozwalające na uzyskanie rezultatów w postaci zidentyfikowania osób, na których mogłoby ciążyć racjonalne podejrzenie udziału w przestępstwach terrorystycznych, a po drugie, niedyskryminacyjne [zob. podobnie opinia 1/15 (umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 172].

181 Ponadto należy przypomnieć, że wszelka zautomatyzowana analiza dokonywana w oparciu o modele i kryteria oparte na założeniu, zgodnie z którym pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, stan zdrowia lub życie seksualne danej osoby mogłyby same w sobie i niezależnie od indywidualnego zachowania tej osoby mieć znaczenie w świetle zapobiegania terroryzmowi, naruszałaby prawa gwarantowane w art. 7 i 8 karty w związku z jej art. 21. Zatem modele i kryteria wcześniej określone do celów zautomatyzowanej analizy mającej na celu zapobieganie działaniom terrorystycznym stanowiącym poważne zagrożenie dla bezpieczeństwa narodowego nie mogą być oparte jedynie na tych szczególnie chronionych danych [zob. podobnie opinia 1/15 (umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 165].

182 Ponadto skoro zautomatyzowane analizy danych o ruchu i danych o lokalizacji wykazują nieuchronnie pewien odsetek błędów, każdy pozytywny wynik uzyskany w wyniku zautomatyzowanego przetwarzania należy poddać indywidualnej weryfikacji w sposób niezautomatyzowany przed przyjęciem indywidualnego środka wywołującego niekorzystne skutki dla osób, których dane dotyczą, takiego jak późniejsze gromadzenie danych o ruchu i danych o lokalizacji w czasie rzeczywistym, taki środek nie może być bowiem oparty w sposób decydujący na samym wyniku automatycznego przetwarzania. Podobnie, aby w praktyce zagwarantować, że wcześniej określone modele i kryteria, ich wykorzystanie oraz używane bazy danych nie będą miały charakteru dyskryminacyjnego i są ograniczone do tego, co ściśle niezbędne w świetle celu polegającego na zapobieganiu działaniom terrorystycznym stanowiącym poważne zagrożenie dla bezpieczeństwa narodowego, niezawodność i aktualność tych wcześniej ustalonych modeli i kryteriów oraz wykorzystywanych baz danych należy poddawać regularnemu przeglądowi [zob. podobnie opinia 1/15 (umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 173, 174]

*W przedmiocie gromadzenia w czasie rzeczywistym danych o ruchu i danych o lokalizacji*

183 Jeśli chodzi o gromadzenie w czasie rzeczywistym danych o ruchu i danych o lokalizacji, o którym mowa w art. L. 851-2 CSI, należy zauważyć, że można wydać na nie indywidualne zezwolenie w odniesieniu do „uprzednio zidentyfikowanej osoby, która może mieć związek z zagrożeniem [terrorystycznym]”. Podobnie, zgodnie z tym przepisem, „jeżeli istnieją poważne podstawy, by sądzić, że jedna lub więcej osób należących do otoczenia osoby, której dotyczy zezwolenie, może

dostarczyć informacji związanych z celem uzasadniającym zezwolenie, zezwolenie to może być również udzielone indywidualnie dla każdej z tych osób”.

184 Dane będące przedmiotem środka tego rodzaju pozwalają właściwym organom krajowym na obserwowanie w okresie ważności zezwolenia w sposób ciągły i w czasie rzeczywistym rozmówców, z którymi osoby, których dane dotyczą, się komunikują, wykorzystywanych przez nie środków, czasu trwania ich połączeń oraz ich miejsc pobytu i ich przemieszczania się. Podobnie wydaje się, że mogą one ujawnić charakter informacji konsultowanych w Internecie. Całokształt tych danych pozwala, jak wynika z pkt 117 niniejszego wyroku, na wyciągnięcie bardzo precyzyjnych wniosków dotyczących życia prywatnego osób, których dane dotyczą, oraz umożliwia ustalenie ich profilu, przy czym taka informacja jest równie newralgiczna z punktu widzenia prawa do poszanowania życia prywatnego, jak sama treść komunikatów.

185 Co się tyczy gromadzenia danych w czasie rzeczywistym, o którym mowa w art. L. 851-4 CSI, przepis ten zezwala na gromadzenie danych technicznych o lokalizacji urządzeń końcowych i na przekazywanie ich w czasie rzeczywistym służbom premiera. Takie dane umożliwiają właściwym służbom, w każdym momencie w okresie ważności zezwolenia, lokalizowanie w sposób ciągły i w czasie rzeczywistym używanych urządzeń końcowych, takich jak telefony komórkowe.

186 Tymczasem uregulowanie krajowe zezwalające na takie gromadzenie w czasie rzeczywistym, podobnie jak uregulowanie, które zezwala na zautomatyzowaną analizę danych, stanowi odstępstwo od ustanowionego w art. 5 dyrektywy 2002/58 zasadniczego obowiązku zapewnienia poufności łączności elektronicznej i związanych z nią danych. Stanowi ono zatem również ingerencję w prawa podstawowe ustanowione w art. 7 i 8 karty i może wywoływać zniechęcające skutki dla wykonywania wolności wypowiedzi zagwarantowanej w art. 11 karty.

187 Należy podkreślić, że ingerencja, jaką stanowi gromadzenie w czasie rzeczywistym danych umożliwiających zlokalizowanie urządzeń końcowych, jest szczególnie poważna, ponieważ dane te umożliwiają właściwym organom krajowym dokładne i stałe monitorowanie przemieszczania się użytkowników telefonów komórkowych. Skoro dane te należy uznać z tego względu za szczególnie newralgiczne, dostęp właściwych organów do takich danych w czasie rzeczywistym należy odróżnić od dostępu do nich w późniejszym czasie, przy czym pierwszy z nich jest bardziej dotkliwy, ponieważ umożliwia niemal dokładne śledzenie tych użytkowników (zob. analogicznie, w odniesieniu do art. 8 EKPC, wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji, CE:ECHR:2018:0208JUD003144612, § 74). Intensywność tej ingerencji rośnie ponadto w sytuacji, gdy gromadzenie w czasie rzeczywistym rozciąga się również na dane o ruchu osób, których dane dotyczą.

188 O ile cel polegający na zapobieganiu terroryzmowi, do którego dąży uregulowanie krajowe rozpatrywane w postępowaniu głównym, może, ze względu na jego znaczenie, uzasadniać ingerencję, jaką niesie ze sobą gromadzenie w czasie rzeczywistym danych o ruchu i danych o lokalizacji, o tyle środek taki może zostać zastosowany, biorąc pod uwagę jego szczególnie inwazyjny charakter, wyłącznie wobec osób, co do których istnieje ważny powód, by podejrzewać, że są one zaangażowane w taki lub inny sposób w działalność terrorystyczną. Co się tyczy danych osób nienależących do tej grupy, mogą one być jedynie przedmiotem dostępu w późniejszym czasie, który zgodnie z orzecznictwem Trybunału może mieć miejsce jedynie w szczególnych sytuacjach, takich jak te, w których chodzi o działalność terrorystyczną, oraz gdy istnieją obiektywne dowody pozwalające na uznanie, że dane te mogłyby w konkretnym przypadku rzeczywiście przyczynić się do zwalczania terroryzmu (zob. podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 119 i przytoczone tam orzecznictwo).

189 Ponadto decyzja zezwalająca na gromadzenie w czasie rzeczywistym danych o ruchu i danych o lokalizacji powinna opierać się na obiektywnych kryteriach przewidzianych w krajowym ustawodawstwie. W szczególności ustawodawstwo to powinno definiować, zgodnie z orzecznictwem przytoczonym w pkt 176 niniejszego wyroku, okoliczności i warunki, w jakich

można wydać zezwolenie na takie gromadzenie, i przewidywać, że – jak wskazano w poprzednim punkcie – może ono dotyczyć jedynie osób wykazujących związek z celem zapobiegania terroryzmowi. Ponadto decyzja zezwalająca na gromadzenie w czasie rzeczywistym danych o ruchu i danych o lokalizacji powinna opierać się na obiektywnych i niedyskryminacyjnych kryteriach przewidzianych w krajowym ustawodawstwie. Aby w praktyce zagwarantować przestrzeganie tych warunków, istotne jest, aby wdrożenie środka zezwalającego na gromadzenie w czasie rzeczywistym podlegało uprzedniej kontroli przeprowadzanej albo przez sąd, albo przez niezależny organ administracyjny, którego decyzja ma skutek wiążący, przy czym ten sąd lub ten organ powinien w szczególności upewnić się, że zezwolenie na takie gromadzenie w czasie rzeczywistym zostało wydane jedynie w granicach tego, co jest ściśle niezbędne (zob. podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 120). W pilnych i należycie uzasadnionych przypadkach kontrola powinna nastąpić w krótkim czasie.

*W przedmiocie informowania osób, których dane zostały zgromadzone lub poddane analizie*

190 Ważne jest, by właściwe organy krajowe gromadzące w czasie rzeczywistym dane o ruchu i dane o lokalizacji informowały o tym osoby, których dane dotyczą, w ramach właściwych procedur krajowych, w przypadku i od momentu, w którym taka informacja nie może zagrozić realizacji zadań spoczywających na tych organach. Informacja ta jest bowiem w rzeczywistości niezbędna, aby umożliwić tym osobom wykonywanie ich praw wynikających z art. 7 i 8 karty, domaganie się dostępu do ich danych osobowych objętych tymi środkami oraz, w razie potrzeby, ich sprostowania lub usunięcia, a także wniesienie, zgodnie z art. 47 akapit pierwszy karty, skutecznego środka prawnego przed sądem; takie prawo jest zresztą wyraźnie zagwarantowane w art. 15 ust. 2 dyrektywy 2002/58 w związku z art. 79 ust. 1 rozporządzenia 2016/679 [zob. podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 121 i przytoczone tam orzecznictwo; a także opinia 1/15 (umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 219, 220].

191 Co się tyczy informacji wymaganych w kontekście zautomatyzowanej analizy danych o ruchu i danych o lokalizacji, właściwy organ krajowy zobowiązany jest opublikować informacje o charakterze ogólnym dotyczące tej analizy, bez konieczności przedstawiania indywidualnych informacji osobom, których dane dotyczą. Natomiast w przypadku, gdy dane odpowiadają parametrom określonym w środku zezwalającym na zautomatyzowaną analizę i gdy organ ten dokonuje identyfikacji osoby, której dane dotyczą, w celu dokładniejszego przeanalizowania dotyczących jej danych, konieczne jest indywidualne poinformowanie tej osoby. Takie poinformowanie może jednak nastąpić jedynie w przypadku i od momentu, w którym nie może ono zagrozić realizacji zadań spoczywających na wspomnianym organie [zob. analogicznie opinia 1/15 (umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 222–224].

192 Mając na względzie całość powyższych rozważań, na pytania drugie i trzecie w sprawie C-511/18 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 nie stoi on na przeszkodzie uregulowaniu krajowemu zobowiązującemu dostawców usług łączności elektronicznej, po pierwsze, do posłużenia się zautomatyzowaną analizą oraz do gromadzenia w czasie rzeczywistym w szczególności danych o ruchu i danych o lokalizacji, a po drugie, do gromadzenia w czasie rzeczywistym danych technicznych o lokalizacji wykorzystywanych urządzeń końcowych, jeśli:

– posłużenie się zautomatyzowaną analizą ogranicza się do sytuacji, w których państwo członkowskie napotyka na poważne zagrożenie dla bezpieczeństwa narodowego, które okazuje się rzeczywiste i aktualne lub przewidywalne, przy czym posłużenie się tą analizą może podlegać skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja ma wiążący skutek, mającej na celu sprawdzenie, czy wystąpiła sytuacja uzasadniająca wspomniany środek, jak również weryfikację poszanowania warunków i gwarancji, które powinny zostać przewidziane, oraz

– korzystanie z gromadzenia w czasie rzeczywistym danych o ruchu i danych o lokalizacji jest ograniczone do osób, wobec których istnieje uzasadniony powód, by podejrzewać, że są one zaangażowane w taki lub inny sposób w działalność terrorystyczną, i podlega uprzedniej kontroli dokonywanej albo przez sąd, albo przez niezależny organ administracyjny, którego decyzja ma wiążący skutek, w celu zapewnienia, że takie gromadzenie w czasie rzeczywistym jest dozwolone jedynie w granicach tego, co jest ściśle niezbędne. W należycie uzasadnionych pilnych przypadkach kontrola powinna nastąpić w krótkim czasie.

***W przedmiocie pytania drugiego w sprawie C-512/18***

193 Poprzez pytanie drugie w sprawie C-512/18 sąd odsyłający dąży w istocie do ustalenia, czy przepisy dyrektywy 2000/31 w związku z art. 6–8 i 11 oraz art. 52 ust. 1 karty należy interpretować w ten sposób, że stoją one na przeszkodzie przepisom krajowym nakładającym na dostawców dostępu do usług internetowej komunikacji publicznej i na dostawców usług hostingowych obowiązek uogólnionego i niezróżnicowanego zatrzymywania między innymi danych osobowych dotyczących tych usług.

194 Uznając, że takie usługi wchodzą w zakres stosowania dyrektywy 2000/31, a nie dyrektywy 2002/58, sąd odsyłający jest zdania, że art. 15 ust. 1 i 2 dyrektywy 2000/31 w związku z jej art. 12 i 14 nie wprowadza sam w sobie zasadniczego zakazu zatrzymywania danych dotyczących tworzenia treści, od którego można jedynie odstąpić w drodze wyjątku. Sąd ten zastanawia się jednak, czy należy utrzymać tę ocenę, biorąc pod uwagę konieczność poszanowania praw podstawowych ustanowionych w art. 6–8 i 11 karty.

195 Ponadto sąd odsyłający wyjaśnia, że jego pytanie dotyczy obowiązku zatrzymywania przewidzianego w art. 6 LCEN w związku z dekretem nr 2011-219. Dane, które rozpatrywani dostawcy usług powinni zatrzymywać na tej podstawie, obejmują w szczególności dane dotyczące tożsamości cywilnej osób, które skorzystały z tych usług, takie jak ich imię i nazwisko, związane z nimi adresy pocztowe, powiązane z nimi adresy poczty elektronicznej lub konta, ich hasła, a w przypadku gdy zawarcie umowy lub otwarcie konta jest płatne, stosowany rodzaj płatności, numer płatności, kwotę, a także datę i godzinę transakcji.

196 Podobnie dane podlegające obowiązkowi zatrzymywania obejmują identyfikatory abonentów, połączeń i używanych urządzeń końcowych, identyfikatory przydzielone do treści, daty i godziny rozpoczęcia i zakończenia połączeń i czynności, a także rodzaje protokołów wykorzystywanych do połączenia z usługą i przekazywania treści. Można wnosić o udzielenie dostępu do tych danych, których okres zatrzymywania wynosi jeden rok, w ramach postępowań karnych i cywilnych w celu zapewnienia przestrzegania przepisów dotyczących odpowiedzialności cywilnej lub karnej, a także w ramach środków gromadzenia informacji, do których stosuje się art. L. 851-1 CSI.

197 W tym względzie należy zauważyć, że zgodnie z art. 1 ust. 2 dyrektywy 2000/31 zbliża ona niektóre przepisy krajowe mające zastosowanie do usług społeczeństwa informacyjnego, o których mowa w jej art. 2 lit. a).

198 Usługi takie obejmują wprawdzie usługi, które są świadczone na odległość za pomocą sprzętu elektronicznego do przetwarzania i przechowywania danych, na indywidualne żądanie odbiorcy usług i zwykle za wynagrodzeniem, takie jak usługi dostępu do Internetu lub sieci łączności oraz usługi hostingowe (zob. podobnie wyroki: z dnia 24 listopada 2011 r., Scarlet Extended, C-70/10, EU:C:2011:771, pkt 40; z dnia 16 lutego 2012 r., SABAM, C-360/10, EU:C:2012:85, pkt 34; z dnia 15 września 2016 r., Mc Fadden, C-484/14, EU:C:2016:689, pkt 55; a także z dnia 7 sierpnia 2018 r., SNB-REACT, C-521/17, EU:C:2018:639, pkt 42 i przytoczone tam orzecznictwo).

199 Jednakże art. 1 ust. 5 dyrektywy 2000/31 stanowi, że dyrektywa ta nie ma zastosowania do zagadnień odnoszących się do usług społeczeństwa informacyjnego, które są objęte dyrektywami 95/46 i 97/66. W tym względzie z motywów 14 i 15 dyrektywy 2000/31 wynika, że ochrona poufności porozumiewania się oraz osób fizycznych w związku z przetwarzaniem danych

osobowych w ramach usług społeczeństwa informacyjnego jest regulowana wyłącznie dyrektywami 95/46 i 97/66, z których ostatnia w art. 5 zakazuje dla celów poufności porozumiewania się wszelkich form przechwytywania lub nadzoru komunikatów.

200 Tym samym kwestie związane z ochroną poufności porozumiewania się i danych osobowych należy oceniać w świetle dyrektywy 2002/58 i rozporządzenia 2016/679, które zastąpiły, odpowiednio, dyrektywę 97/66 i dyrektywę 95/46, przy czym ochrona, jaką ma zapewnić dyrektywa 2000/31, w żadnym wypadku nie może naruszać wymogów wynikających z dyrektywy 2002/58 i z rozporządzenia 2016/679 (zob. podobnie wyrok z dnia 29 stycznia 2008 r., Promusicae, C-275/06, EU:C:2008:54, pkt 57).

201 Nałożony przez przepisy krajowe, o których mowa w pkt 195 niniejszego wyroku, na dostawców dostępu do usług internetowej komunikacji publicznej oraz na dostawców usług hostingowych obowiązek zatrzymywania danych osobowych związanych z tymi usługami należy zatem – jak wskazał w istocie rzecznik generalny w pkt 141 opinii w sprawach połączonych La Quadrature du Net i in. (C-511/18 i C-512/18, EU:C:2020:6) – oceniać w świetle dyrektywy 2002/58 lub rozporządzenia 2016/679.

202 Zatem w zależności od tego, czy świadczenie usług objętych tym uregulowaniem krajowym wchodzi w zakres dyrektywy 2002/58, będzie ono regulowane albo przez tę ostatnią dyrektywę, a w szczególności przez jej art. 15 ust. 1 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, albo przez rozporządzenie 2016/679, w szczególności przez art. 23 ust. 1 rzeczonego rozporządzenia w związku z tymi samymi postanowieniami karty.

203 W niniejszej sprawie nie można wykluczyć, jak wskazała Komisja Europejska w swoich uwagach na piśmie, że niektóre usługi, do których mają zastosowanie przepisy krajowe wskazane w pkt 195 niniejszego wyroku, stanowią usługi łączności elektronicznej w rozumieniu dyrektywy 2002/58, czego ustalenie należy do sądu odsyłającego.

204 W tym względzie należy zauważyć, że dyrektywa 2002/58 obejmuje usługi łączności elektronicznej, które spełniają warunki określone w art. 2 lit. c) dyrektywy 2002/21, do którego odsyła art. 2 dyrektywy 2002/58 i który definiuje usługę łączności elektronicznej jako „usługę zazwyczaj świadczoną za wynagrodzeniem, polegającą całkowicie lub częściowo [głównie] na przekazywaniu sygnałów w sieciach łączności elektronicznej, w tym usługi telekomunikacyjne i usługi transmisyjne świadczone poprzez sieci nadawcze”. Co się tyczy usług społeczeństwa informacyjnego, o których mowa w pkt 197 i 198 niniejszego wyroku, a które są objęte dyrektywą 2000/31, stanowią one usługi łączności elektronicznej, ponieważ polegają całkowicie lub głównie na przekazywaniu sygnałów w sieciach łączności elektronicznej (zob. podobnie wyrok z dnia 5 czerwca 2019 r., Skype Communications, C-142/18, EU:C:2019:460, pkt 47, 48).

205 Zatem usługi dostępu do Internetu, które wydają się objęte uregulowaniem krajowym, o którym mowa w pkt 195 niniejszego wyroku, stanowią, jak potwierdza motyw 10 dyrektywy 2002/21, usługi łączności elektronicznej w rozumieniu tej dyrektywy (zob. podobnie wyrok z dnia 5 czerwca 2019 r., Skype Communications, C-142/18, EU:C:2019:460, pkt 37). Jest tak również w przypadku usług poczty w Internecie, co do których nie wydaje się wykluczone, że wchodzą one również w zakres tego uregulowania krajowego, ponieważ z technicznego punktu widzenia wiążą się one całkowicie lub głównie z przekazywaniem sygnałów w sieciach łączności elektronicznej (zob. podobnie wyrok z dnia 13 czerwca 2019 r., Google, C-193/18, EU:C:2019:498, pkt 35, 38).

206 Jeśli chodzi o wymogi wynikające z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz z art. 52 ust. 1 karty, należy odesłać do wszystkich ustaleń i ocen dokonanych w ramach odpowiedzi udzielonej na pytania pierwsze w sprawach C-511/18 i C-512/18 oraz na pytania pierwsze i drugie w sprawie C-520/18.

207 Co się tyczy wymogów wynikających z rozporządzenia 2016/679, należy przypomnieć, że ma ono w szczególności na celu, jak wynika z jego motywu 10, zapewnienie wysokiego poziomu ochrony

osób fizycznych w Unii i w tym celu zapewnienie spójnego i jednolitego stosowania zasad ochrony podstawowych praw i wolności tych osób w odniesieniu do przetwarzania danych osobowych w całej Unii (zob. podobnie wyrok z dnia 16 lipca 2020 r., Facebook Ireland i Schrems, C-311/18, EU:C:2020:559, pkt 101).

208 W tym celu każde przetwarzanie danych osobowych powinno, z zastrzeżeniem odstępstw dopuszczalnych w art. 23 rozporządzenia 2016/679, być zgodne z zasadami dotyczącymi przetwarzania danych osobowych oraz praw osoby, której dane dotyczą, określonymi, odpowiednio, w rozdziałach II i III tego rozporządzenia. W szczególności każde przetwarzanie danych osobowych powinno, po pierwsze, być zgodne z zasadami określonymi w art. 5 wspomnianego rozporządzenia, a po drugie, spełniać przesłanki legalności wymienione w art. 6 tego rozporządzenia (zob. analogicznie, w odniesieniu do dyrektywy 95/46, wyrok z dnia 30 maja 2013 r., Worten, C-342/12, EU:C:2013:355, pkt 33 i przytoczone tam orzecznictwo).

209 Co się tyczy bardziej konkretnie art. 23 ust. 1 rozporządzenia 2016/679, należy zauważyć, że przepis ten, podobnie do tego, co przewidziano w art. 15 ust. 1 dyrektywy 2002/58, pozwala państwom członkowskim na ograniczenie, w świetle przewidzianych w nim celów oraz za pomocą środków ustawodawczych, zakresu obowiązków i praw, o których w nim mowa, „jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym” zamierzonemu celowi. Każdy akt ustawodawczy przyjęty na tej podstawie musi spełniać zwłaszcza szczególne wymogi określone w art. 23 ust. 2 tego rozporządzenia.

210 Tym samym art. 23 ust. 1 i 2 rozporządzenia 2016/679 nie może być interpretowany w ten sposób, że przyznaje on państwom członkowskim uprawnienie do naruszenia poszanowania życia prywatnego w sposób sprzeczny z art. 7 karty ani też innych gwarancji w niej przewidzianych (zob. analogicznie, w odniesieniu do dyrektywy 95/46, wyrok z dnia 20 maja 2003 r., Österreichischer Rundfunk i in., C-465/00, C-138/01 i C-139/01, EU:C:2003:294, pkt 91). W szczególności, podobnie jak w przypadku art. 15 ust. 1 dyrektywy 2002/58, uprawnienie przyznane państwom członkowskim na mocy art. 23 ust. 1 rozporządzenia 2016/679 może być wykonywane wyłącznie z poszanowaniem wymogu proporcjonalności, zgodnie z którym odstępstwa od ochrony danych osobowych i jej ograniczenia muszą ograniczać się do tego, co ściśle niezbędne (zob. analogicznie, w odniesieniu do dyrektywy 95/46, wyrok z dnia 7 listopada 2013 r., IPI, C-473/12, EU:C:2013:715, pkt 39 i przytoczone tam orzecznictwo).

211 Z powyższego wynika, że ustalenia i oceny dokonane w ramach odpowiedzi udzielonej na pytania pierwsze w sprawach C-511/18 i C-512/18, a także na pytania pierwsze i drugie w sprawie C-520/18 mają zastosowanie mutatis mutandis do art. 23 rozporządzenia 2016/679.

212 W świetle powyższych rozważań na pytanie drugie w sprawie C-512/18 należy odpowiedzieć, że dyrektywę 2000/31 należy interpretować w ten sposób, iż nie ma ona zastosowania w dziedzinie ochrony poufności porozumiewania się i osób fizycznych w związku z przetwarzaniem danych osobowych w ramach usług społeczeństwa informacyjnego, ponieważ ochrona ta jest w zależności od przypadku regulowana przez dyrektywę 2002/58 lub przez rozporządzenie 2016/679. Artykuł 23 ust. 1 rozporządzenia 2016/679 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty należy interpretować w ten sposób, że stoi on na przeszkodzie przepisom krajowym nakładającym na dostawców dostępu do usług internetowej komunikacji publicznej i na dostawców usług hostingowych obowiązek uogólnionego i niezróżnicowanego zatrzymywania między innymi danych osobowych dotyczących tych usług.

***W przedmiocie pytania trzeciego w sprawie C-520/18***

213 Poprzez pytanie trzecie w sprawie C-520/18 sąd odsyłający dąży w istocie do ustalenia, czy sąd krajowy może zastosować przepis prawa krajowego, który upoważnia go do ograniczenia w czasie skutków stwierdzenia niezgodności z prawem, którego ma on dokonać na mocy tego prawa w odniesieniu do ustawodawstwa krajowego nakładającego na dostawców usług łączności

elektronicznej obowiązek, między innymi dla realizacji celów związanych z ochroną bezpieczeństwa narodowego i zwalczaniem przestępczości, uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji, ze względu na jego niezgodność z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty.

214 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 [wyroki: z dnia 15 lipca 1964 r., Costa, 6/64, EU:C:1964:66, s. 1159, 1160; a także 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 i przytoczone tam orzecznictwo].

215 Zgodnie z zasadą pierwszeństwa w braku możliwości 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 nie stosując, z własnej inicjatywy, wszelkich sprzecznych z nimi przepisów prawa krajowego, także późniejszych, bez konieczności żądania uprzedniego zniesienia tych przepisów w drodze ustawodawczej lub w jakimkolwiek innym trybie konstytucyjnym ani bez konieczności oczekiwania na takie uchylenie [wyroki: z dnia 22 czerwca 2010 r., Melki i Abdeli, C-188/10 i C-189/10, EU:C:2010:363, pkt 43 i przytoczone tam orzecznictwo; z dnia 24 czerwca 2019 r., Popławski, C-573/17, EU:C:2019:530, pkt 58; a także 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 160].

216 Jedynie Trybunał może, w drodze wyjątku oraz 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 [zob. podobnie wyroki: z dnia 23 października 2012 r., Nelson i in., C-581/10 i C-629/10, EU:C:2012:657, pkt 89, 91; z dnia 23 kwietnia 2020 r., Herst, C-401/18, EU:C:2020:295, pkt 56, 57; a także z dnia 25 czerwca 2020 r., A i in. (turbiny wiatrowe w Aalter i Nevele), C-24/19, EU:C:2020:503, pkt 84 i przytoczone tam orzecznictwo].

217 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 (zob. podobnie wyrok z dnia 29 lipca 2019 r., Inter-Environnement Wallonie i Bond Beter Leefmile Vlaanderen, C-411/17, EU:C:2019:622, pkt 177 i przytoczone tam orzecznictwo).

218 Jednakże Trybunał orzekł w sprawie, w której rozważana była zgodność 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 Leefmile Vlaanderen, C-411/17, EU:C:2019:622, pkt 175, 176, 179, 181).

219 Tymczasem, w przeciwieństwie do pominięcia obowiązku proceduralnego takiego jak uprzednia

ocena oddziaływania przedsięwzięcia w szczególnej dziedzinie 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 analogicznej do tej, o której mowa w poprzednim punkcie. Utrzymanie w mocy skutków przepisów krajowych takich jak rozpatrywane w postępowaniu głównym oznaczałoby bowiem, że przepisy te w dalszym ciągu nakładają 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.

220 W związku z tym sąd odsyłający nie może zastosować przepisu prawa krajowego, który upoważnia go do ograniczenia w czasie skutków stwierdzenia niezgodności z prawem ustawodawstwa krajowego rozpatrywanego w postępowaniu głównym, którego ma on dokonać na mocy tego prawa.

221 Niemniej jednak w uwagach przedstawionych Trybunałowi VZ, WY i XX podnoszą, że pytanie trzecie porusza w sposób dorozumiany, lecz nieuchronny, kwestię, czy prawo Unii stoi na przeszkodzie wykorzystywaniu w ramach postępowania karnego informacji i dowodów uzyskanych w wyniku uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji niezgodnego z tym prawem.

222 W tym względzie i w celu udzielenia sądowi odsyłającemu użytecznej odpowiedzi 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 poważnych przestępstw, informacji i dowodów uzyskanych w wyniku takiego zatrzymywania danych sprzecznego z prawem Unii.

223 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 równoważności) (zob. podobnie wyroki: z dnia 6 października 2015 r., Târşia, C-69/14, EU:C:2015:662, pkt 26, 27; z dnia 24 października 2018 r., XC i in., C-234/17, EU:C:2018:853, pkt 21, 22 i przytoczone tam orzecznictwo; z dnia 19 grudnia 2019 r., Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, pkt 33).

224 Co się tyczy zasady równoważności, do sądu krajowego prowadzącego postępowanie karne oparte na informacjach lub dowodach uzyskanych z naruszeniem wymogów wynikających z dyrektywy 2002/58 należy zbadanie, czy prawo krajowe regulujące to postępowanie przewiduje mniej korzystne zasady w zakresie dopuszczalności i wykorzystania takich informacji i dowodów niż przepisy regulujące informacje i dowody uzyskane z naruszeniem prawa wewnętrznego.

225 Co się tyczy zasady skuteczności, należy zauważyć, 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 byłyby niepotrzebnie szkodliwe dla osoby podejrzanej o popełnienie przestępstw. Tymczasem cel ten może zgodnie z prawem krajowym zostać osiągnięty 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.

226 Niemniej jednak z orzecznictwa Trybunału wynika, że konieczność wykluczenia informacji i dowodów uzyskanych z naruszeniem przepisów prawa Unii powinna być oceniana w szczególności w świetle zagrożenia, jakie dopuszczalność takich informacji i dowodów stwarza dla poszanowania zasady kontradyktoryjności, a tym samym prawa do rzetelnego procesu (zob. podobnie wyrok z dnia 10 kwietnia 2003 r., Steffensen, C-276/01, EU:C:2003:228, pkt 76, 77). 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 (zob. podobnie wyrok z dnia 10 kwietnia 2003 r., Steffensen, C-276/01, EU:C:2003:228, pkt 78, 79).

227 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 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.

228 W świetle powyższych rozważań na pytanie trzecie w sprawie C-520/18 należy odpowiedzieć, że sąd krajowy nie może zastosować przepisu prawa krajowego, który upoważnia go do ograniczenia w czasie skutków stwierdzenia niezgodności z prawem, którego ma on dokonać na mocy tego prawa w odniesieniu do ustawodawstwa krajowego nakładającego na dostawców usług łączności elektronicznej obowiązek, w szczególności w celu ochrony bezpieczeństwa narodowego i zwalczania przestępczości, uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji niezgodnego z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty. Ów art. 15 ust. 1, interpretowany w świetle zasady skuteczności, zobowiązuje krajowy sąd karny do nieuwzględnienia informacji i dowodów uzyskanych w wyniku uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji niezgodnego z prawem Unii 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.

**W przedmiocie kosztów**

229 Dla stron w postępowaniach głównych niniejsze postępowanie ma charakter incydentalny, dotyczy bowiem kwestii podniesionych przed sądami odsyłającymi, do nich zatem należy rozstrzygnięcie o kosztach. Koszty poniesione w związku z przedstawieniem uwag Trybunałowi, inne niż koszty stron w postępowaniach głównych, 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, w celach, o których mowa w tym art. 15 ust. 1, prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji. Natomiast wspomniany art. 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 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;**

– **przewidującym w celu ochrony bezpieczeństwa narodowego, 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;**

– **przewidującym w celu ochrony bezpieczeństwa narodowego, zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego uogólnione i niezróżnicowane zatrzymywanie adresów IP przydzielonych źródłu połączenia, w okresie ograniczonym do tego, co ściśle niezbędne;**

– **przewidującym w celu ochrony bezpieczeństwa narodowego, zwalczania przestępczości i ochrony bezpieczeństwa publicznego uogólnione i niezróżnicowane zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej; oraz**

– **umożliwiającym, w celu zwalczania poważnej przestępczości oraz, a fortiori, ochrony bezpieczeństwa narodowego, posłużenie się nakazem skierowanym do dostawców 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 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 warunków 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 i 11 oraz art. 52 ust. 1 karty praw podstawowych należy interpretować w ten sposób, że nie stoi on na przeszkodzie uregulowaniu krajowemu zobowiązującemu dostawców usług łączności elektronicznej, po pierwsze, do posłużenia się zautomatyzowaną analizą oraz do gromadzenia w czasie rzeczywistym w szczególności danych o ruchu i danych o lokalizacji, a po drugie, do gromadzenia w czasie rzeczywistym danych technicznych o lokalizacji wykorzystywanych urządzeń końcowych, jeśli:**

– **posłużenie się zautomatyzowaną analizą ogranicza się do sytuacji, w których państwo członkowskie napotyka na poważne zagrożenie dla bezpieczeństwa narodowego, które okazuje się rzeczywiste i aktualne lub przewidywalne, przy czym posłużenie się tą analizą może podlegać skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja ma wiążący skutek, mającej na celu sprawdzenie, czy wystąpiła sytuacja uzasadniająca wspomniany środek, jak również weryfikację poszanowania warunków i gwarancji, które powinny zostać przewidziane, oraz**

– **korzystanie z gromadzenia w czasie rzeczywistym danych o ruchu i danych o lokalizacji jest ograniczone do osób, wobec których istnieje uzasadniony powód, by podejrzewać, że są one zaangażowane w taki lub inny sposób w działalność terrorystyczną, i podlega uprzedniej kontroli dokonywanej albo przez sąd, albo przez niezależny organ administracyjny, którego decyzja ma wiążący skutek, w celu zapewnienia, że takie gromadzenie w czasie rzeczywistym jest dozwolone jedynie w granicach tego, co jest ściśle niezbędne. W należycie uzasadnionych pilnych przypadkach kontrola powinna nastąpić w krótkim czasie.**

3) **Dyrektywę 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywę o handlu elektronicznym) należy interpretować w ten sposób, że nie ma ona zastosowania w dziedzinie ochrony poufności porozumiewania się i osób fizycznych w związku z przetwarzaniem danych osobowych w ramach usług społeczeństwa informacyjnego, ponieważ ochrona ta jest w zależności od przypadku regulowana przez dyrektywę 2002/58, zmienioną dyrektywą 2009/136, lub przez rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46. Artykuł 23 ust. 1 rozporządzenia 2016/679 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty praw podstawowych należy interpretować w ten sposób, że stoi on na przeszkodzie przepisom krajowym nakładającym na dostawców dostępu do usług internetowej komunikacji publicznej i na dostawców usług hostingowych obowiązek uogólnionego i niezróżnicowanego zatrzymywania między innymi danych osobowych dotyczących tych usług.**

4) **Sąd krajowy nie może zastosować przepisu prawa krajowego, który upoważnia go do ograniczenia w czasie skutków stwierdzenia niezgodności z prawem, którego ma on dokonać na mocy tego prawa w odniesieniu do ustawodawstwa krajowego nakładającego na dostawców usług łączności elektronicznej obowiązek, w szczególności w celu ochrony bezpieczeństwa narodowego i zwalczania przestępczości, uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji niezgodnego z art. 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. Ów art. 15 ust. 1, interpretowany w świetle zasady skuteczności, zobowiązuje krajowy sąd karny do nieuwzględnienia informacji i dowodów uzyskanych w wyniku uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji niezgodnego z prawem Unii 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.**

Podpisy

---

* Język postępowania: francuski.