Zbiór Orzeczeń

OPINIA RZECZNIKA GENERALNEGO
MANUELA CAMPOSA SÁNCHEZA-BORDONY
przedstawiona w dniu 15 stycznia 2020 r.[1]

Sprawy połączone C-511/18 i C-512/18

La Quadrature du Net,
French Data Network,
Fédération des fournisseurs d'accès à Internet associatifs,
Igwan.net (C-511/18)
przeciwko
Premier ministre,
Garde des Sceaux, ministre de la Justice,
Ministre de l'Intérieur,
Ministre des Armées

[wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Conseil d'État (radę stanu, Francja)]

Odesłanie prejudycjalne – Przetwarzanie danych osobowych i ochrona życia prywatnego w sektorze łączności elektronicznej – Ochrona bezpieczeństwa narodowego i walka z terroryzmem – Dyrektywa 2002/58/WE – Zakres zastosowania – Artykuł 1 ust. 3 – Artykuł 15 ust. 3 – Artykuł 4 ust. 2 TUE – Karta praw podstawowych Unii Europejskiej – Artykuły 6, 7, 8, 11, 47 i art. 52 ust. 1 – Uogólnione i niezróżnicowane zatrzymywanie danych dotyczących połączeń i danych umożliwiających identyfikację twórców treści – Zbieranie danych dotyczących ruchu i lokalizacji – Dostęp do danych

1. W ostatnich latach Trybunał kontynuował utrwaloną linię orzeczniczą w zakresie zatrzymywania i dostępu do danych osobowych, której kamieniami milowymi są następujące orzeczenia:

– wyrok z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in.[2], w którym stwierdzono nieważność dyrektywy 2006/24/WE[3] ze względu na to, że umożliwiała ona nieproporcjonalną ingerencję w prawa przyznane na mocy art. 7 i 8 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą");

– wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in.[4], w którym dokonano wykładni art. 15 ust. 1 dyrektywy 2002/58/WE[5];

1 Język oryginału: hiszpański.

2 Sprawy połączone C-293/12 i C-594/12, w których wyrok jest zwany dalej „wyrokiem Digital Rights", EU:C:2014:238.

3 Dyrektywa Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz.U. 2006, L 105, s. 54).

4 Sprawy połączone C-203/15 i C-698/15, w których wyrok jest zwany dalej „wyrokiem Tele2 Sverige i Watson", EU:C:2016:970.

5 Dyrektywa Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. 2002, L 201, s. 37).

– wyrok z dnia 2 października 2018 r., Ministerio Fiscal[6], w którym potwierdzono wykładnię tego samego przepisu dyrektywy 2002/58.

2. Wyroki te (w szczególności drugi z wymienionych) budzą niepokój władz niektórych państw członkowskich, ponieważ rzekomo prowadzą do pozbawienia ich instrumentu, który uznają za niezbędny dla zapewnienia bezpieczeństwa narodowego i walki z przestępczością i terroryzmem. Dlatego też niektóre z tych państw członkowskich opowiadają się za zmianą lub doprecyzowaniem tego orzecznictwa.

3. Tę samą obawę wyraziły niektóre sądy państw członkowskich w czterech wnioskach o wydanie orzeczenia w trybie prejudycjalnym[7], w odniesieniu do których przedstawiam dziś opinie.

4. Cztery wspomniane sprawy dotyczą przede wszystkim kwestii zastosowania dyrektywy 2002/58 do działań związanych z bezpieczeństwem narodowym oraz walką z terroryzmem. Gdyby dyrektywa ta miała mieć zastosowanie w tym zakresie, należałoby wyjaśnić, w jakim stopniu państwa członkowskie mogą ograniczyć chronione dyrektywą prawo do prywatności. Wreszcie należy przeanalizować, w jakim stopniu różne uregulowania krajowe (Zjednoczonego Królestwa[8], belgijskie[9] i francuskie[10]) w tej dziedzinie są zgodne z prawem Unii, którego wykładni dokonał Trybunał Sprawiedliwości.

I. Ramy prawne

A. Prawo Unii

1. Dyrektywa 2002/58

5. Artykuł 1 („Zakres i cel”) tej dyrektywy 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 we Wspólnocie tego typu danych oraz urządzeń i usług łączności elektronicznej.

[…]

3. Niniejsza dyrektywa nie ma zastosowania do działalności, która wykracza poza zakres Traktatu ustanawiającego Wspólnotę Europejską, takiej jak działalność określona w tytułach V i VI Traktatu o Unii Europejskiej, ani, w żadnym wypadku do działalności dotyczącej bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając dobrobyt gospodarczy państwa, gdy działalność odnosi się do spraw bezpieczeństwa państwa) i działalności państwa w dziedzinie prawa karnego”.

6 Sprawa C-207/16, w której wyrok jest zwany dalej „sprawą Ministerio Fiscal”, EU:C:2018:788.

7 Oprócz wspomnianych dwóch spraw (C-511/18 i C-512/18), sprawy: C-623/17, Privacy International; C-520/18, Ordre des barreaux francophones et germanophone i in.

8 Sprawa Privacy International, C-623/17.

9 Sprawa Ordre des barreaux francophones et germanophone i in., C-520/18.

10 Sprawy połączone La Quadrature du Net i in., C-511/18; C-512/18

6. Artykuł 3 („Usługi”) stanowi:

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

7. Artykuł 5 („Poufność komunikacji”) stanowi w ust. 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 [zatrzymywania], które jest niezbędne do przekazania komunikatu bez uszczerbku dla zasady poufności”.

8. Artykuł 6 („Dane o ruchu”) stanowi:

„1. Dane o ruchu dotyczące abonentów i użytkowników przetwarzane i przechowywane [zatrzymywane] 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”.

9. Artykuł 15 („Stosowanie niektórych przepisów dyrektywy 95/46/WE[[11]]”) w ust. 1 stanowi:

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

11 Dyrektywa 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).

2. Dyrektywa 2000/31[12]

10. Artykuł 14 tej dyrektywy stanowi:

„1. Państwa członkowskie zapewniają, żeby w przypadku świadczenia usługi społeczeństwa informacyjnego polegającej na przechowywaniu informacji przekazanych przez usługobiorcę usługodawca nie był odpowiedzialny za informacje przechowywane na żądanie usługobiorcy, pod warunkiem że:

[…].

3. Niniejszy artykuł nie ma wpływu na możliwość wymagania od usługodawcy przez sądy lub organy administracyjne, zgodnie z systemem prawnym państw członkowskich, żeby przerwał on naruszenia prawa lub im zapobiegł oraz nie ma wpływu na możliwość ustanowienia procedur regulujących usuwanie lub uniemożliwianie dostępu do tych informacji przez państwa członkowskie".

11. Artykuł 15 stanowi:

„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".

3. Rozporządzenie 2016/679[13]

12. Zgodnie z art. 2 („Materialny zakres stosowania") tego rozporządzenia:

„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;

c) przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;

12 Dyrektywa Parlamentu Europejskiego i Rady (WE) 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).

13 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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 (ogólne rozporządzenie o ochronie danych) (Dz.U. 2016, L 119, s. 1).

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.

[…]".

13. Artykuł 23 („Ograniczenia") ust. 1 tego rozporządzenia brzmi następująco:

„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".

14. W art. 95 („Stosunek do dyrektywy 2002/58/WE") rozporządzenie to 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/WE".

B. Prawo krajowe

1. Code de la sécurité intérieure (francuski kodeks bezpieczeństwa wewnętrznego)

15. Zgodnie z art. L. 851-1 tego kodeksu:

„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 code des postes et des communications électroniques kodeksu poczty i łączności elektronicznej] oraz osób, o których mowa w art. 6 ust. I pkt 1 i 2 loi n.º 2004-575 […] pour la confiance dans l'économie numérique [ustawy nr 2004-575 […] o zaufaniu w gospodarce cyfrowej], 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 […]".

16. W art. L. 851-2 i L. 851-4 tego kodeksu uregulowano, w różnych celach i na różne sposoby, dostęp administracyjny w czasie rzeczywistym do zatrzymywanych w ten sposób danych dotyczących połączeń.

17. Artykuł L. 851-2 zezwala, wyłącznie na potrzeby zapobiegania terroryzmowi, na zbieranie informacji lub dokumentów od tych samych podmiotów, o których mowa w art. L. 851-1. Takie zbieranie informacji, które dotyczy tylko jednej lub kilku osób wcześniej zidentyfikowanych jako mogące mieć związek z zagrożeniem terroryzmem, odbywa się w czasie rzeczywistym. To samo dotyczy art. L. 851-4, który zezwala na przekazanie w czasie rzeczywistym przez operatorów wyłącznie danych technicznych dotyczących lokalizacji urządzeń końcowych [14].

18. Artykuł L. 851-3 zezwala na zobowiązanie 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" [15].

19. Artykuł L. 851-5 stanowi, że pod pewnymi warunkami „dozwolone może być użycie urządzenia technicznego umożliwiającego lokalizację osoby, pojazdu lub przedmiotu w czasie rzeczywistym".

20. Zgodnie z art. L. 851-6 ust. I możliwe jest, pod pewnymi warunkami, „gromadzenie […] bezpośrednio, za pomocą przyrządu lub urządzenia technicznego, o którym mowa w art. 226-3 ust. 1 code pénal [kodeksu karnego], danych technicznych umożliwiających identyfikację urządzenia końcowego lub numeru abonenta jego użytkownika, jak również danych dotyczących lokalizacji używanych urządzeń końcowych".

14 Zdaniem sądu odsyłającego zastosowanie tych technik nie wiąże się z nałożeniem na dostawców dodatkowego wymogu przechowywania danych wykraczającego poza to, co jest konieczne do fakturowania ich usług, sprzedawania ich oraz świadczenia usług o wartości dodanej.

15 Zdaniem sądu odsyłającego wspomniana technika, która nie wiąże się z uogólnionym i niezróżnicowanym przechowywaniem danych, ma na celu jedynie gromadzenie przez określony czas tych spośród wszystkich danych o połączeniach przetwarzanych przez te podmioty, które mogłyby mieć związek z takim poważnym przestępstwem.

2. Code des postes et des communications électroniques (francuski kodeks poczty i łączności elektronicznej)

21. Zgodnie z art. L. 34-1, w jego brzmieniu mającym zastosowanie do okoliczności faktycznych:

„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 artykułów od 323-1 do 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] 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 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".

22. Na mocy art. R. 10-13 ust. I operatorzy powinni zatrzymywać do celów wykrywania, stwierdzania i ścigania przestępstw następujące dane:

„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".

23. Zgodnie z art. R. 10-13 ust. II tego samego przepisu w przypadku działalności w zakresie telefonii operator musi również zatrzymywać dane, które pozwalają na identyfikację pochodzenia i lokalizacji połączenia.

24. W myśl ust. III rzeczonego artykułu wspomniane dane muszą być zatrzymywane przez okres jednego roku od chwili ich zarejestrowania.

3. Loi n.º 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (francuska ustawa nr 2004-575 z dnia 21 czerwca 2004 r. o zaufaniu w gospodarce cyfrowej)

25. Artykuł 6 ust. II akapit pierwszy ustawy nr 2004-575 stanowi, że osoby, których działalność polega na oferowaniu dostępu do usług internetowej komunikacji publicznej, oraz 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 mają obowiązek „posiadać i zatrzymywać dane umożliwiające identyfikację każdego, kto przyczynił się do stworzenia treści lub części treści usług, których są usługodawcami".

26. Ustęp II akapit trzeci tego samego przepisu stanowi, że organ sądowy może zażądać od tych podmiotów przekazania danych wskazanych w akapicie pierwszym.

27. Ustęp II akapit ostatni stanowi, że dekret Conseil d'État (rady stanu) „określa dane, o których mowa w akapicie pierwszym, oraz określa czas trwania i szczegółowe zasady ich zatrzymywania"[16].

16 Informacje te zostały określone w drodze décret n.º 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 (dekretem nr 2011-219 z dnia 25 lutego 2011 r. w sprawie przechowywania danych umożliwiających identyfikację każdej osoby, która przyczyniła się do stworzenia treści umieszczonych w Internecie). W ramach tego dekretu na uwagę zasługują: a) art. 1 ust. 1, zgodnie z którym podmioty oferujące dostęp do usług komunikacji internetowej muszą przechowywać następujące dane: identyfikator połączenia, identyfikator przypisany do danego abonenta, identyfikator urządzenia końcowego użytego do połączenia, datę i godzinę rozpoczęcia i zakończenia połączenia, cechy charakterystyczne linii abonenta; b) zgodnie z art. 1 ust. 2 podmioty, które oferują, nawet nieodpłatnie, do publicznego udostępniania za pomocą usług publicznej komunikacji internetowej, przechowywanie sygnałów, tekstów, obrazów, dźwięków lub wszelkiego rodzaju wiadomości dostarczonych przez odbiorców tych usług, dla każdej operacji muszą przechowywać następujące dane: identyfikator połączenia u źródła komunikacji, identyfikator przypisany treści będącej przedmiotem operacji, rodzaje protokołów użytych do połączenia z usługą i do przekazania treści, charakter operacji, datę i godzinę operacji, identyfikator użyty przez autora operacji; oraz c) wreszcie, art. 1 ust. 3, który stanowi, że podmioty wymienione w dwóch poprzednich ustępach muszą zatrzymywać następujące informacje podane przez użytkownika przy zawarciu umowy lub tworzeniu konta: identyfikator połączenia podczas tworzenia konta; imię, nazwisko lub nazwę firmy; adresy pocztowe, użyte pseudonimy, adresy e-mail lub adresy konta, numery telefonów, zaktualizowane hasło i dane umożliwiające weryfikację lub zmianę hasła.

II. Okoliczności faktyczne i pytania prejudycjalne

A. Sprawa C-511/18

28. La Quadrature du Net, French Data Network, Igwan.net i Fédération des fournisseurs d'accès à internet associatifs (zwane dalej „skarżącymi") wniosły do Conseil d'État (rady stanu) o stwierdzenie nieważności kilku dekretów wykonawczych do niektórych przepisów kodeksu bezpieczeństwa wewnętrznego [17].

29. Skarżące twierdziły co do zasady, że zarówno zaskarżone dekrety, jak i wspomniane przepisy kodeksu bezpieczeństwa wewnętrznego są sprzeczne z prawem do poszanowania życia prywatnego, prawem do ochrony danych osobowych i prawem do skutecznego środka odwoławczego, zagwarantowanym, odpowiednio, w art. 7, 8 i 47 karty.

30. W związku z powyższym Conseil d'État (rada stanu) zwróciła się do Trybunału z następującymi pytaniami prejudycjalnymi:

„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, […] 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?".

17 Zaskarżone zostały następujące dekrety: a) décret n.º 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (dekret nr 2015-1185 z dnia 28 września 2015 r. w sprawie powołania wyspecjalizowanych służb wywiadowczych); b) décret n.º 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (dekret 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); c) décret n.º 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 libre VIII du code de la sécurité intérieure (dekret 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); oraz d) décret n.º 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (dekret nr 2016-67 z dnia 29 stycznia 2016 r. w sprawie technik gromadzenia danych wywiadowczych).

B. Sprawa C-512/18

31. Skarżące w sporze leżącym u podstawy sprawy C-511/18, z wyjątkiem Igwan.net, również zwróciły się do Conseil d'État (rady stanu) o stwierdzenie nieważności decyzji odmownej (wynikającej z bezczynności organu administracji) w przedmiocie skierowanego przez nie wniosku o uchylenie art. R. 10-13 code des postes et des communications électroniques oraz dekretu nr 2011-219 z dnia 25 lutego 2011 r.

32. Zdaniem tych skarżących zaskarżone przepisy nakładają obowiązek zatrzymywania danych dotyczących ruchu, lokalizacji i połączenia, który to obowiązek, ze względu na swój ogólny charakter, stanowi nieproporcjonalną ingerencję w prawo do poszanowania życia prywatnego i rodzinnego, prawo do ochrony danych osobowych i wolność wypowiedzi, zagwarantowane w art. 7, 8 i 11 karty, z naruszeniem art. 15 ust. 1 dyrektywy 2002/58.

33. W ramach wspomnianej skargi Conseil d'État (rada stanu) wystąpiła z następującym odesłaniem prejudycjalnym:

„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?".

III. Postępowanie przed Trybunałem i stanowiska stron

34. Niniejsze wnioski o wydanie orzeczenia w trybie prejudycjalnym zostały zarejestrowane w Trybunale Sprawiedliwości w dniu 3 sierpnia 2018 r.

35. Uwagi na piśmie zostały złożone przez La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, French Data Network, rządy: belgijski, czeski, cypryjski, duński, niemiecki, hiszpański, estoński, francuski, węgierski, irlandzki, polski, szwedzki i Zjednoczonego Królestwa, a także przez Komisję.

36. W dniu 9 września 2019 r. odbyła się jawna rozprawa, którą przeprowadzono łącznie także dla spraw C-623/17, Privacy International, i C-520/18, Ordre des barreaux francophones et germanophone i in. W rozprawie tej udział wzięły strony występujące w czterech postępowaniach w przedmiocie odesłań prejudycjalnych, wyżej wymienione rządy oraz rządy: Niderlandów i Norwegii, a także Komisja oraz Europejski Inspektor Ochrony Danych.

IV. Analiza

37. Pytania Conseil d'État (rady stanu) można podzielić na trzy grupy:

– po pierwsze, czy krajowe przepisy nakładające na dostawców usług łączności elektronicznej obowiązek zatrzymywania w uogólniony i niezróżnicowany sposób danych dotyczących połączeń (pierwsze pytanie w sprawie C-511/18 i w sprawie C-512/18), a w szczególności danych umożliwiających identyfikację twórców treści oferowanych przez wspomnianych dostawców (drugie pytanie w sprawie C-512/18), są zgodne z prawem Unii;

– po drugie, czy prawidłowość procedur gromadzenia danych dotyczących połączeń jest w każdym przypadku uzależniona od spełnienia wymogu informowania osób, których te dane dotyczą, kiedy prowadzone dochodzenia nie są zagrożone (trzecie pytanie w sprawie C-511/18).

– po trzecie, czy gromadzenie w czasie rzeczywistym danych dotyczących ruchu i lokalizacji, bez obowiązku ich zatrzymywania, jest zgodne – i na jakich warunkach – z dyrektywą 2002/58 (drugie pytanie w sprawie C-511/18).

38. Podsumowując, konieczne jest określenie, czy zgodne z prawem Unii są przepisy krajowe nakładające na dostawców usług łączności elektronicznej dwa rodzaje obowiązków: a) po pierwsze, *gromadzenia* niektórych danych, ale nie ich zatrzymywanie; b) po drugie, *zatrzymywanie* danych dotyczących połączeń i danych, które umożliwiają identyfikację twórców treści usług świadczonych przez rzeczonych dostawców.

39. Na wstępie należy rozstrzygnąć to, czy, właśnie ze względu na kontekst [18], w którym wspomniane przepisy krajowe zostały przyjęte (to znaczy w okolicznościach, w których bezpieczeństwo narodowe może być zagrożone), zastosowanie ma dyrektywa 2002/58.

A. W przedmiocie możliwości stosowania dyrektywy 2002/58

40. Sąd odsyłający uznaje, że sporne przepisy są objęte zakresem zastosowania dyrektywy 2002/58. Jego zdaniem wynika to z orzecznictwa ustalonego w wyroku Tele2 Sverige i Watson oraz potwierdzonego w wyroku Ministerio Fiscal.

41. Natomiast niektóre rządy, które wzięły udział w postępowaniu, twierdzą, że sporne przepisy nie są objęte wspomnianym zakresem. Na poparcie swojego stanowiska powołują się one m.in. na wyrok z dnia 30 maja 2006 r., Parlament/Rada i Komisja [19].

42. Zgadzam się z Conseil d'État (radą stanu), że wyrok Tele2 Sverige i Watson rozstrzygnął tę część debaty, potwierdzając, że dyrektywa 2002/58 ma zastosowanie co do zasady w przypadku, gdy dostawcy usług elektronicznych są ustawowo zobowiązani przez ustawę do zatrzymywania danych ich abonentów i do umożliwiania dostępu do nich organom władzy publicznej. Bez znaczenia jest przy tym okoliczność, że obowiązki są nakładane na dostawców ze względów związanych z bezpieczeństwem narodowym.

43. Należy podkreślić, że, gdyby pojawiła się rozbieżność między wyrokiem Tele2 Sverige i Watson a wcześniejszymi wyrokami, należałoby przyznać pierwszeństwo wyrokowi Tele2 Sverige i Watson, ponieważ jest on późniejszy i został potwierdzony wyrokiem Ministerio Fiscal. Uważam jednak, że taka rozbieżność nie występuje, co spróbuję wyjaśnić.

18 „Kontekst […] poważnych i trwałych zagrożeń dla bezpieczeństwa narodowego, a zwłaszcza zagrożenia terrorystycznego", jak wskazano w pytaniu pierwszym w sprawie C-511/18.

19 Sprawy połączone C-317/04 i C-318/04, w których wyrok jest zwany dalej „wyrokiem Parlament/Rada i Komisja", EU:C:2006:346.

1. Wyrok Parlament/Rada i Komisja

44. Sprawy rozstrzygnięte wyrokiem Parlament/Rada i Komisja dotyczyły:

– Porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych PNR [Passenger Name Records (nazwy rekordu pasażera)] dotyczących przelotu pasażera przez przewoźników lotniczych władzom amerykańskim [20];

– odpowiedniego charakteru ochrony danych osobowych zawartych w nazwach rekordu pasażera (PNR) przekazywanych wspomnianym organom [21].

45. Trybunał stwierdził, że przekazywanie tych danych stanowiło ich przetwarzanie mające na celu ochronę bezpieczeństwa publicznego, jak również działalność prowadzoną przez państwo w obszarze regulowanym prawem karnym. Zgodnie z art. 3 ust. 2 tiret pierwsze dyrektywy 95/46 obie sporne decyzje nie były objęte zakresem zastosowania tej dyrektywy.

46. Dane te były początkowo gromadzone przez przewoźników lotniczych w ramach działalności – sprzedaży biletów – objętej zakresem zastosowania prawa Unii. Jednakże przetwarzanie tych danych, jak wskazano w spornej decyzji, nie jest „[niezbędne] w celu świadczenia usług, lecz [uznaje się je] za niezbędne w celu ochrony bezpieczeństwa publicznego oraz w celu zwalczania przestępczości” [22].

47. Trybunał przyjął zatem, biorąc pod uwagę cel przetwarzania danych, podejście celowościowe: jeśli przetwarzanie to miało na celu ochronę bezpieczeństwa publicznego, należało uznać, że wykraczało poza zakres zastosowania dyrektywy 95/46. Cel ten nie był jednak jedynym decydującym kryterium [23], dlatego w wyroku podkreślono, że przekazanie to „następuje […] w ramach ustanowionych przez władze publiczne i mających na celu ochronę bezpieczeństwa publicznego” [24].

48. Wyrok Parlament/Rada i Komisja pozwala zatem na dokonanie oceny różnicy między klauzulą wyłączającą a klauzulą ograniczającą określoną w dyrektywie 95/46 (klauzule analogiczne do tych przewidzianych w dyrektywie 2002/58). W rzeczywistości jednak te dwa rodzaje klauzul dotyczą podobnych celów interesu ogólnego, co wywołuje powstanie wątpliwości co do ich odpowiedniego zakresu, jak wskazał rzecznik generalny Y. Bot [25].

20 Decyzja Rady 2004/496/WE z dnia 17 maja 2004 r. w sprawie zawarcia Porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych dotyczących nazwy rekordu pasażera (PNR) przez przewoźników lotniczych do departamentu bezpieczeństwa wewnętrznego Stanów Zjednoczonych, biura ceł i ochrony granic (Dz.U. 2004, L 183, s. 83; sprostowanie Dz.U. 2005, L 255, s. 168) (sprawa C-317/04).

21 Decyzja Komisji 2004/535/WE z dnia 14 maja 2004 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Passenger Name Record (PNR) pasażerów lotniczych przekazywanych do biura celnego i ochrony granic Stanów Zjednoczonych (Dz.U. 2004, L 235, s. 11) (sprawa C-318/04).

22 Wyrok Parlament/Rada i Komisja, pkt 57. W pkt 58 podkreślono, że okoliczność, iż „dane […] gromadzone są przez podmioty prywatne do celów działalności gospodarczej i że to te podmioty przekazują dane do państwa trzeciego”, nie oznacza, że rzeczone przekazanie nie stanowi jednego z przypadków niestosowania dyrektywy 95/46, wymienionych w art. 3 ust. 2 tiret pierwsze owej dyrektywy, gdyż „przekazanie to następuje […] w ramach ustanowionych przez władze publiczne i mających na celu ochronę bezpieczeństwa publicznego”.

23 Zostało to następnie podkreślone przez rzecznika generalnego Y. Bota w jego opinii w sprawie Irlandia/Parlament i Rada (C-301/06, EU:C:2008:558). Rzecznik Y. Bot stwierdził, że wyrok Parlament/Rada i Komisja „nie oznacza […], iż samo zbadanie celu, któremu ma służyć przetwarzanie danych osobowych, jest istotne dla włączenia lub wyłączenia takiego przetwarzania z zakresu stosowania systemu ochrony danych wprowadzonego dyrektywą 95/46. Należy również sprawdzić, w ramach jakiego rodzaju działalności ma miejsce takie przetwarzanie danych. Jedynie w przypadku, w którym takie przetwarzanie następuje w celu wykonywania działalności właściwej państwom lub władzom państwowym, odmiennej od dziedzin działalności jednostek, przetwarzanie to jest wyłączone ze wspólnotowego systemu ochrony danych osobowych, ustanowionego w dyrektywie 95/46, i to na podstawie art. 3 ust. 2 tiret pierwsze tej dyrektywy” (pkt 122).

24 Wyrok Parlament/Rada i Komisja, pkt 58. Głównym celem porozumienia było zobowiązanie przewoźników lotniczych świadczących usługi przewozu pasażerów między Unią a Stanami Zjednoczonymi do zapewnienia władzom amerykańskim dostępu elektronicznego do PNR (nazw rekordów pasażerów) znajdujących się w ich systemach informatycznych dotyczących kontroli rezerwacji i wylotów. Wprowadzało ono zatem formę współpracy międzynarodowej między Unią a Stanami Zjednoczonymi w celu zwalczania terroryzmu i innych poważnych przestępstw, próbując pogodzić ten cel z celem ochrony danych osobowych pasażerów. W tym kontekście nałożony na przewoźników obowiązek nie różnił się bardzo od bezpośredniej wymiany danych między organami publicznymi.

25 Opinia rzecznika generalnego Y. Bota w sprawie Irlandia/Parlament i Rada (C-301/06, EU:C:2008:558, pkt 127).

49. Wątpliwości te prawdopodobnie uzasadniają stanowisko zajęte przez państwa członkowskie, które opowiadają się za tym, że dyrektywa 2002/58 nie ma zastosowania w tym kontekście. W ocenie tych państw interes ochrony bezpieczeństwa narodowego jest zabezpieczany jedynie poprzez zastosowanie przewidzianego w art. 1 ust. 3 dyrektywy 2002/58 wyłączenia. Jednakże temu samemu interesowi służą również ograniczenia dozwolone na mocy art. 15 ust. 1 wymienionej dyrektywy, w tym ograniczenie dotyczące bezpieczeństwa narodowego. Przepis ów byłby zbędny, gdyby dyrektywa 2002/58 nie miałaby mieć zastosowania w przypadku jakiegokolwiek powołania się na bezpieczeństwo narodowe.

2. Wyrok Tele2 Sverige i Watson

50. W wyroku Tele2 Sverige i Watson rozpatrywana była kwestia zgodności z prawem Unii pewnych systemów krajowych nakładających na dostawców publicznie dostępnych usług łączności elektronicznej obowiązek zatrzymywania danych dotyczących łączności elektronicznej. Były to zatem co do zasady przypadki identyczne z tymi, których dotyczą rozpatrywane w niniejszej sprawie odesłania prejudycjalne.

51. Rozpatrując ponownie możliwość zastosowania prawa Unii – tym razem na mocy dyrektywy 2002/58 – Trybunał zauważył przede wszystkim, że „zakres zastosowania dyrektywy 2002/58 należy oceniać przy uwzględnieniu, w szczególności, jej ogólnej systematyki” [26].

52. W tym kontekście Trybunał wskazał, iż „[p]rawdą jest, że środki ustawodawcze, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, odnoszą się do działalności właściwej państwom lub władzom państwowym i niezwiązanej z dziedzinami, w których prowadzą działalność jednostki […]. Co więcej, cele, do których, zgodnie z tym przepisem, środki te muszą prowadzić, w niniejszym przypadku ochrona bezpieczeństwa narodowego […], pokrywają się zasadniczo z celami działalności, o których mowa w art. 1 ust. 3 tej dyrektywy” [27].

53. Cel środków, które zgodnie z art. 15 ust. 1 dyrektywy 2002/58 mogą być podejmowane przez państwa członkowskie w celu ograniczenia prawa do poszanowania życia prywatnego (w tym względzie), pokrywa się zatem z celem uzasadniającym wyłączenie niektórych rodzajów działalności państwowej z systemu ustanowionego dyrektywą, zgodnie z jej art. 1 ust. 3.

54. Jednakże Trybunał uznał, iż, „z uwagi na ogólną systematykę dyrektywy 2002/58”, okoliczność ta nie pozwalała na „stwierdzenie, że środki ustawodawcze, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, są wyłączone z zakresu stosowania tej dyrektywy, gdyż brak tego wyłączenia oznaczałby pozbawienie rzeczonego art. 15 ust. 1 wszelkiej skuteczności (effet utile). Przy stosowaniu tego przepisu należy bowiem założyć, że środki krajowe, które są w nim wymienione, […] wchodzą w zakres stosowania tej dyrektywy, ponieważ ta ostatnia upoważnia wyraźnie państwa członkowskie do ich przyjmowania wyłącznie z poszanowaniem ustanowionych w niej warunków” [28].

55. Ponadto ograniczenia dozwolone na mocy art. 15 ust. 1 dyrektywy 2002/58 „normują działalność dostawców usług łączności elektronicznej do celów, o których mowa w tym przepisie”. Dlatego też rzeczony przepis, w związku z art. 3 wymienionej dyrektywy, „należy interpretować w ten sposób, że owe środki ustawodawcze są objęte zakresem jej stosowania” [29].

26 Wyrok Tele2 Sverige i Watson, pkt 67.

27 Ibidem, pkt 72.

28 Ibidem, pkt 73.

29 Ibidem, pkt 74.

56. W konsekwencji Trybunał uznał, że zakresem zastosowania dyrektywy 2002/58 objęty jest zarówno środek ustawodawczy, który nakłada na dostawców „obowiązek zatrzymywania danych o ruchu i danych o lokalizacji, ponieważ taka działalność niewątpliwie wiąże się z przetwarzaniem przez nich danych osobowych”[30], jak i środek ustawodawczy dotyczący dostępu władz do danych zatrzymywanych przez tych dostawców[31].

57. Przyjęta przez Trybunał w wyroku Tele2 Sverige i Watson wykładnia dyrektywy 2002/58 została przezeń powtórzona w wyroku Ministerio Fiscal.

58. Czy można uznać, że wyrok Tele2 Sverige i Watson stanowi mniej lub bardziej dorozumiany zwrot w stosunku do orzecznictwa wynikającego z wyroku Parlament/Rada i Komisja? Takie jest np. stanowisko rządu Irlandii, którego zdaniem tylko ten ostatni wyrok jest zgodny z podstawą prawną dyrektywy 2002/58 i nie narusza art. 4 ust. 2 TUE[32].

59. Rząd francuski uważa z kolei, że sprzeczności można uniknąć, jeśli weźmie się pod uwagę, iż orzecznictwo wynikające z wyroku Tele2 Sverige i Watson odnosi się do działalności prowadzonej państw członkowskich w obszarze uregulowanym prawem karnym, natomiast stanowisko przyjęte w wyroku Parlament/Rada i Komisja dotyczy bezpieczeństwa i obronności państwa. W związku z tym orzecznictwo wynikające z wyroku Tele2 Sverige i Watson nie miałoby zastosowania do niniejszej sprawy, w której należałoby oprzeć się na rozwiązaniu przyjętym w wyroku Parlament/Rada i Komisja[33].

60. Jak już wskazałem, uważam, że można znaleźć rozwiązanie pośrednie między tymi dwoma wyrokami, inne jednak niż to zaproponowane przez rząd francuski. Nie podzielam zaproponowanego przezeń rozwiązania, ponieważ moim zdaniem ustalenia zawarte w wyroku Tele2 Sverige i Watson, wyraźnie odnoszące się do walki z terroryzmem[34], można rozszerzyć na wszelkie inne zagrożenia dla bezpieczeństwa narodowego (terroryzm jest tylko jednym z nich).

3. Możliwość dokonania wykładni wyroku Parlament/Rada i Komisja w sposób zgodny z wyrokiem Tele2 Sverige i Watson

61. Moim zdaniem w wyrokach Tele2 Sverige i Watson oraz Ministerio Fiscal Trybunał wziął pod uwagę podstawy ustanowienia klauzul wyłączającej i ograniczającej, a także – istniejący między tymi dwoma rodzajami klauzul związek systemowy.

62. Choć w sprawie Parlament/Rada i Komisja Trybunał stwierdził, że przetwarzanie danych nie wchodzi w zakres zastosowania dyrektywy 95/46, to, jak już wskazałem, owo stwierdzenie wynikało z okoliczności, iż, w kontekście prowadzonej między Unią Europejską a Stanami Zjednoczonymi współpracy w ramach typowych stosunków międzynarodowych, państwowy wymiar działalności musiał mieć pierwszeństwo przed faktem, że wspomniane przetwarzanie miało również wymiar handlowy lub prywatny. Jedną z rozpatrywanych wówczas kwestii było właśnie to, jaka jest właściwa podstawa prawna spornej decyzji.

30 Ibidem, pkt 75.

31 Ibidem, pkt 76.

32 Punkty 15 i 16 uwag na piśmie rządu irlandzkiego.

33 Punkty 34–50 uwag na piśmie rządu francuskiego.

34 Wyrok Tele2 Sverige i Watson, pkt 103, 119.

63. Natomiast w odniesieniu do środków krajowych rozpatrywanych w wyrokach Tele2 Sverige i Watson oraz Ministerio Fiscal Trybunał przyznał pierwszeństwo wewnętrznemu aspektowi przetwarzania danych: ramy prawne, w których dokonywano tego przetwarzania, były wyłącznie krajowe, w związku z czym pozbawione aspektu zewnętrznego, który charakteryzował przedmiot wyroku Parlament/Rada i Komisja.

64. Skutkiem przypisywania aspektom: międzynarodowemu i wewnętrznemu (handlowemu i prywatnemu) przetwarzania danych różnego znaczenia było to, że w pierwszym przypadku klauzula wyłączająca zastosowanie prawo Unii została ustanowiona jako najbardziej odpowiednia dla ochrony interesu ogólnego dotyczącego ochrony bezpieczeństwa narodowego. Natomiast tym w drugim przypadku realizacji wspomnianego interesu mogła skutecznie służyć przewidziana w art. 15 ust. 1 dyrektywy 2002/58 klauzula ograniczająca.

65. Należałoby jeszcze uwzględnić inną rozbieżność, związaną z odmiennym kontekstem normatywnym: każdy z tych wyroków koncentrował się na wykładni dwóch przepisów, które, wbrew temu, co widać na pierwszy rzut oka, nie są takie same.

66. Wyrok Parlament/Rada i Komisja dotyczył bowiem wykładni art. 3 ust. 2 dyrektywy 95/46, natomiast wyrok Tele2 Sverige i Watson dotyczył art. 1 ust. 3 dyrektywy 2002/58. Po uważnym zapoznaniu się z tymi przepisami można zauważyć rozbieżność wystarczającą do uzasadnienia kierunków, w którym podążył Trybunał w jednym i w drugim z wydanych przezeń wyroków.

67. Zgodnie z art. 3 ust. 2 dyrektywy 95/46 „[n]iniejsza dyrektywa *nie ma zastosowania do przetwarzania danych osobowych* […] w ramach działalności wykraczającej poza zakres prawa Wspólnoty, […] a w żadnym razie do *działalności* na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarczą państwa, gdy *działalność* ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności państwa w obszarach prawa karnego” [35].

68. Natomiast zgodnie z art. 1 ust. 3 dyrektywy 2002/58 dyrektywa ta „*nie ma zastosowania do działalności*, która wykracza poza zakres traktatu ustanawiającego Wspólnotę Europejską […], 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” [36].

69. O ile art. 3 ust. 2 dyrektywy 95/46 wyłącza *przetwarzanie danych* – w zakresie, w jakim jest to istotne dla niniejszej sprawy – na rzecz bezpieczeństwa państwa, art. 1 ust. 3 dyrektywy 2002/58 wprowadza to wyłączenie w odniesieniu do *działalności* mającej na celu zapewnienie – również w zakresie, w jakim jest to istotne dla niniejszej sprawy – bezpieczeństwa państwa.

70. Różnica ta nie jest bez znaczenia. Dyrektywa 95/46 wyłączyła ze swojego zakresu zastosowania działalność („przetwarzanie danych osobowych”), która może być wykonywana przez kogokolwiek. Wyłączone zostało w szczególności przetwarzanie, którego przedmiotem było m.in. bezpieczeństwo państwa. Charakter *podmiotu* przetwarzającego dane był jednak bez znaczenia. Podejście przyjęte w celu określenia wyłączonych z zakresu zastosowania rodzajów działalności było zatem celowościowe podobnie jak brak rozróżnienia w odniesieniu do wykonujących je podmiotów.

35 Wyróżnienie własne.

36 Wyróżnienie własne.

71. Widać zatem, że w sprawie Parlament/Rada i Komisja Trybunał wziął przede wszystkim pod uwagę cel, jakiemu służy przetwarzanie danych. Nie miał przy tym znaczenia fakt, że „dane […] gromadzone są przez podmioty prywatne do celów działalności gospodarczej i że to te podmioty przekazują dane do państwa trzeciego", ponieważ zasadniczą kwestią była okoliczność polegająca na tym, iż „przekazanie to następuje […] w ramach ustanowionych przez władze publiczne i mających na celu ochronę bezpieczeństwa publicznego"[37].

72. Natomiast „działalność na rzecz bezpieczeństwa państwa", nieobjęta zakresem stosowania dyrektywy 2002/58 rozpatrywanym w sprawie Tele2 Sverige i Watson, nie może być przypisana żadnemu innemu podmiotowi oprócz państwa jako takiego. Ponadto działalność ta nie obejmuje wykonywanych przez państwo zadań normatywnych lub regulacyjnych, lecz wyłącznie działania władz publicznych.

73. W rzeczywistości *rodzaje działalności* wymienione w art. 1 ust. 3 dyrektywy 2002/58 „stanowią w każdym wypadku działalność właściwą państwom i organom państwowym, odmienną od dziedzin działalności podmiotów indywidualnych"[38]. „Działalność" ta nie może mieć jednak charakteru normatywnego. Gdyby tak było, to wszystkie przepisy przyjęte przez państwa członkowskie w odniesieniu do przetwarzania danych osobowych pozostałyby poza zakresem stosowania dyrektywy 2002/58, nawet jeśli miałyby być uzasadnione koniecznością zapewnienia bezpieczeństwa państwa.

74. Z jednej strony oznaczałoby to znaczną utratę skuteczności wspomnianej dyrektywy, gdyż samo powołanie się na tak nieokreślone pojęcie prawne jak bezpieczeństwo narodowe wystarczyłoby do tego, by zabezpieczenia ustanowione przez prawodawcę Unii w celu ochrony danych osobowych obywateli nie miały zastosowania wobec państw członkowskich. Ochrona ta jest niewykonalna bez udziału państw członkowskich, a jej gwarancja jest zapewniona dla obywatela również w stosunku do krajowych organów publicznych.

75. Z drugiej strony wykładnia pojęcia „działalności państwa", obejmująca działalność polegającą na uchwalaniu norm i przepisów prawnych, pozbawiłaby sensu art. 15 dyrektywy 2002/58, który właśnie uprawnia państwa członkowskie – ze względów związanych z ochroną m.in. bezpieczeństwa narodowego – do przyjmowania „środków ustawodawczych" w celu ograniczenia zakresu niektórych praw i obowiązków określonych w wymienionej dyrektywie[39].

76. Jak podkreślił Trybunał w sprawie Tele2 Sverige i Watson, „zakres zastosowania dyrektywy 2002/58 należy oceniać przy uwzględnieniu, w szczególności, jej ogólnej systematyki"[40]. Z tego punktu widzenia wykładnia art. 1 ust. 3 i art. 15 ust. 1 dyrektywy 2002/58, która nadaje im sens nie powodując utraty ich skuteczności, to taka wykładnia, która w odniesieniu do pierwszego z nich ustanawia materialnoprawne wyłączenie odnoszące się do rodzajów *działalności* prowadzonych przez państwa członkowskie w dziedzinie ochrony bezpieczeństwa narodowego (i w dziedzinach równoważnych), zaś w odniesieniu do drugiego przepisu ustanawia uprawnienie do przyjmowania *środków ustawodawczych* (to znaczy przepisów prawa powszechnego), które, ze względu na ochronę bezpieczeństwa narodowego, wpływają na działalność prowadzoną przez jednostki podlegające władzy państw członkowskich poprzez ograniczenie praw zagwarantowanych w dyrektywie 2002/58.

37 Parlament/Rada i Komisja, pkt 58.

38 Wyrok Ministerio Fiscal, pkt 32. Zobacz podobnie wyrok Tele2 Sverige i Watson, pkt 72.

39 Trudno byłoby bowiem twierdzić, że art. 15 ust. 1 dyrektywy 2002/58 pozwala na ograniczenie ustanowionych praw i obowiązków w dziedzinie, która, tak jak bezpieczeństwo narodowe, byłaby co do zasady poza zakresem stosowania tej dyrektywy zgodnie z art. 1 ust. 3 tejże dyrektywy. Jak stwierdził Trybunał w wyroku Tele2 Sverige i Watson, pkt 73, przy stosowaniu art. 15 ust. 1 dyrektywy 2002/58 „należy […] założyć, że środki krajowe, 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".

40 Wyrok Tele2 Sverige i Watson, pkt 67.

4. Wyłączenie bezpieczeństwa narodowego w dyrektywie 2002/58

77. Pojęcie bezpieczeństwa narodowego (lub jego synonim „bezpieczeństwo państwa" z art. 15 ust. 1) zostało użyte w dyrektywie 2002/58 w dwojakim znaczeniu. Po pierwsze, stanowi ono podstawę *wyłączenia* (stosowania tej dyrektywy) w odniesieniu do wszystkich rodzajów działalności państw członkowskich, które go „dotyczą". Po drugie, stanowi ono podstawę *ograniczenia*, które musi nastąpić w drodze ustawy, praw i obowiązków ustanowionych w dyrektywie 2002/58, to znaczy w odniesieniu do działalności o charakterze prywatnym lub handlowym i niezwiązanej *zastrzeżonymi* tylko dla państwa dziedzinami *działalności* [41].

78. Do jakiej działalności odnosi się art. 1 ust. 3 dyrektywy 2002/58? W mojej ocenie sama Conseil d'État (rada stanu) podaje dobry przykład, gdy wymienia art. L. 851-5 i L. 851-6 kodeksu bezpieczeństwa wewnętrznego, odnosząc się do „technik gromadzenia informacji wywiadowczych, które są wdrażane bezpośrednio przez państwo bez regulowania działalności dostawców usług łączności elektronicznej poprzez nałożenie na nich szczególnych obowiązków" [42].

79. Uważam, że ten element ma kluczowe znaczenie dla określenia zakresu wyłączenia ustanowionego w art. 1 ust. 3 dyrektywy 2002/58. Ustanowiony w tej dyrektywie system nie obejmuje *działalności* mającej na celu zapewnienie bezpieczeństwa narodowego, która jest prowadzona przez władze publiczne na własny rachunek i nie wymaga współpracy ze strony jednostek, a zatem – nie wiąże się z nałożeniem na nie obowiązków w zakresie prowadzonej przez nie działalności gospodarczej.

80. Zakres działalności władz publicznych wyłączonych z ogólnego systemu regulującego przetwarzanie danych osobowych należy jednak interpretować w sposób ścisły. W szczególności nie można rozszerzyć pojęcia *bezpieczeństwa narodowego*, za które odpowiedzialność spoczywa, zgodnie z art. 4 ust. 2 TUE, wyłącznie na każdym państwie członkowskim na inne, mniej lub bardziej do niego zbliżone dziedziny życia publicznego.

81. Ze względu na to, iż niniejsze odesłania prejudycjalne dotyczą zaangażowania jednostek (to znaczy podmiotów, które świadczą użytkownikom usługi łączności elektronicznej), a nie tyko interwencji władz państwowych, nie ma konieczności szczegółowego analizowania kwestii określenia granic bezpieczeństwa narodowego *sensu stricto*.

82. Uważam jednak, że pewną wskazówką w tym względzie może być kryterium zastosowane w decyzji ramowej 2006/960/WSiSW [43], w której art. 2 lit. a) wprowadzono rozróżnienie, po pierwsze, pomiędzy organami ścigania w szerokim znaczeniu – obejmującym „krajowe służby policji, służby celne lub inny organ upoważniony na mocy prawa krajowego do wykrywania, zapobiegania i ścigania przestępstw lub działalności przestępczej oraz do wykonywania władzy publicznej i stosowania środków przymusu w kontekście takich działań" – i, po drugie „[a]gencj[e] lub jednost[ki] zajmując[e] się głównie sprawami bezpieczeństwa narodowego" [44].

41 Jak zauważył na marginesie rzecznik generalny H. Saugmandsgaard Øe w swojej opinii w sprawie Ministerio Fiscal (C-207/16, EU:C:2018:300, pkt 47), „nie należy mylić z jednej strony danych osobowych przetwarzanych *bezpośrednio* w ramach czynności – władczych – państwa w dziedzinie prawa karnego, a z drugiej strony w ramach czynności – o charakterze handlowym – dostawcy usług łączności elektronicznej, które są *następnie* wykorzystywane przez właściwe organy państwa".

42 Punkty 18 i 21 postanowienia odsyłającego w sprawie C-511/18.

43 Decyzja ramowa Rady z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej (Dz.U. 2006, L 386, s. 89).

44 Podobnie art. 1 ust. 4 decyzji ramowej Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.U. 2008, L 350, s. 60) stanowił, że decyzja ta „nie narusza podstawowych interesów bezpieczeństwa narodowego i określonych działań wywiadowczych w zakresie bezpieczeństwa narodowego".

83. W motywie jedenastym dyrektywy 2002/58 stwierdzono, że dyrektywa ta, „podobnie jak dyrektywa 95/46 […], nie odnosi się do kwestii ochrony podstawowych praw i wolności związanych z działalnością, która nie jest regulowana prawem [Unii]". Dyrektywa 2002/58 „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 państwa […]".

84. Między dyrektywą 95/46 a dyrektywą 2002/58 istnieje bowiem ciągłość, jeśli chodzi o kompetencje państw członkowskich w zakresie bezpieczeństwa narodowego. Żadna nich nie ma na celu ochrony praw podstawowych w tej szczególnej dziedzinie, w której działalność państw członkowskich nie jest „regulowana prawem [Unii]".

85. „Równowaga", o której mowa we wspomnianym motywie, wynika z konieczności poszanowania kompetencji przysługujących państwom członkowskim w dziedzinie bezpieczeństwa narodowego, gdy państwa te wykonują owe kompetencje w *sposób bezpośredni i przy użyciu własnych środków*. Natomiast w przypadku, gdy, nawet z tych samych względów związanych z bezpieczeństwem narodowym, wymagany jest udział jednostek, na które nakładane są określone obowiązki, przesądza to o objęciu uregulowaną prawem Unii dziedziną (ochrony życia prywatnego przysługującej tych podmiotom prywatnym).

86. Zarówno dyrektywa 95/46, jak i dyrektywa 2002/58 dążą do osiągnięcia wspomnianej równowagi, zezwalając na to, by prawa jednostek mogły zostać ograniczone na mocy regulacji prawnych przyjętych przez państwa odpowiednio na podstawie ich art. 13 ust. 1 i art. 15 ust. 1. W tym względzie te dwie dyrektywy nie różnią się od siebie.

87. Jeśli chodzi o rozporządzenie nr 2016/679, w którym stworzono (nowe) ogólne ramy ochrony danych osobowych, jego art. 2 ust. 2 wyklucza zastosowanie owego rozporządzenia do „przetwarzania danych osobowych" przez państwa członkowskie „w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE".

88. O ile w dyrektywie 95/46 dokoywano kwalifikacji przetwarzania danych osobowych jedynie ze względu jego cel, bez względu na to, jaki podmiot dokonywał tego przetwarzania, to w rozporządzeniu nr 2016/679 przetwarzanie wyłączone z zakresu zastosowania owego rozporządzenia jest określone zarówno na podstawie celu, w jakim jest dokonywane, jak i podmiotów go dokonujących: z tego zakresu zastosowania wyłączone zostało przetwarzanie dokonywane przez państwa członkowskie w ramach *działalności* nieobjętej zakresem prawa Unii [art. 2 ust. 2 lit. a) i b)] oraz przetwarzanie dokonywane przez organy władzy w *celu zwalczania przestępstw i ochrony* przed zagrożeniami dla bezpieczeństwa publicznego [45].

89. Te rodzaje prowadzonej przez władzę publiczną muszą być ustalane w sposób ścisły pod rygorem pozbawienia skuteczności przepisów prawa Unii w dziedzinie ochrony życia prywatnego. Rozporządzenie nr 2016/679 przewiduje w art. 23 – zgodnie z art. 15 ust. 1 dyrektywy 2002/58 – ograniczenie, w *drodze środków ustawodawczych*, ustanowionych w nim praw i obowiązków w przypadku, gdy jest to konieczne dla ochrony m.in. takich celów jak bezpieczeństwo państwa, obrona lub bezpieczeństwo publiczne. Pragnę ponownie podkreślić, że, gdyby ochrona wymienionych celów była wystarczająca do ustalenia istnienia wyłączenia z zakresu zastosowania rozporządzenia nr 2016/679, powołanie się na bezpieczeństwo państwa jako uzasadnienie ograniczenia, w drodze środków ustawodawczych, praw gwarantowanych tym rozporządzeniem, byłoby zbyteczne.

45 Rozporządzenie 2016/679 wyłącza bowiem przetwarzanie danych dokonywane przez państwa członkowskie w ramach *działalności*, która nie jest objęta zakresem stosowania prawa Unii, a także przetwarzanie danych dokonywane przez organy władzy w *celach związanych z ochroną* bezpieczeństwa publicznego.

90. Podobnie jak w przypadku dyrektywy 2002/58 niespójne byłoby, gdyby środki ustawodawcze przewidziane w art. 23 rozporządzenia nr 2016/679 (który – pragnę podkreślić – zezwala na ograniczenie przez państwo praw do poszanowania życia prywatnego obywateli ze względów związanych z bezpieczeństwem państwa) były objęte zakresem stosowania tego rozporządzenia, a jednocześnie, gdyby ochrona bezpieczeństwa państwa skutkowałaby po prostu do brakiem możliwości stosowania owego rozporządzenia, co wiązałoby się z brakiem uznania jakiegokolwiek prawa podmiotowego.

B. Potwierdzenie orzecznictwa wynikającego z wyroku Tele2 Sverige i Watson i możliwości jego rozwinięcia

91. Po przeprowadzeniu w mojej opinii w sprawie C-520/18 szczegółowej analizy[46] orzecznictwa Trybunału w tej dziedzinie opowiedziałem się za utrzymaniem owego orzecznictwa w mocy, jednocześnie proponując przyjęcie pewnej interpretacji w odniesieniu do jego treści.

92. Odnoszę się do tej analizy, chociaż uważam, że jej przytaczanie nie jest niezbędne. Przedstawione w dalszej części uwagi na temat pytań prejudycjalnych przedłożonych przez Conseil d'État (radę stanu) należy zatem odczytywać w świetle odpowiednich punktów opinii w sprawie C-520/18.

C. Odpowiedź na pytania prejudycjalne

1. W przedmiocie obowiązku zatrzymywania danych (pierwsze pytanie prejudycjalne w sprawach C-511/18 i C-512/18 oraz drugie pytanie prejudycjalne w sprawie C-512/18)

93. W odniesieniu do nałożonego na dostawców usług łączności elektronicznej obowiązku zatrzymywania danych sąd odsyłający zmierza w szczególności do ustalenia:

– czy obowiązek ten, wymagalny na podstawie art. 15 ust. 1 dyrektywy 2002/58, stanowi ingerencję uzasadnioną „prawem do bezpieczeństwa osobistego" zagwarantowanym w art. 6 karty oraz nadrzędnymi względami bezpieczeństwa narodowego (pytanie pierwsze w sprawach C-511/18 i C-512/18 oraz pytanie trzecie w sprawie C-511/18);

– czy dyrektywa 2000/31 zezwala na zatrzymywanie danych mogących umożliwić identyfikację osób, które przyczyniły się do stworzenia treści dostępnych publicznie w Internecie (pytanie drugie w sprawie C-512/18).

a) Uwagi wstępne

94. Conseil d'État (rada stanu) powołuje się na prawa podstawowe ustanowione w art. 7 (poszanowanie życia prywatnego i rodzinnego), art. 8 (ochrona danych osobowych) i art. 11 (wolność wypowiedzi i informacji) karty. Są to bowiem prawa, które zdaniem Trybunału mogą zostać naruszone przez ustanowienie obowiązku zatrzymywania danych dotyczących ruchu, który organy krajowe nakładają na dostawców usług łączności elektronicznej[47].

95. Sąd odsyłający powołuje się również na chronione na mocy art. 6 karty prawo do bezpieczeństwa osobistego. Sąd odsyłający powołuje się na nie raczej jako na czynnik mogący uzasadniać nałożenie wspomnianego obowiązku niż jako na prawo, które mogłoby zostać ewentualnie naruszone.

46 Punkty 27–68.

47 Zobacz podobnie wyrok Tele2 Sverige i Watson, pkt 92, w którym przywołano w drodze analogii wyrok Digital Rights, pkt 25, 70.

96. Zgadzam się z Komisją, że takie powołanie się na art. 6 może być niejednoznaczne. Podobnie jak Komisja uważam, że wymienionego przepisu nie należy interpretować w ten sposób, iż może on „nakładać na Unię pozytywny obowiązek przyjęcia środków mających na celu ochronę osób przed czynami zabronionymi” [48].

97. Bezpieczeństwo gwarantowane na mocy rzeczonego artykułu karty nie jest tożsame z bezpieczeństwem publicznym. Inaczej mówiąc, ma ono tyle wspólnego z bezpieczeństwem publicznym co każde inne prawo podstawowe w zakresie, w jakim bezpieczeństwo publiczne jest niezbędnym warunkiem korzystania z praw i wolności podstawowych.

98. Jak przypomina Komisja, odpowiednikiem art. 6 karty jest, jak stwierdzono w dołączonych do karty wyjaśnieniach, art. 5 europejskiej Konwencji praw człowieka (zwanej dalej „EKPC”). Z brzmienia art. 5 EKPC wynika, że „bezpieczeństwo”, które przepis ten chroni, jest ściśle osobiste, rozumiane jako gwarancja prawa do wolności fizycznej przed arbitralnym zatrzymaniem lub aresztowaniem. Jest to zatem bezpieczeństwo polegające na tym, że nikt nie może zostać pozbawiony wolności z wyjątkiem przypadków przewidzianych w ustawie oraz zgodnie z przesłankami i procedurami określonymi w ustawie.

99. Chodzi zatem o *bezpieczeństwo osobiste* odnoszące się do warunków, po spełnieniu których fizyczna wolność osób może zostać ograniczona [49], nie zaś o *bezpieczeństwo publiczne*, nieodłącznie związane z istnieniem państwa, które jest w rozwiniętym społeczeństwie niezbędną przesłanką pogodzenia wykonywania uprawnień publicznych z korzystaniem z praw indywidualnych.

100. Jednakże niektóre z rządów wnoszą raczej o uwzględnienie prawa do bezpieczeństwa w drugim z wymienionych znaczeń. W rzeczywistości Trybunał nie pominął tego znaczenia, lecz, co więcej, wyraźnie o nim wspominał w swoich wyrokach [50] i opiniach [51]. Trybunał nigdy nie negował znaczenia leżących w interesie ogólnym celów w zakresie ochrony bezpieczeństwa narodowego i porządku publicznego [52], walki z terroryzmem, prowadzonej w celu utrzymania międzynarodowego pokoju i bezpieczeństwa oraz walki z poważną przestępczością, prowadzonej w celu zapewnienia bezpieczeństwa publicznego [53], którą słusznie określił jako mającą „pierwszorzędne” znaczenie [54]. Jak Trybunał wskazał wcześniej, „ochrona bezpieczeństwa publicznego przyczynia się również do ochrony praw i wolności innych osób” [55].

101. Możliwość, jaką dają niniejsze odesłania prejudycjalne, mogłaby zostać wykorzystana do wyraźniejszego zaproponowania poszukiwania równowagi między prawem do bezpieczeństwa osobistego, z jednej strony, a prawem do poszanowania życia prywatnego i prawem do ochrony danych osobowych, z drugiej strony. Pozwoliłoby to uniknąć zarzutu faworyzowania tych drugich kosztem pierwszego z wymienionych praw.

102. Moim zdaniem motyw jedenasty i art. 15 ust. 1 dyrektywy 2002/58, w których jest mowa o wymogach dotyczących konieczności przyjmowania danych środków w *społeczeństwie demokratycznym* i ich proporcjonalności, odnoszą się do tej właśnie równowagi. Pragnę podkreślić, że prawo do bezpieczeństwa jest nierozerwalnie związane z samym istnieniem i przetrwaniem

48 Punkt 37 uwag Komisji.

49 W przyjętej przez ETPC wykładni. Zobacz w szczególności wyrok z dnia 5 lipca 2016 r. w sprawie Buzadji przeciwko Republice Mołdawii, ECHR:2016:0705JUD002375507, § 84, w którym stwierdzono, że podstawowym celem ustanowionego w art. 5 EKPC prawa jest zapobieganie arbitralnemu lub nieuzasadnionemu pozbawieniu wolności osobistej.

50 Wyrok Digital Rights, pkt 42.

51 Opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r. (zwana dalej „opinią 1/15”, EU:C:2017:592, pkt 149 i przytoczone tam orzecznictwo).

52 Wyrok z dnia 15 lutego 2016 r., N. (C-601/15 PPU, EU:C:2016:84, pkt 53).

53 Wyrok Digital Rights, pkt 42 i przytoczone tam orzecznictwo.

54 Ibidem, pkt 51.

55 Opinia 1/15, pkt 149.

demokracji, co uzasadnia konieczność pełnego jego uwzględnienia w ramach oceny rzeczonej proporcjonalności. Innymi słowy, choć przestrzeganie zasady poufności danych ma pierwszorzędne znaczenie w społeczeństwie demokratycznym, to nie można również lekceważyć znaczenia kwestii związanych z bezpieczeństwem.

103. Należy zatem wziąć pod uwagę kontekst poważnego i trwałego zagrożenia dla bezpieczeństwa narodowego, w szczególności tego związanego z terroryzmem, jak stwierdzono w pkt 119 in fine wyroku Tele2 Sverige i Watson. W ramach systemu krajowego reakcja na napotkane zagrożenia może być proporcjonalna do ich charakteru i poziomu, przy czym reakcja ta niekoniecznie musi być identyczna z reakcją innych państw członkowskich.

104. Należy wreszcie dodać, że powyższe uwagi nie stoją na przeszkodzie temu, by w rzeczywiście *wyjątkowych* sytuacjach, charakteryzujących się bezpośrednim zagrożeniem lub nadzwyczajnym ryzykiem, które uzasadniają oficjalne ogłoszenie stanu wyjątkowego w państwie członkowskim, ustawodawstwo krajowe przewidywało, przez ograniczony czas, możliwość nałożenia tak szerokiego i ogólnego obowiązku zatrzymywania danych, jaki zostanie uznany za konieczny [56].

105. W konsekwencji należałoby przeformułować pierwsze pytanie obu odesłań prejudycjalnych, zadając je raczej w kontekście możliwości uzasadnienia ingerencji we względy bezpieczeństwa narodowego. Wątpliwość dotyczyłaby zatem kwestii, czy nałożony na dostawców usług łączności elektronicznej obowiązek jest zgodny z art. 15 ust. 1 dyrektywy 2002/58.

b) Ocena

1) Charakterystyka, w świetle orzecznictwa Trybunału, przepisów krajowych w postaci przedstawionej w obu odesłaniach prejudycjalnych

106. Jak wynika z postanowień odsyłających, w przepisach rozpatrywanych w obu postępowaniach, po przeprowadzeniu których wydano te postanowienia, ustanowiony został obowiązek zatrzymywania danych:

– przez operatorów łączności elektronicznej, a zwłaszcza podmioty, które oferują dostęp do usług internetowej komunikacji publicznej; oraz

– przez osoby fizyczne lub prawne, które oferują, również nieodpłatnie, do publicznego udostępniania w Internecie, przechowywanie sygnałów, tekstów, obrazów, dźwięków lub wszelkiego rodzaju wiadomości dostarczanych przez odbiorców tych usług [57].

107. Operatorzy muszą zatrzymywać przez okres jednego roku, licząc od chwili zarejestrowania, informacje umożliwiające identyfikację użytkownika, dane dotyczące używanych końcowych urządzeń komunikacyjnych, cechy techniczne, datę, godzinę i czas trwania każdego połączenia, dane dotyczące żądanych lub używanych usług dodatkowych i ich dostawców, a także dane umożliwiające identyfikację odbiorcy połączenia, a w przypadku działalności w zakresie telefonii, dane, które pozwalają na identyfikację pochodzenia i lokalizacji połączenia [58].

56 Zobacz moją opinię w sprawie C-520/18, pkt 105–107.

57 Wynika to z art. L. 851-1 kodeksu bezpieczeństwa wewnętrznego, który odsyła do art. L. 34-1 kodeksu poczty i łączności elektronicznej oraz do art. 6 ustawy nr 2004-575 o zaufaniu w gospodarce cyfrowej.

58 Wynika to z brzmienia art. R. 10-13 kodeksu poczty i łączności elektronicznej.

108. Jeśli chodzi w szczególności o usługi dostępu do Internetu i usługi przechowywania danych, wydaje się, że przepisy krajowe ustanawiają wymóg przechowywania adresów IP [59], haseł dostępu oraz, w przypadku zawarcia umowy lub otwarcia rachunku płatniczego, rodzaju dokonanej płatności, a także jej numeru referencyjnego, kwoty, daty i godziny transakcji [60].

109. Wspomniany obowiązek zatrzymywania został ustanowiony w celu wykrywania, stwierdzania i ścigania przestępstw [61]. Oznacza to, że – jak zostanie wykazane – w przeciwieństwie do obowiązku *zbierania* danych dotyczących ruchu i lokalizacji, obowiązek *ich zatrzymywania* nie został ustanowiony wyłącznie w celu zapobiegania terroryzmowi [62].

110. Jeśli chodzi o warunki *dostępu* do zatrzymanych danych, z informacji przekazanych w aktach sprawy wynika, że albo są to warunki przewidziane dla powszechnie obowiązującego systemu (interwencja organu sądowego), albo taki dostęp jest ograniczony do indywidualnie wyznaczonych i upoważnionych funkcjonariuszy, po uzyskaniu uprzedniego zezwolenia premiera, wydanego na podstawie niewiążącej opinii niezależnego organu administracyjnego [63].

111. Łatwo zauważyć, że, jak wskazała Komisja [64], dane, których wymóg zatrzymywania został ustanowiony w przepisach krajowych, odpowiadają zasadniczo danym zbadanym przez Trybunał w wyrokach Digital Rights oraz Tele2 Sverige i Watson [65]. Podobnie jak w owych wyrokach, dane te podlegają „obowiązkowi uogólnionego i niezróżnicowanego zatrzymywania", jak zupełnie szczerze stwierdza Conseil d'État (rada stanu) na początku jej pytań prejudycjalnych.

112. Jeśli tak jest – czego ocena ostatecznie należy do sądu odsyłającego – można jedynie stwierdzić, że rozpatrywane uregulowanie stanowi „szczególnie daleko posuniętą ingerencję w prawa podstawowe, o których mowa w art. 7 i 8 karty" [66].

113. Żadna ze stron postępowania nie zakwestionowała tego, że takie uregulowanie stanowi ingerencję we wspomniane prawa. Nie ma potrzeby dalszego analizowania powyższej okoliczności, nawet jeśli miałoby to mieć na celu przypomnienie, że naruszenie tych praw prowadzi nieuchronnie do naruszenia podstaw społeczeństwa, którego celem jest poszanowanie m.in. zagwarantowanego w karcie prawa do życia prywatnego.

114. Zastosowanie orzecznictwa ustanowionego w wyroku Tele2 Sverige i Watson oraz potwierdzonego wyrokiem Ministerio Fiscal prowadziłoby oczywiście do stwierdzenia, że uregulowanie takie jak będące przedmiotem sporu w niniejszej sprawie „wykracza […] poza granice tego, co jest absolutnie konieczne, i nie można go uznać za uzasadnione w demokratycznym społeczeństwie, jak tego wymaga art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty" [67].

59 Do sądu odsyłającego należy zweryfikowanie tej okoliczności, co do której zostały wyrażone rozbieżności na rozprawie.

60 Artykuł 1 dekretu nr 2011-219.

61 Artykuł R. 10-13 kodeksu poczty i łączności elektronicznej.

62 Zarówno La Quadrature du Net, jak i Fédération des fournisseurs d'accès á Internet associatifs podkreślają szeroki zakres celów, jakim służy zatrzymywanie, przyznane władzom uprawnienia dyskrecjonalne, brak obiektywnych kryteriów służących jego określeniu i znaczenie przypisywane tym postaciom przestępstw, których nie można określić jako poważne.

63 Commission nationale de contrôle des techniques de renseignement (krajowa komisja ds. kontroli technik wywiadowczych). Zobacz w tym względzie uwagi rządu francuskiego, pkt 145–148.

64 Punkt 60 uwag Komisji.

65 W rzeczywistości zakres tych danych jest nieco szerszy, ponieważ w przypadku usług dostępu do Internetu wydaje się, iż obejmują one przechowywanie adresu IP lub haseł dostępu.

66 Wyrok Tele2 Sverige i Watson, pkt 100.

67 Ibidem, pkt 107.

115. Podobnie bowiem jak uregulowanie analizowane w wyroku Tele2 Sverige i Watson, również uregulowanie rozpatrywane w niniejszej sprawie „obejmuje w sposób uogólniony wszystkich abonentów i zarejestrowanych użytkowników i dotyczy wszystkich środków łączności elektronicznej i wszystkich danych o ruchu [oraz] nie przewiduje jakiegokolwiek zróżnicowania, ograniczenia ani wyjątku zależnego od zamierzonego celu”[68]. W konsekwencji, „ma ono zastosowanie nawet wobec tych osób, co do których brak jest dowodów mogących sugerować, że ich zachowanie może mieć związek, chociażby pośredni i daleki, z poważnymi przestępstwami”, i to nie przewidując żadnych wyjątków, „więc w rezultacie ma zastosowanie nawet wobec tych osób, których łączność na gruncie przepisów prawa krajowego objęta jest tajemnicą zawodową”[69].

116. Podobnie, sporne uregulowanie „nie wymaga istnienia żadnego związku między danymi, których zatrzymywanie nakazuje, a zagrożeniem dla bezpieczeństwa publicznego. Nie zawiera ono zwłaszcza żadnych ograniczeń czasowych czy geograficznych ani ograniczeń do grupy osób, które można podejrzewać o taki czy inny rodzaj uczestnictwa w poważnym przestępstwie, tak by obowiązek zatrzymywania danych obejmował tylko te dane, co do których z jakiegoś powodu można zakładać, że mają znaczenie dla walki z przestępczością”[70].

117. Z powyższego wynika, że rzeczone uregulowanie „wykracza […] poza granice tego, co jest absolutnie konieczne, i nie można go uznać za uzasadnione w demokratycznym społeczeństwie, jak tego wymaga art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty”[71].

118. W związku z powyższym Trybunał stwierdził, że odpowiednie przepisy krajowe są niezgodne z art. 15 ust. 1 dyrektywy 2002/58 w zakresie, w jakim przewidują one „do celów zwalczania przestępczości uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej”[72].

119. Powstaje zatem pytanie, czy orzecznictwo Trybunału dotyczące zatrzymywania danych osobowych może zostać nie tyle podważone, co przynajmniej uzupełnione w przypadku, gdy celem owego „uogólnionego i niezróżnicowanego” zatrzymywania danych jest walka z terroryzmem. Pytanie pierwsze w sprawie C-511/18 zostało podniesione właśnie „w kontekście poważnych i trwałych zagrożeń dla bezpieczeństwa narodowego, a zwłaszcza zagrożenia terrorystycznego”.

120. Ponieważ jednak jest to *kontekst faktyczny*, w którym ustanowiony został obowiązek zatrzymywania danych, niewątpliwie jego *kontekst normatywny* nie dotyczy jedynie terroryzmu. W ramach systemu zatrzymywania i dostępu do danych, który jest przedmiotem zawisłego przed Conseil d’État (radą stanu) sporu, wspomniany obowiązek jest uzależniony od celów, dla których prowadzone jest uogólnione wykrywanie, stwierdzanie i ściganie przestępstw.

121. W każdym razie pragnę przypomnieć, że walka z terroryzmem nie została pominięta w uzasadnieniu wyroku Tele2 Sverige i Watson, a Trybunał nie uznał, że ta forma przestępczości wymaga wprowadzenia jakichś zmian w jego orzecznictwie[73].

122. W związku z powyższym, co do zasady uważam, że na zadane przez sąd odsyłający pytanie oparte na szczególnym charakterze zagrożenia terrorystycznego należałoby odpowiedzieć w taki sam sposób, w jaki Trybunał wypowiedział się w wyroku Tele2 Sverige i Watson.

68 Ibidem, pkt 105.

69 Ibidem.

70 Wyrok Tele2 Sverige i Watson, pkt 106.

71 Ibidem, pkt 107.

72 Ibidem, pkt 112.

73 Ibidem, pkt 103.

123. Jak wskazałem w opinii w sprawie Stichting Brein, „pewność stosowania prawa nakłada na organy sądowe obowiązek jeżeli nie bezwzględnego stosowania *stare decisis*, to przynajmniej rozważnego stosowania się do tego, co same wcześniej postanowiły one po dojrzałej refleksji nad określonym zagadnieniem prawnym”[74].

2) Ograniczone zatrzymywanie danych w kontekście istniejących zagrożeń dla bezpieczeństwu państwa, włącznie z zagrożeniem terrorystycznym

124. Czy możliwe byłoby jednak wyjaśnienie lub uzupełnienie tego orzecznictwa z uwagi na jego konsekwencje dla walki z terroryzmem lub ochrony państwa przed innymi podobnymi zagrożeniami dla bezpieczeństwa narodowego?

125. Podkreśliłem już, że samo zatrzymywanie danych osobowych stanowi ingerencję w prawa zagwarantowane w art. 7, 8 i 11 karty[75]. Niezależnie od tego, że ostatecznie celem zatrzymywania danych jest umożliwienie retrospektywnego lub jednoczesnego *dostępu* do tych danych w określonej chwili[76], samo zatrzymywanie danych innych niż te, które są ściśle niezbędne do przekazania komunikatu lub do fakturowania usług świadczonych przez dostawcę, stanowi przekroczenie granic ustanowionych w art. 5 i 6 dyrektywy 2002/58.

126. Użytkownicy tych usług (w rzeczywistości niemalże wszyscy obywatele w najbardziej rozwiniętych społeczeństwach) mają lub powinni mieć uzasadnione oczekiwania w tym sensie, że jedynymi danymi, które mogą być zatrzymywane bez ich zgody, są te dane, które mogą być przechowywane zgodnie ze wspomnianymi przepisami. Przewidziane w art. 15 ust. 1 dyrektywy 2002/58 wyjątki należy interpretować w oparciu o powyższą przesłankę.

127. Jak już wyjaśniłem, Trybunał w wyroku Tele2 Sverige i Watson odrzucił koncepcję uogólnionego i niezróżnicowanego zatrzymywania danych osobowych, również w odniesieniu do walki z terroryzmem[77].

128. Wobec podniesionych zarzutów nie uważam, by orzecznictwo oparte na tym wyroku nie doceniało zagrożenia terrorystycznego jako szczególnie poważnej formy przestępczości, dążącej do wyraźnego celu polegającego na podważenia władzy państwowej i destabilizacji lub zniszczenia jej instytucji. Walka z terroryzmem ma dosłownie kluczowe znaczenie dla państwa i jego sukcesu, który jest celem leżącym w interesie publicznym, niezbędnym dla funkcjonowania państwa prawa.

74 Sprawa C-527/15, EU:C:2016:938, pkt 41.

75 Jak Trybunał zauważył w opinii 1/15, pkt 124, „udostępnianie danych osobowych podmiotowi trzeciemu, takiemu jak organ rządowy, stanowi ingerencję w prawo podstawowe gwarantowane w art. 7 karty, niezależnie od tego, w jaki sposób te dane zostaną później wykorzystane. To samo dotyczy zatrzymania danych osobowych, jak również dostępu do tych danych w celu ich wykorzystania przez organy rządowe. W tym względzie nie ma znaczenia okoliczność, czy informacje związane z życiem prywatnym mają charakter szczególnie chroniony, ani też to, czy też ze względu na tę ingerencję zainteresowane osoby doświadczyły ewentualnych niedogodności”.

76 Jak wskazał rzecznik generalny P. Cruz Villalón w opinii w sprawie Digital Rights, C-293/12 i C-594/12 (EU:C:2013:845, pkt 72), „zbieranie i przede wszystkim przechowywanie w gigantycznych bazach danych wielu różnych danych generowanych lub przetwarzanych w ramach większości zwykłych połączeń elektronicznych obywateli Unii stanowi daleko posuniętą ingerencję w ich życie prywatne, nawet jeśli jest to tylko stworzenie warunków do zapewnienia możliwości wstecznej kontroli ich aktywności zarówno osobistej, jak i zawodowej. Gromadzenie tych danych tworzy warunki dla monitorowania, które chociaż odbywa się jedynie wstecznie przy okazji wykorzystywania danych, zagraża jednak w sposób ciągły przez cały okres ich przechowywania prawu obywateli Unii do tajemnicy życia prywatnego. Wywołane tym niejasne poczucie inwigilacji stawia w wyjątkowo ostrym świetle kwestię długości okresu przechowywania danych”.

77 Wyrok Tele2 Sverige i Watson, pkt 103: „nie może […] uzasadniać stwierdzenia, że przepisy krajowe przewidujące uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji należy uznać za konieczne do celów prowadzenia tej walki”.

129. Praktycznie wszystkie rządy, które wzięły udział w postępowaniu, a także Komisja, zgodziły się, że, pomijając trudności techniczne, częściowe tylko i zróżnicowane zatrzymywanie danych osobowych pozbawiłoby krajowe służby wywiadowcze możliwości dostępu do informacji niezbędnych do identyfikacji zagrożeń dla bezpieczeństwa publicznego i obronności państwa, a także do ścigania sprawców zamachów terrorystycznych [78].

130. W odniesieniu do powyższej oceny wydaje mi się istotne, aby podkreślić, że walki z terroryzmem nie można rozważać wyłącznie w kategoriach jej skuteczności. Stanowi to utrudnienie, lecz także przesądza o jej niezwykłości, jeśli środki i metody walki z terroryzmem są zgodne z wymogami państwa prawa, które polega przede wszystkim na utrzymaniu władzy i siły w granicach prawa, w szczególności zgodnie z porządkiem prawnym, którego powodem i celem istnienia jest obrona praw podstawowych.

131. O ile w przypadku terroryzmu wystarczy, że podejmowane w jego ramach działania spełniają wyłącznie kryterium czystej (i maksymalnej) skuteczności zamachów na ustanowiony porządek, o tyle w przypadku państwa prawa jego skuteczność jest definiowana w kategoriach, które nie pozwalają na pominięcie, w ramach jego obrony, procedur i gwarancji nadających mu charakter zgodnego z prawem porządku. Koncentrując się jedynie wokół samej skuteczności, państwo prawa utraciłoby swą odróżniającą cechę, a w skrajnych przypadkach mogłoby samo stać się zagrożeniem dla obywatela. W sytuacji, w której władza publiczna uzyskałaby zbyt daleko sięgające instrumenty służące ściganiu przestępstw, wykorzystując które mogłaby ona ignorować lub podważać prawa podstawowe, nic nie byłoby w stanie stanąć na przeszkodzie temu, aby jej niekontrolowane i całkowicie swobodne działanie ostatecznie stałoby się szkodliwe dla wolności wszystkich.

132. Pragnę podkreślić, że skuteczność władzy publicznej napotyka na barierę nie do przebycia, jaką są prawa podstawowe obywateli, których ograniczenia, w myśl art. 52 ust. 1 karty, mogą być wprowadzone jedynie w drodze ustawy i z poszanowaniem ich istoty, „gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób” [79].

133. W odniesieniu do warunków, po spełnieniu których, zgodnie z wyrokiem Tele2 Sverige i Watson, dopuszczalne byłoby *indywidualne* zachowywanie danych, odsyłam do mojej opinii w sprawie C-520/18 [80].

134. Okoliczności, w których informacje, jakimi dysponują organy ścigania, pozwalają na uzasadnione podejrzenie przygotowania zamachu terrorystycznego, mogą stanowić uzasadnioną przesłankę ustanowienia obowiązku zatrzymywania niektórych danych. Tym bardziej przesłankę tę może stanowić rzeczywiste popełnienie zamachu. O ile w tym ostatnim przypadku samo popełnienie przestępstwa może stanowić czynnik uzasadniający przyjęcie wspomnianego środka, o tyle w przypadku wystąpienia jedynie podejrzenia co do ewentualnego zamachu konieczne byłoby, aby okoliczności stanowiące podstawę przyjęcia owego środka zapewniały minimalny stopień wiarygodności, niezbędny do obiektywnego wyważenia znaczenia przesłanek mogących uzasadniać jego przyjęcie.

78 Taka jest na przykład interpretacja proponowana przez rząd francuski, który ilustruje to stwierdzenie konkretnymi przykładami dotyczącymi użyteczności uogólnionego zatrzymywania danych, które umożliwiło reakcję państwa na poważne zamachy terrorystyczne, jakie miały miejsce w jego kraju w ostatnich latach (uwagi rządu francuskiego, pkt 107, 122–126).

79 Wyrok z dnia 15 lutego 2016 r., N. (C-601/15 PPU, EU:C:2016:84, pkt 50). Jest to zatem kwestia trudnej równowagi między porządkiem publicznym a wolnością, o której już wspomniałem i do której zasadniczo dążą wszystkie uregulowania Unii. Jako przykład może służyć dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.U. 2017, L 88, s. 6). Dyrektywa ta stanowi w art. 20 ust. 1, że państwa członkowskie powinny zapewnić, by podmioty odpowiedzialne za prowadzenie postępowań przygotowawczych w sprawie przestępstw terrorystycznych lub za oskarżanie w sprawie takich przestępstw „miały dostęp do skutecznych narzędzi stosowanych w postępowaniu przygotowawczym”, a jednocześnie w motywie 21 stwierdza, że takie skuteczne narzędzia należy wykorzystywać „w sposób ukierunkowany, uwzględniając zasadę proporcjonalności oraz rodzaj i wagę przestępstw objętych postępowaniem przygotowawczym, a także należy przestrzegać prawa do ochrony danych osobowych”.

80 Punkty 87–95.

135. Chociaż jest to trudne, to jednak możliwe jest dokładne określenie zgodnie z obiektywnymi kryteriami, zarówno kategorii danych, których przechowywanie uważa się za niezbędne, jak i kręgu osób, których dane te dotyczą. Z pewnością najbardziej *praktyczne i skuteczne* byłoby uogólnione i niezróżnicowane przechowywanie wszelkich danych, które mogą być gromadzone przez dostawców usług łączności elektronicznej, jednak wskazałem już, że tej kwestii nie można rozstrzygać w kategoriach *skuteczności praktycznej*, lecz *skuteczności prawnej* oraz w kontekście państwa prawa.

136. Zadanie to ma typowo ustawodawczy charakter w wyznaczonych w orzecznictwie Trybunału granicach. Ponownie odsyłam do uwag przedstawionych w tej kwestii w mojej opinii w sprawie C-520/18 [81].

3) Dostęp do przechowywanych danych

137. Wychodząc z założenia, że operatorzy gromadzili dane zgodnie z przepisami dyrektywy 2002/58 oraz że dane te były przechowywane na podstawie art. 15 ust. 1 [82], dostęp właściwych organów władzy do tych informacji powinien się odbywać zgodnie z warunkami ustanowionymi przez Trybunał i analizowanymi przeze mnie w opinii w sprawie C-520/18, do której odsyłam [83].

138. W związku z powyższym, również w niniejszym przypadku uregulowanie krajowe powinno ustanawiać materialne i proceduralne warunki regulujące dostęp właściwych organów władz krajowych do przechowywanych danych [84]. W kontekście niniejszych odesłań prejudycjalnych warunki te umożliwiłyby uzyskanie dostępu do danych dotyczących osób podejrzewanych o planowanie, popełnianie czy też popełnienie już aktu terrorystycznego, bądź też zaangażowanych w taki akt [85].

139. Ważne jest jednak, aby dostęp do rozpatrywanych danych był, z wyjątkiem należycie uzasadnionych pilnych przypadków, poddany uprzedniej kontroli sądu lub niezależnego organu administracyjnego, a rozstrzygnięcie tego sądu lub organu następowało na uzasadniony wniosek owych organów [86]. W związku z tym tam, gdzie nie jest możliwe dokonanie abstrakcyjnej oceny ustawy, gwarantowana jest ocena dokonywana *in concreto* przez wspomniany niezależny organ, zobowiązany w równym stopniu do zapewnienia bezpieczeństwa państwa i obrony praw podstawowych obywateli.

4) Obowiązek zatrzymywania danych umożliwiających identyfikację twórców treści w świetle dyrektywy 2000/31 (drugie pytanie prejudycjalne w sprawie C-512/18)

140. Sąd odsyłający powołuje się na dyrektywę 2000/31 jako na punkt odniesienia służący ustaleniu tego, czy możliwe jest nałożenie na niektóre podmioty [87] i na operatorów oferujących usługi komunikacji publicznej obowiązku 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".

81 Punkty 100–107.

82 Przy założeniu, że spełnione są warunki określone w pkt 122 wyroku Tele2 Sverige i Watson, Trybunał przypomniał, iż art. 15 ust. 1 dyrektywy 2002/58 nie dopuszcza odstępstw od art. 4 ust. 1 i 1a, który wymaga od dostawców przyjęcia środków pozwalających zapewnić ochronę przechowywanych danych przed ryzykiem nadużycia lub bezprawnego dostępu. W tym względzie Trybunał orzekł, że „uwzględniając ilość zatrzymywanych danych, ich newralgiczny charakter oraz prawdopodobieństwo bezprawnego uzyskania dostępu do nich, dostawcy usług łączności elektronicznej, aby zapewnić integralność i poufność tych danych, muszą zapewnić za pomocą środków technicznych i organizacyjnych szczególnie wysoki poziom ochrony i bezpieczeństwa. W szczególności uregulowanie krajowe powinno ustanawiać zarówno wymóg przechowywania danych na terytorium Unii, jak też nieodwracalnego ich niszczenia po upływie okresu ich przechowywania".

83 Punkty 52–60.

84 Wyrok Tele2 Sverige i Watson, pkt 118.

85 Ibidem, pkt 119.

86 Ibidem, pkt 120.

87 Te, które „oferują […] do publicznego udostępniania za pomocą usług publicznej komunikacji internetowej, przechowywanie sygnałów, tekstów, obrazów, dźwięków lub wszelkiego rodzaju wiadomości dostarczonych przez odbiorców tych usług […]".

141. Zgadzam się z Komisją co do braku znaczenia oceny zgodności rzeczonego obowiązku z dyrektywą 2000/31 [88] byłaby pozbawiona znaczenia, skoro art. 1 ust. 5 lit. b) tej dyrektywy wyłącza ze swego zakresu stosowania „zagadnie[nia] odnosząc[e] się do usług społeczeństwa informacyjnego objętych dyrektywami 95/46/WE oraz 97/66/WE", które to przepisy odpowiadają obecnie rozporządzeniu nr 2006/679 i dyrektywie 2002/58 [89], których art. 23 ust. 1 oraz art. 15 ust. 1 moim zdaniem należy interpretować w określony wyżej sposób.

2. W przedmiocie obowiązku zbierania w czasie rzeczywistym danych dotyczących ruchu i lokalizacji (drugie pytanie prejudycjalne w sprawie C-511/18)

142. W ocenie sądu odsyłającego art. L. 851-2 kodeksu bezpieczeństwa wewnętrznego zezwala, wyłącznie w celu zapobiegania terroryzmowi, na zbieranie w czasie rzeczywistym informacji o osobach wcześniej zidentyfikowanych jako mogące mieć związek z zagrożeniem terroryzmem. Podobnie art. L. 851-4 tego kodeksu zezwala na przekazywanie w czasie rzeczywistym przez operatorów danych technicznych dotyczących lokalizacji urządzeń końcowych.

143. Zdaniem sądu odsyłającego techniki te nie nakładają na dostawców obowiązku zatrzymywania danych, który wykraczałby poza to, co jest konieczne do fakturowania i sprzedaży ich usług.

144. Ponadto zgodnie z art. L. 851-3 kodeksu bezpieczeństwa wewnętrznego operatorzy łączności elektronicznej i dostawcy technologii mogą zostać zobowiązani 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 nie obejmuje uogólnionego i niezróżnicowanego zatrzymywania danych polega na zbieraniu, przez ograniczony czas, danych dotyczących połączeń, które mogą być związane z przestępstwem o charakterze terrorystycznym.

145. Moim zdaniem warunki, których spełnienie jest wymagane do uzyskania dostępu do zatrzymywanych danych osobowych powinny mieć również zastosowanie w przypadku uzyskiwania w czasie rzeczywistym dostępu do danych generowanych w trakcie połączeń elektronicznych. Odsyłam zatem do uwag poczynionych w odniesieniu do tej kwestii. Nie ma znaczenia, czy chodzi o dane, które zostały zatrzymane, czy też te uzyskiwane w czasie rzeczywistym, ponieważ w obu przypadkach uzyskuje się wiedzę o danych osobowych bez względu na to, czy są to dane przeszłe, czy obecne.

146. Konkretnie, jeżeli dostęp uzyskiwany w czasie rzeczywistym jest konsekwencją połączeń wykrytych w wyniku zautomatyzowanego przetwarzania, takiego jak to określone w art. L. 851-3 kodeksu bezpieczeństwa wewnętrznego, wymagane jest, aby wcześniej ustalone modele i kryteria tego przetwarzania były konkretne, wiarygodne i niedyskryminacyjne, ułatwiając identyfikację osób, wobec których można mieć uzasadnione podejrzenia co do ich udziału w działalności terrorystycznej [90].

88 Sąd odsyłający powołuje się na tę dyrektywę w sposób ogólny, bez wskazania żadnego konkretnego przepisu, w drugim pytaniu w sprawie C-512/18.

89 Punkty 112 i 113 pisemnych uwag Komisji.

90 Wyrok Digital Rights, pkt 59.

3. W przedmiocie obowiązku informowania osób, których dane dotyczą (trzecie pytanie prejudycjalne w sprawie C-511/18)

147. Trybunał orzekł, że organy, którym przyznano dostęp do danych, powinny poinformować o tej okoliczności osoby, których dane dotyczą, pod warunkiem nienarażenia na szwank prowadzonych postępowań dochodzeniowo-śledczych. Obowiązek ten został ustanowiony ze względu na to, że wspomniana informacja jest niezbędna do tego, aby umożliwić rzeczonym osobom wykonanie prawa do skutecznej ochrony sądowej, wyraźnie przewidzianego w art. 15 ust. 2 dyrektywy 2002/58, w przypadku naruszenia ich praw [91].

148. W ramach trzeciego pytania w sprawie C-511/18 Conseil d'État (rada stanu) zmierza do ustalenia, czy taki wymóg informowania jest bezwarunkowy, czy też możliwe jest zwolnienie z niego w przypadku ustanowienia innych gwarancji, takich jak te opisane w postanowieniu odsyłającym.

149. Jak wskazał sąd odsyłający [92], wspomniane gwarancje polegają na możliwości zwrócenia się do samej Conseil d'État (rady stanu) osób, które zamierzają sprawdzić, czy dana technika wywiadowcza została zastosowana niezgodnie z prawem. Organ ten mógłby w stosownych przypadkach unieważnić zezwolenie na zastosowanie środka i nakazać zniszczenie zgromadzonych danych w ramach procedury, która nie przewiduje zwykłej zasady kontradyktoryjności postępowań sądowych.

150. Sąd odsyłający jest zdania, że uregulowanie to nie narusza prawa do skutecznej ochrony sądowej. Uważam jednak, że teoretycznie można by przyjąć taką możliwość w odniesieniu do osób, które decydują się na sprawdzenie tego, czy są przedmiotem operacji wywiadowczej. Natomiast wspomniane prawo nie jest przestrzegane, jeżeli osoby, które są lub były przedmiotem takiej operacji, nie są informowane o tej okoliczności i w związku z tym nie mogą nawet rozważać tego, czy ich prawa zostały, czy też nie zostały naruszone.

151. Gwarancje sądowe, do których odnosi się sąd odsyłający, wydają się być uzależnione od inicjatywy osoby, która podejrzewa, że jest przedmiotem gromadzenia danych dotyczących jej samej. Jednakże dostęp do sądu w celu obrony praw musi być skuteczny w odniesieniu do wszystkich, co oznacza, że osoba, która była przedmiotem przetwarzania dotyczących jej danych osobowych, musi mieć możliwość zakwestionowania na drodze sądowej zgodności z prawem rzeczonego przetwarzania i w związku z tym musi być poinformowana o istnieniu owego przetwarzania.

152. Jak niewątpliwie wynika z przekazanych informacji, postępowanie sądowe może zostać wszczęte z urzędu lub na podstawie skargi administracyjnej, lecz w każdym razie osoba, której dane dotyczą, musi mieć zapewnioną możliwość wszczęcia owego postępowania, w związku z czym konieczne jest powiadomienie jej, że jej dane osobowe były przedmiotem określonego przetwarzania. Obrona praw tej osoby nie może się opierać na okolicznościach, że dowiedziała się ona o wspomnianym przetwarzaniu od osób trzecich lub za pomocą własnych środków.

153. W związku z powyższym, w zakresie, w jakim nie zagraża to tokowi postępowań dochodzeniowych, w odniesieniu do których udzielono dostępu do zatrzymywanych danych, należy poinformować o tym dostępie osobę, której dane dotyczą.

91 Wyrok Tele2 Sverige i Watson, pkt 121.

92 Punkty 8–11 postanowienia odsyłającego.

154. Inną sprawą jest okoliczność polegająca na tym, że, w sytuacji, gdy osoba, której dane dotyczą, postanowi wziąć udział w postępowaniu sądowym już po tym, gdy poinformowano ją o udzieleniu dostępu do jej danych, prowadzone już po tym fakcie postępowanie sądowe musi spełniać wymogi dotyczące poufności i zastrzegania danych, które są nieodłącznie związane z kontrolą działania władz publicznych w obszarach wrażliwych, takich jak bezpieczeństwo i obrona państwa. Powyższa kwestia nie ma jednak żadnego związku z niniejszymi odesłaniami, w związku z czym moim zdaniem nie ma potrzeby, aby Trybunał wypowiadał się w tym względzie.

V. Wnioski

155. W świetle powyższych uwag proponuję, aby Trybunał odpowiedział na pytania zadane przez Conseil d'État (radę stanu, Francja) w następujący sposób:

Artykuł 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), w związku z art. 7, 8, 11 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej, należy interpretować w ten sposób, że:

1) stoi on na przeszkodzie uregulowaniu krajowemu, które w kontekście poważnych i trwałych zagrożeń dla bezpieczeństwa narodowego, a zwłaszcza zagrożenia terrorystycznego, nakłada na operatorów i dostawców usług łączności elektronicznej obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych dotyczących ruchu i lokalizacji wszystkich abonentów, a także danych umożliwiających identyfikację twórców treści oferowanych przez dostawców tych usług;

2) stoi on na przeszkodzie uregulowaniu krajowemu, które nie ustanawia obowiązku informowania osób, których dane dotyczą, o przetwarzaniu ich danych osobowych przez właściwe organy, który to obowiązek nie obejmuje przypadków, w których poinformowanie to zagraża działaniu wspomnianych organów.

3) nie stoi on na przeszkodzie uregulowaniu krajowemu, które zezwala na gromadzenie w czasie rzeczywistym danych dotyczących ruchu i lokalizacji określonych osób w zakresie, w jakim działania te są prowadzone zgodnie z procedurami ustanowionymi w odniesieniu do uzyskiwania dostępu do danych osobowych zatrzymywanych zgodnie z prawem i przy zachowaniu tych samych gwarancji.