Zbiór Orzeczeń

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

Sprawa C-520/18

Ordre des barreaux francophones et germanophone,
Académie Fiscale ASBL,
UA,
Liga voor Mensenrechten ASBL,
Ligue des Droits de l'Homme ASBL,
VZ,
WY,
XX
przeciwko
Conseil des ministres,
przy udziale:
Child Focus

[wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Cour constitutionnelle (trybunał konstytucyjny, Belgia)]

Odesłanie prejudycjalne – Przetwarzanie danych osobowych i ochrona życia prywatnego w sektorze łączności elektronicznej – Dyrektywa 2002/58/WE – Zakres zastosowania – Artykuł 1 ust. 3 – Artykuł 15 ust. 1 – Artykuł 4 ust. 2 TUE – Karta praw podstawowych Unii Europejskiej – Artykuły 4, 6, 7, 8, 11 i 52 ust. 1 – Obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych dotyczących ruchu i lokalizacji – Skuteczność dochodzeń prowadzonych w sprawach karnych i inne cele leżące w interesie publicznym

1. Trybunał w ostatnich latach kontynuował utrwaloną linię orzecznictwa w zakresie zatrzymywania i dostępu do danych osobowych, w 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 w art. 7 i 8 Karty praw podstawowych Unii Europejskiej;

[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).

– 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];

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

2. Wyroki te (w szczególności drugi z nich) budzą niepokój władz niektórych państw członkowskich, ponieważ ich zdaniem prowadzą one do pozbawienia ich instrumentu, który uznają za niezbędny dla zapewnienia bezpieczeństwa narodowego oraz walki z przestępczością i terroryzmem. Dlatego niektóre z tych państw członkowskich opowiadają się za zmianą lub doprecyzowaniem wspomnianego 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 w stosunku do działań związanych z bezpieczeństwem narodowym oraz walką z terroryzmem. Gdyby dyrektywa ta miała mieć zastosowanie w tym zakresie, należałoby następnie wyjaśnić, w jakim stopniu państwa członkowskie mogą ograniczyć chronione przez nią prawo do poszanowania życia prywatnego. Wreszcie należy przeanalizować, w jakim stopniu różne przepisy krajowe (Zjednoczonego Królestwa[8], belgijskie[9] i francuskie[10]) w tej dziedzinie są zgodne z prawem Unii w dokonanej przez Trybunał wykładni.

5. Po zapoznaniu się z wyrokiem Digital Rights Cour constitutionnelle (trybunał konstytucyjny, Belgia) stwierdził nieważność przepisów krajowych, za pomocą których dokonano częściowej transpozycji do prawa krajowego uznanej za nieważną w tym wyroku dyrektywy 2006/24. Ustawodawca belgijski przyjął następnie nowe uregulowanie, którego zgodność z prawem Unii została ponownie podważona w następstwie wydania wyroku Tele2 Sverige i Watson.

6. Szczególna cecha niniejszego odesłania polega na tym, że stwarza ono możliwość tymczasowego utrzymania w mocy skutków przepisu krajowego, którego unieważnienie przez sądy krajowe wynika z jego niezgodności z prawem Unii.

I. Ramy prawne

A. Prawo Unii

7. Odsyłam do odpowiedniej części mojej opinii w sprawach C-511/18 i C-512/18.

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).

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

7 Oprócz niniejszej (sprawa C-520/18, Ordre des barreaux francophones et germanophone i in.) chodzi o sprawy połączone C-511/18 i C-512/18 La Quadrature du Net i in. oraz o sprawę C-623/17, Privacy International.

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.

B. Prawo krajowe. Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques [11]

8. Artykuł 4 tej ustawy stanowi, że art. 126 loi du 13 juin 2005 relative aux communications électroniques [12] otrzymuje następujące brzmienie:

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

Niniejszy artykuł nie odnosi się do treści połączeń.

[…]

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

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

2. służby wywiadowcze i służby bezpieczeństwa w celu wypełniania misji wywiadowczych podjętych z wykorzystaniem metod zbierania danych, o których mowa w art. 16/2, 18/7 i 18/8 loi du 30 novembre 1998 organique des services de renseignement et de Sécurité [13] na określonych w tej ustawie warunkach;

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

4. służby ratownicze udzielające pomocy na miejscu, jeżeli w następstwie zgłoszenia alarmowego nie uzyskają od dostawcy lub danego operatora danych identyfikacyjnych osoby dzwoniącej […] lub otrzymały niepełne dane. Żądanie to może dotyczyć wyłącznie danych identyfikacyjnych zgłaszającego i może być skierowane wyłącznie w ciągu 24 godzin od dokonania zgłoszenia;

11 Ustawa z dnia 29 maja 2016 r. o zbieraniu i zatrzymywaniu danych w sektorze łączności elektronicznej, zwana dalej „ustawą z dnia 29 maja 2016 r." (Moniteur belge z dnia 18 lipca 2016 r., s. 44717).

12 Ustawa z dnia 13 czerwca 2005 r. o łączności elektronicznej, zwana dalej „ustawą z 2005 r." (*Moniteur belge* z dnia 20 czerwca 2005 r., s. 28070).

13 Ustawa organiczna z dnia 30 listopada 1998 r. o służbie wywiadowczej i służbie bezpieczeństwa, zwana dalej „ustawą z 1998 r." (*Moniteur belge* z dnia 18 grudnia 1998 r., s. 40312).

5. funkcjonariusze policji z Cellule des personnes disparues de la Police Fédérale (prowadzonej przez policję federalną komórki ds. osób zaginionych) w ramach pomocy osobie zagrożonej, poszukiwania osób, których zaginięcie budzi podejrzenia oraz jeżeli istnieją uzasadnione poszlaki lub przesłanki wskazujące na fakt bezpośredniego zagrożenia integralności fizycznej osoby zaginionej. Do danego operatora lub dostawcy można zwrócić się, za pośrednictwem służby policji wyznaczonej przez króla, o udostępnienie wyłącznie danych, o których mowa w ust. 3 akapity pierwszy i drugi, dotyczących osoby zaginionej i zatrzymywanych przez 48 godzin poprzedzających złożenie żądania udostępnienia danych;

6. service de mediation pour les telecommunications (służba mediacji w telekomunikacji) w celu ustalenia tożsamości osoby, która w sposób niedozwolony wykorzystała sieć lub usługę łączności elektronicznej […]. Żądanie to może obejmować wyłącznie dane identyfikacyjne.

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

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

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

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

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

Król, w drodze dekretu konsultowanego z radą ministrów, na wniosek ministra sprawiedliwości i ministra oraz po zasięgnięciu opinii Commission de la protection de la vie privée (komisji ochrony życia prywatnego) i instytutu, ustala rodzaje danych podlegających przechowaniu z podziałem na typy kategorii określonych w akapitach 1–3, jak również wymogi, które dane te muszą spełniać.

4. Zatrzymując dane, o których mowa w ust. 3, dostawcy i operatorzy wymienieni w ust. 1 akapit pierwszy:

1. gwarantują, że przechowywane dane są takiej samej jakości i podlegają takim samym zasadom bezpieczeństwa i ochrony jak dane w sieci;

2. dbają o to, by w stosunku do zatrzymywanych danych stosowane były właściwe środki techniczne i organizacyjne mające na celu ochronę tych danych przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, a także nieupoważnionym lub bezprawnym zatrzymywaniem, przetwarzaniem, dostępem lub ujawnieniem;

3. gwarantują, że dostęp do danych zatrzymywanych, aby uczynić zadość żądaniom organów, o których mowa w ust. 2, przyznawany jest wyłącznie jednemu lub kilku członkom komórki koordynacyjnej, o której mowa w art. 126/1 ust. 1;

4. zatrzymują dane na terytorium Unii Europejskiej;

5. stosują środki ochrony technicznej, które powodują, że dane stają się, natychmiast po ich rejestracji, nieodczytywalne i nieużyteczne dla jakiejkolwiek osoby, która nie jest uprawniona do dostępu;

6. bez uszczerbku dla art. 122 i 123, po określonego w ust. 3 upływie okresu ich przechowania, niszczą dane zatrzymywane na dowolnego rodzaju nośnikach;

7. zapewniają możliwość śledzenia tego, w jaki sposób wykorzystywane są dane zatrzymywane w związku z uwzględnieniem poszczególnych żądań udostępnienia takich danych skierowanych przez organ, o którym mowa w ust. 2.

Możliwość śledzenia, o której mowa w ust. 1 pkt 7, realizowana jest za pomocą prowadzonego rejestru. Instytut i Commission pour la protection de la vie privée mogą kontrolować ten rejestr lub zażądać kopii jego całości lub części. Instytut i Commission pour la protection de la vie privée zawierają porozumienie o współpracy w sprawie wglądu i kontroli zawartości rejestru.

5. Minister i minister sprawiedliwości przekazują corocznie Izbie Reprezentantów statystyki na temat zatrzymywania danych generowanych lub przetwarzanych w ramach świadczenia ogólnie dostępnych usług lub udostępniania ogólnie dostępnych sieci łączności.

Statystyki te obejmują w szczególności:

1. przypadki, w których właściwym organom przekazane zostały informacje zgodnie z mającym zastosowanie prawem krajowym;

2. czas, jaki upłynął między datą, od której dane były zatrzymywane, a datą, w której właściwe organy zażądały ich przekazania;

3. przypadki, w których wnioski o udostępnienie danych nie mogły zostać uwzględnione.

Statystyki te nie mogą obejmować danych osobowych.

[…]”.

9. Artykuł 5 wprowadza do ustawy z 2005 r. art. 126/1 o następującym brzmieniu:

„1. W ramach każdego operatora i dostawcy, o których mowa w art. 126 ust. 1 akapit pierwszy, powołuje się komórkę koordynacyjną odpowiedzialną za przekazywanie upoważnionym w przepisach prawa organom władzy w Belgii, na ich wniosek, danych zatrzymywanych na podstawie art. 122, 123 i 126, danych identyfikacyjnych osoby inicjującej połącznie zgodnie z art. 107 ust. 2 akapit pierwszy i danych, których udostępnienia można być wymagane na mocy art. 46 bis, 88 bis i 90 ter kodeksu postępowania karnego oraz art. 18/7, 18/8, 18/16 i 18/17 [ustawy z 1998 r.].

[…]

2. Operatorzy i dostawcy, o których mowa w art. 126 ust. 1 akapit pierwszy, ustanawiają wewnętrzną procedurę ustosunkowywania się do kierowanych przez te organy żądań udzielenia dostępu do danych osobowych użytkowników. Przedstawiają oni instytutowi, na wniosek, informacje o tych procedurach, liczbie otrzymanych wniosków, ich uzasadnieniu prawnym oraz udzielonej przez nich odpowiedzi.

[…]

3. Operatorzy i dostawcy, o których mowa w art. 126 ust. 1 akapit pierwszy, wyznaczają jednego lub kilku pełnomocników ds. ochrony danych osobowych, którzy muszą spełniać kumulatywnie przesłanki wymienione w ust. 1 akapit trzeci.

[…]

Przy wykonywaniu swoich zadań pełnomocnik ds. ochrony danych osobowych działa w sposób niezależny oraz ma dostęp do wszystkich danych osobowych przekazywanych władzom i do wszystkich pomieszczeń dostawcy lub operatora.

[…]

4. Król, w drodze dekretu konsultowanego z radą ministrów i po uzyskaniu opinii Commission pour la protection de la vie privée i instytutu ustala:

[…]

2. wymogi, jakie musi spełnić komórka koordynacyjna, z uwzględnieniem sytuacji tych operatorów i dostawców, którzy otrzymują niewiele żądań kierowanych przez organy sądowe, nie mają siedziby w Belgii lub działają głównie z zagranicy;

3. informacje, jakie należy przekazywać instytutowi oraz Commission pour la protection de la vie privée zgodnie z ust. 1 i 3 oraz organy, które mają dostęp do tych informacji;

4. inne zasady regulujące współpracę operatorów i dostawców, o których mowa w art. 126 ust. 1 akapit pierwszy, z władzami belgijskimi lub z niektórymi z nich w zakresie przekazywania danych, o których mowa w ust. 1, w tym – o ile to konieczne i w odniesieniu do każdego zainteresowanego organu – formę i treść kierowanego żądania.

[…]”.

10. Artykuł 8 stanowi, że art. 46 bis ust. 1 kodeksu postępowania karnego otrzymuje następujące brzmienie:

„1. Prowadząc dochodzenie w sprawie przestępstwa, prokurator może, w drodze pisemnej i uzasadnionej decyzji, korzystając w razie potrzeby z pomocy operatora sieci łączności elektronicznej, dostawcy usługi łączności elektronicznej lub wyznaczonej przez króla służby policyjnej, na podstawie wszystkich posiadanych przez niego informacji lub w drodze dostępu do rejestrów klientów operatorów lub dostawców usługi, przystąpić lub nakazać przystąpienie do:

1. identyfikacji abonenta lub regularnego użytkownika usługi łączności elektronicznej lub użytego środka łączności elektronicznej;

2. identyfikacji usług łączności elektronicznej, których abonentem jest określona osoba lub z których zazwyczaj korzysta określona osoba.

Należy wykazać, że przyjmowany środek jest proporcjonalny w odniesieniu do celu polegającego na poszanowaniu życia prywatnego i pomocniczy w stosunku do każdego innego obowiązku w ramach dochodzenia.

W wyjątkowo nagłych przypadkach każdy funkcjonariusz policji sądowej może, za uprzednią ustną zgodą prokuratora oraz w drodze uzasadnionej decyzji na piśmie, zażądać przekazania wspomnianych danych. Funkcjonariusz policji sądowej powiadamia prokuratora w ciągu 24 godzin o tej uzasadnionej pisemnej decyzji oraz o uzyskanych informacjach i uzasadnia wyjątkowo nagły charakter.

W odniesieniu do przestępstw, które nie są zagrożone karą jednego roku pozbawienia wolności lub surowszą, prokurator lub, w wyjątkowo nagłych przypadkach, funkcjonariusz policji sądowej może zażądać przekazania danych, o których mowa w ust. 1, wyłącznie z okresu sześciu miesięcy poprzedzających wydanie przez niego decyzji.

2. Operator sieci łączności elektronicznej i dostawca usług łączności elektronicznej, który jest zobowiązany do przekazania danych, o których mowa w ust. 1, przekazuje żądane dane prokuratorowi lub funkcjonariuszowi policji sądowej w terminie określonym przez króla […].

[…]

Każdy, kto w ramach pełnionej funkcji dowiaduje się o danym środku lub pomaga w jego podjęciu, jest zobowiązany do zachowania tajemnicy. Każde naruszenie wspomnianej tajemnicy jest karane zgodnie z przepisami art. 458 kodeksu karnego.

Odmowa przekazania danych podlega karze grzywny w wysokości od 26 EUR do 10 000 EUR”.

11. Artykuł 9 nadaje art. 88 bis kodeksu postępowania karnego następujące brzmienie:

„1. Jeżeli istnieją poważne poszlaki wskazujące na możliwość popełnienia przestępstwa zagrożonego karą pozbawienia wolności w wymiarze nie mniejszym niż jeden rok, a sędzia śledczy stwierdzi, że istnieją okoliczności wskazujące na konieczność uzyskania wiadomości elektronicznych lub lokalizacji pochodzenia lub przeznaczenia wiadomości elektronicznych w celu ustalenia stanu faktycznego, sędzia ten jest uprawniony, korzystając w razie potrzeby

bezpośrednio lub za pośrednictwem służby policyjnej wyznaczonej przez króla z pomocy operatora sieci łączności elektronicznej lub dostawcy usługi łączności elektronicznej, do podjęcia decyzji dotyczącej:

1. uzyskania danych dotyczących ruchu środków łączności elektronicznej, z których lub do których kierowane są lub były wiadomości elektroniczne;

2. lokalizacji pochodzenia lub przeznaczenia wiadomości elektronicznych.

W przypadkach przewidzianych w akapicie pierwszym, w odniesieniu do każdego środka łączności elektronicznej, dla którego ustalono dane dotyczące połączenia lub w przypadku którego ustalono miejsce pochodzenia lub przeznaczenia wiadomości telekomunikacyjnej, w protokole podaje się dzień, godzinę, czas trwania oraz, jeśli to konieczne, miejsce, z którego nastąpiła łączność elektroniczna.

Sędzia śledczy wskazuje, w drodze uzasadnionego postanowienia, okoliczności faktyczne sprawy, które uzasadniają skorzystanie z tego środka, to, że jest on proporcjonalny w stosunku do celu polegającego na poszanowaniu życia prywatnego i pomocniczy w stosunku do każdego innego obowiązku w ramach dochodzenia.

Sędzia śledczy określa również okres, przez jaki dany środek może mieć zastosowanie w przyszłości, przy czym okres ten nie może przekraczać dwóch miesięcy od daty wydania postanowienia, z możliwością odnowienia, oraz w danym przypadku okres w przeszłości, który jest objęty postanowieniem zgodnie z ust. 2.

[…]

2. W odniesieniu do zastosowania środka, o którym mowa w ust. 1 akapit pierwszy, do danych dotyczących ruchu lub lokalizacji przechowywanych na podstawie art. 126 ustawy […] z 2005 r. […], stosuje się następujące przepisy:

– w odniesieniu do przestępstw wymienionych w księdze II tytuł I ter kodeksu karnego sędzia śledczy może, w drodze postanowienia, zażądać danych za okres dwunastu miesięcy poprzedzających datę wydania postanowienia;

– w przypadku innych przestępstw wymienionych w art. 90 ter ust. 2–4, które nie zostały wymienione w tiret pierwszym, w przypadku przestępstw, które zostały popełnione w ramach organizacji przestępczej i o których mowa w art. 324 bis kodeksu karnego, lub w przypadku przestępstw zagrożonych karą pozbawienia wolności co najmniej pięciu lat sędzia śledczy może zażądać, w drodze postanowienia, danych za okres dziewięciu miesięcy poprzedzających datę wydania postanowienia;

– w przypadku innych przestępstw sędzia śledczy może żądać danych obejmujących wyłącznie okres sześciu miesięcy poprzedzających datę wydania postanowienia.

3. Wspomniany środek może dotyczyć środków łączności elektronicznej adwokata lub lekarza wyłącznie w sytuacji, gdy osoba taka jest podejrzana o popełnienie przestępstwa, o którym mowa w ust. 1, lub o udział w popełnieniu takiego przestępstwa lub jeśli określone okoliczności wskazują, że osoby podejrzane o popełnienie rzeczonych przestępstw wykorzystują środki łączności elektronicznej należące do tej osoby.

Środek może zostać przyjęty wyłącznie po uprzednim poinformowaniu, odpowiednio, dziekana właściwej rady adwokackiej lub prezesa izby lekarskiej. Te same osoby zostaną poinformowane przez sędziego śledczego o informacjach, które uzna on za objęte tajemnicą zawodową. Informacje te nie są wyszczególniane w protokole.

4. […]

Każdy, kto w ramach pełnionej funkcji dowiaduje się o danym środku lub pomaga w jego podjęciu, jest zobowiązany do zachowania tajemnicy. Każde naruszenie wspomnianej tajemnicy jest karane zgodnie z przepisami art. 458 kodeksu karnego.

[…]".

12. Na podstawie art. 12, art. 13 ustawy z 1998 r. otrzymuje następujące brzmienie:

„Służby wywiadowcze i służby bezpieczeństwa mogą wyszukiwać, gromadzić, odbierać i przetwarzać informacje i dane osobowe, które mogą być przydatne w wykonywaniu ich zadań, i aktualizować dokumentację dotyczącą wydarzeń, grup i osób mających znaczenie dla wykonywania ich zadań.

Informacje zawarte we wspomnianej dokumentacji muszą mieć związek z celem danej sprawy i ograniczać się do jej potrzeb.

Służby wywiadowcze i służby bezpieczeństwa zapewniają bezpieczeństwo danych dotyczących ich źródeł oraz informacji i danych osobowych dostarczonych z tych źródeł.

Funkcjonariusze służb wywiadowczych i służb bezpieczeństwa mają dostęp do informacji, zapytań i danych osobowych gromadzonych i przetwarzanych przez ich służby, o ile są one przydatne w wykonywaniu ich funkcji lub zadań. […]".

13. Artykuł 14 nadaje nowe brzmienie art. 18/3 ustawy z 1998 r., który obecnie stanowi:

„1. Specjalne metody zbierania danych wymienionych w art. 18/2 ust. 1 mogą zostać wdrożone w sytuacji potencjalnego zagrożenia, o którym mowa w art. 18/1, o ile zwykłe metody zbierania danych nie są wystarczające dla uzyskania informacji potrzebnych do powodzenia misji wywiadowczej. Specjalną metodę należy wybrać w zależności od wagi potencjalnego zagrożenia, w odniesieniu do którego się ją wdraża.

Metoda specjalna może zostać wdrożona dopiero po uzasadnionej decyzji pisemnej kierownika danej służby i po powiadomieniu o tej decyzji komisji.

2. W decyzji kierownika danej służby wskazywane są:

1. charakter tej specjalnej metody;

2. w zależności od przypadku – osoby fizyczne lub prawne, stowarzyszenia lub zrzeszenia, obiekty, miejsca, wydarzenia lub informacje podlegające tej specjalnej metodzie;

3. potencjalne zagrożenie, które uzasadnia zastosowanie tej specjalnej metody;

4. okoliczności faktyczne, które uzasadniają zastosowanie tej specjalnej metody oraz pomocniczy i proporcjonalny charakter tej metody, w tym uwzględniające związek między pkt 2 a pkt 3;

5. okres, w którym można stosować tę specjalną metodę, liczony od dnia powiadomienia o decyzji komisji;

[…]

9. w stosownych przypadkach – poważne poszlaki świadczące o tym, że adwokat, lekarz lub dziennikarz uczestniczy lub uczestniczył aktywnie i osobiście w tworzeniu lub rozwoju potencjalnego zagrożenia;

10. w przypadku, gdy zastosowanie ma art. 18/8 – uzasadnienie czasu trwania okresu, którego dotyczy zbieranie danych;

[…]

8. Kierownik służby nakazuje zakończenie stosowania specjalnej metody, jeżeli ustąpiło potencjalne zagrożenie, które uzasadniało zastosowanie tego środka, jeżeli metoda nie jest już przydatna dla celu, dla którego ją zastosowano, albo jeżeli stwierdzono, że dopuszczono się naruszenia prawa. Kierownik służby informuje niezwłocznie komisję o swojej decyzji. […]”.

14. Artykuł 18/8 ustawy z 1988 r. brzmi następująco:

„1. Służby wywiadowcze i służby bezpieczeństwa mogą, w celu wykonywania swoich zadań, w razie konieczności zwracając się o wsparcie techniczne do operatora sieci łączności elektronicznej lub dostawcy usługi łączności elektronicznej, przystąpić lub nakazać przystąpienie do:

1. uzyskiwania danych dotyczących ruchu środków łączności elektronicznej, z których lub do których kierowane są lub były wiadomości elektroniczne;

2. lokalizacji pochodzenia lub przeznaczenia wiadomości elektronicznych.

[…]

2. w odniesieniu do stosowania metody, o której mowa w ust. 1, do danych zatrzymywanych na podstawie art. 126 ustawy z […] 2005 r. […] zastosowanie mają następujące przepisy:

1. w odniesieniu do potencjalnego zagrożenia związanego z działalnością, która może mieć związek z organizacjami przestępczymi lub sektami, kierownik danej służby może w swojej decyzji zażądać jedynie danych za okres nie dłuższy niż sześć miesięcy poprzedzających wydanie decyzji;

2. w odniesieniu do potencjalnego zagrożenia innego niż wymienione w pkt 1 i 3 kierownik danej służby może w swojej decyzji zażądać danych za okres nie dłuższy niż dziewięć miesięcy poprzedzających wydanie decyzji;

3. w odniesieniu do potencjalnego zagrożenia związanego z działalnością, która może mieć związek z terroryzmem lub ekstremizmem, kierownik danej służby może w swojej decyzji zażądać jedynie danych za okres nie dłuższy niż dwanaście miesięcy poprzedzających wydanie decyzji. […]".

II. Okoliczności faktyczne i pytania prejudycjalne

15. W wyroku z dnia 11 czerwca 2015 r.[14] Cour constitutionnelle stwierdził nieważność art. 126 ustawy z 2005 r. w jego nowym brzmieniu z tych samych powodów, dla których Trybunał stwierdził nieważność dyrektywy 2006/24 w wyroku Digital Rights.

16. W związku ze wspomnianym stwierdzeniem nieważności ustawodawca krajowy przyjął (przed wydaniem wyroku Tele 2 Sverige i Watson) ustawę z dnia 29 maja 2016 r.

17. VZ i in., Ordre des barreaux francophones et germanophone (zwany dalej „Ordre des barreaux"), Liga voor Mensenrechten ASBL (zwana dalej „LMR"), Ligue des Droits de l'Homme ASBL (zwana dalej „LDH") i Académie Fiscale ASBL (zwana dalej „Académie Fiscale") wnieśli do sądu odsyłającego kilka skarg konstytucyjnych na wspomnianą ustawę, podnosząc co do zasady, że wykracza ona poza to, co jest ściśle konieczne, i nie zapewnia wystarczających gwarancji ochrony.

18. W tym kontekście Cour constitutionnelle przedłożył Trybunałowi Sprawiedliwości następujące pytania:

„1) Czy art. 15 ust. 1 dyrektywy 2002/58/WE w związku z prawem do bezpieczeństwa zagwarantowanym w art. 6 Karty praw podstawowych Unii Europejskiej (»karty«) oraz prawem do ochrony danych osobowych zagwarantowanym w art. 7, 8 i art. 52 ust. 1 karty […] należy interpretować w ten sposób, że sprzeciwia się on uregulowaniu krajowemu takiemu jak rozpatrywane w postępowaniu głównym, przewidującemu dla operatorów i dostawców usług łączności elektronicznej powszechny obowiązek [zatrzymywania] wszystkich danych o ruchu i lokalizacji w rozumieniu dyrektywy 2002/58/WE, generowanych lub przetwarzanych w ramach świadczenia tych usług, które to uregulowanie ma na celu nie tylko dochodzenie, wykrywanie i karanie poważnych przestępstw, ale także zapewnienie bezpieczeństwa narodowego, obrony terytorium i bezpieczeństwa publicznego oraz zapobieganie, dochodzenie, wykrywanie i karanie przestępstw innych niż poważne lub zapobieganie niedozwolonemu używaniu systemów łączności elektronicznej lub realizuje inny cel, który jest wymieniony w art. 23 ust. 1 rozporządzenia [Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. 2016, L 119, s. 1)] i który ponadto jest objęty gwarancjami określonymi w tym uregulowaniu w zakresie przechowywania danych i dostępu do nich?

2) Czy art. 15 ust. 1 dyrektywy 2002/58/WE w związku z art. 4, 7, 8, 11 i art. 52 ust. 1 karty […] należy interpretować w ten sposób, że sprzeciwia się on uregulowaniu krajowemu takiemu jak rozpatrywane w postępowaniu głównym, które przewiduje spoczywający na operatorach i dostawcach usług łączności elektronicznej powszechny obowiązek [zatrzymywania] danych o ruchu i lokalizacji w rozumieniu dyrektywy 2002/58/WE, generowanych lub przetwarzanych przez nich w związku ze świadczeniem tych usług, jeżeli uregulowanie to ma

[14] Wyrok nr 84/2015, *Moniteur belge* z dnia 11 sierpnia 2015 r.

na celu wypełnienie pozytywnych obowiązków nałożonych na organy zgodnie z art. 4 i 8 karty, polegających na ustanowieniu ram prawnych, które umożliwiają skuteczne prowadzenie dochodzenia w sprawach karnych oraz skuteczne zwalczanie wykorzystywania seksualnego małoletnich, a także skuteczne zidentyfikowanie sprawcy czynu karalnego nawet w przypadku korzystania ze środków łączności elektronicznej?

3) Jeżeli na podstawie odpowiedzi udzielonych na pierwsze lub drugie pytanie prejudycjalne Cour constitutionnelle (trybunał konstytucyjny) miałby dojść do wniosku, że zaskarżona ustawa narusza jeden lub więcej obowiązków wynikających z przepisów wskazanych w tych pytaniach, czy mógłby on tymczasowo utrzymać w mocy skutki ustawy z dnia 29 maja 2016 r. o [zbieraniu i zatrzymywaniu] danych w sektorze łączności elektronicznej, aby uniknąć niepewności prawa i zapewnić możliwość dalszego wykorzystywania danych uprzednio [zebranych i zatrzymywanych] do celów określonych w [ustawie]?".

III. Postępowanie przed Trybunałem

19. Niniejsze odesłanie prejudycjalne wpłynęło do Trybunału w dniu 2 sierpnia 2018 r.

20. Uwagi na piśmie zostały złożone przez VZ i in., Académie Fiscale, LMR, LDH, Ordre des barreaux, Fondation pour Enfants Disparus et Sexuellement Exploités (Child Focus), rządy: niemiecki, belgijski, Zjednoczonego Królestwa, czeski, cypryjski, duński, hiszpański, estoński, francuski, węgierski, Irlandia, rządy niderlandzki, polski i szwedzki, a także przez Komisję.

21. W dniu 9 września 2019 r. odbyła się jawna rozprawa, którą przeprowadzono łącznie także dla spraw C-511/18, C-512/18, C-623/17 i w której udział wzięły strony występujące w czterech postępowaniach w przedmiocie odesłań prejudycjalnych, wyżej wymienione rządy oraz rząd Norwegii, a także Komisja oraz Europejski Inspektor Ochrony Danych.

IV. Analiza

22. Pierwsze pytanie niniejszego odesłania pokrywa się co do zasady z pytaniami zadanymi w sprawach połączonych C-511/18 i C-512/28. Pytanie to różni się jednak od tych ostatnich pod względem celów, realizacji których służy uregulowanie krajowe: obejmują one nie tylko walkę z terroryzmem i najpoważniejszymi formami przestępczości lub ochronę bezpieczeństwa narodowego, lecz także „obronę terytorium, bezpieczeństwo publiczne, dochodzenie, wykrywanie i ściganie przestępstw innych niż poważne" oraz, ogólnie rzecz biorąc, każdy z celów przewidzianych w art. 23 ust. 1 rozporządzenia nr 2016/679.

23. Drugie pytanie wiąże się z pierwszym, uzupełniając je, gdyż ma ono na celu ustalenie, czy pozytywne obowiązki spoczywające na władzy publicznej w zakresie dochodzenia i karania wykorzystywania seksualnego małoletnich uzasadniają przyjmowanie spornych środków.

24. Trzecie pytanie zostało zadane na wypadek, gdyby przepis krajowy był niezgodny z prawem Unii. Sąd odsyłający zmierza do ustalenia, czy w takim przypadku możliwe byłoby tymczasowe utrzymanie w mocy skutków ustawy z dnia 29 maja 2016 r.

25. Zbadam powyższe kwestie, analizując przede wszystkim możliwość zastosowania dyrektywy 2002/58, w związku z czym odniosę się do moich opinii w sprawach innych ze wspomnianych odesłań prejudycjalnych. W drugiej kolejności przedstawię główne kierunki, w których rozwija się orzecznictwo Trybunału w tej dziedzinie i możliwości jego rozwoju. Wreszcie, spróbuję udzielić odpowiedzi na każde z zadanych pytań prejudycjalnych.

A. Możliwość zastosowania dyrektywy 2002/58

26. Podobnie jak w przypadku pozostałych trzech odesłań prejudycjalnych, również w niniejszym przypadku poddano w wątpliwość możliwość zastosowania dyrektywy 2002/58. Biorąc pod uwagę zbieżność stanowisk zajmowanych w tym względzie przez państwa członkowskie, odsyłam do ujęcia tej kwestii w opinii w sprawach połączonych C-511/18 i C-512/18 [15].

B. Orzecznictwo Trybunału dotyczące zatrzymywania danych osobowych i udzielania organom władzy publicznej dostępu do nich do w ramach dyrektywy 2002/58

1. Zasada poufności połączeń i związanych z nimi danych

27. Przepisy dyrektywy 2002/58 „dookreślają i uzupełniają" dyrektywę 95/46/WE [16] w celu osiągnięcia wysokiego poziomu ochrony danych osobowych w kontekście świadczenia usług łączności elektronicznej [17].

28. Artykuł 5 ust. 1 dyrektywy 2002/58 stanowi, że państwa członkowskie muszą zapewnić w swoim ustawodawstwie krajowym poufność komunikacji za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej; muszą one również zapewnić poufność odpowiednich danych o ruchu.

29. Ta poufność komunikacji obejmuje m.in. (art. 5 ust. 1 zdanie drugie dyrektywy 2002/58) zakaz przechowywania przez jakiekolwiek osoby inne niż użytkownicy, bez ich zgody, danych o ruchu związanych z łącznością elektroniczną. Wyjątek „stanowią podmioty posiadające upoważnienia […] oraz techniczne przechowywanie, które jest niezbędne do przekazania komunikatu" [18].

30. Artykuły 5, 6 i 9 ust. 1 dyrektywy 2002/58 mają na celu zachowanie poufności komunikacji i związanych z nią danych oraz zminimalizowanie ryzyka nadużyć. Jej zakres należy oceniać w świetle motywu trzydziestego wspomnianej dyrektywy, zgodnie z którym „[s]ystemy dostarczania sieci i usług łączności elektronicznej powinny być zaprojektowane w taki sposób, aby ograniczać ilość niezbędnych danych osobowych do ścisłego *minimum*" [19].

15 Punkt 40 i nast.

16 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). Zobacz art. 1 ust. 2 dyrektywy 2002/58. Dyrektywa 95/46 została uchylona z dniem 25 maja 2018 r. rozporządzeniem nr 2016/679. W związku z tym, w zakresie, w jakim dyrektywa 2002/58 odnosi się do dyrektywy 95/46 lub nie ustanawia własnych uregulowań, konieczne jest uwzględnienie przepisów tego rozporządzenia (zob. art. 94 ust. 1 i 2 rozporządzenia nr 2016/679).

17 Wyrok Tele2 Sverige i Watson, pkt 82, 83.

18 Ibidem, pkt 85 i przytoczone tam orzecznictwo.

19 Ibidem, pkt 87. Wyróżnienie własne.

31. W odniesieniu do tych danych wyróżnia się:

– dane o *ruchu*, których przetwarzanie i zatrzymywanie jest dozwolone wyłącznie w zakresie niezbędnym do naliczenia opłat za usługi, wprowadzania ich do obrotu i świadczenia usług o wartości dodanej (art. 6 dyrektywy 2002/58) i przez niezbędny do tego czas. Po upływie tego okresu dane, które podlegały przetwarzaniu i zatrzymywaniu, powinny zostać usunięte lub zanonimizowane [20];

– dane dotyczące *lokalizacji* inne niż dane o ruchu mogą być przetwarzane wyłącznie po spełnieniu pewnych warunków i po ich anonimizacji lub za zgodą użytkowników lub abonentów (art. 9 ust. 1 dyrektywy 2002/58) [21].

2. Klauzula ograniczająca przewidziana w art. 15 ust. 1 dyrektywy 2002/58

32. Artykuł 15 ust. 1 dyrektywy 2002/58 zezwala państwom członkowskim na „uchwal[anie] środk[ów] ustawodawcz[ych] w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4, i art. 9" tej dyrektywy.

33. Wszelkie ograniczenia muszą stanowić „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]".

34. Takie wyliczenie celów ma charakter wyczerpujący [22]: tytułem przykładu („między innymi") dozwolone są „środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie".

35. W każdym razie „[w]szystkie 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". Artykuł 15 ust. 1 dyrektywy 2002/58 należy zatem interpretować w świetle praw podstawowych zagwarantowanych w karcie [23].

36. Spośród praw uznanych w karcie Trybunał wymienił – w zakresie, w jakim jest to istotne w niniejszej sprawie – prawo do poszanowania życia prywatnego (art. 7), prawo do ochrony danych osobowych (art. 8) i prawo do wolności wypowiedzi (art. 11) [24].

37. Trybunał podkreślił również, jako wytyczną dla dokonywanej przezeń wykładni art. 15 ust. 1 dyrektywy 2002/58, że ograniczenia dotyczące obowiązku zapewnienia poufności komunikacji i związanych z nią danych o ruchu powinny podlegać ścisłej wykładni.

20 Ibidem, pkt 86 i przytoczone tam orzecznictwo.

21 Ibidem, pkt 86 in fine.

22 Ibidem, pkt 90.

23 Ibidem, pkt 91 i przytoczone tam orzecznictwo.

24 Ibidem, pkt 93 i przytoczone tam orzecznictwo.

38. W szczególności Trybunał odrzucił możliwość „uczynienia reguły z odstępstwa od tego mającego zasadnicze znaczenie obowiązku, a szczególności od zakazu przechowywania tych danych, ustanowionego w art. 5 tej dyrektywy, gdyż w znacznym stopniu pozbawiłoby to ten przepis jego znaczenia” [25].

39. Powyższe dwa spostrzeżenia wydają mi się decydujące dla zrozumienia, dlaczego Trybunał uznał, że uogólnione i niezróżnicowane zatrzymywanie danych dotyczących ruchu i lokalizacji, związanych z łącznością elektroniczną, jest niezgodne z dyrektywą 2002/58.

40. Poprzez powyższe stwierdzenie Trybunał jedynie zastosował „współmiernie” [26] kryterium proporcjonalności, które stosował już wcześniej [27]: „ochrona prawa podstawowego do poszanowania życia prywatnego na poziomie Unii wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co absolutnie konieczne” [28].

3. Proporcjonalność zatrzymywania danych

a) Nieproporcjonalność uogólnionego i niezróżnicowanego zatrzymywania

41. Trybunał uznał, że walka z poważną przestępczością, w szczególności z przestępczością zorganizowaną i terroryzmem, ma pierwszorzędne znaczenie dla zapewnienia bezpieczeństwa publicznego, zaś jej skuteczność może w znacznym stopniu zależeć od wykorzystania nowoczesnych technik dochodzeniowo-śledczych. Dodał, że „jednakże tego rodzaju cel interesu ogólnego, mimo że ma on fundamentalne znaczenie, sam w sobie nie uzasadnia stwierdzenia, że system zatrzymywania danych taki jak ten ustanowiony przez dyrektywę 2006/24, jest konieczny do celów tej walki” [29].

42. Aby móc stwierdzić, czy taki środek ogranicza się do tego, co jest ściśle niezbędne, Trybunał podkreślił przede wszystkim to, jak szczególnie mocno ingeruje on w prawa podstawowe ustanowione w art. 7 i 8 karty [30]. Owa szczególna waga ingerencji wynika właśnie z okoliczności, iż ustawodawstwo krajowe przewidywało „uogólnione i niezróżnicowane zatrzymywanie *wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników w odniesieniu do wszystkich środków łączności elektronicznej i że nakłada ono na dostawców usług łączności elektronicznej obowiązek zatrzymywania tych danych w sposób regularny i ciągły, i to bez żadnych wyjątków*” [31].

43. Ta ingerencja w życie obywateli, jaką stanowił rzeczony środek, znajduje odzwierciedlenie w dokonanych przez Trybunał ocenach dotyczących skutków zatrzymywania danych.

25 Ibidem, pkt 89.

26 Użycie tego przysłówka w wyroku Tele2 Sverige i Watson, pkt 95, wynika z motywu jedenastego dyrektywy 2002/58.

27 Wyrok Digital Rights, pkt 48: „[M]ając na uwadze, po pierwsze, znaczącą rolę, jaką odgrywa ochrona danych osobowych w świetle prawa podstawowego do poszanowania życia prywatnego oraz, po drugie, zakres i wagę ingerencji w to prawo, której źródłem jest dyrektywa 2006/24, uprawnienia dyskrecjonalne prawodawcy Unii są ograniczone, skutkiem czego kontrola tych uprawnień musi mieć charakter ścisły”.

28 Wyrok Tele2 Sverige i Watson, pkt 96 i przytoczone tam orzecznictwo.

29 Wyrok Digital Rights, pkt 51. Zobacz podobnie wyrok Tele2 Sverige i Watson, pkt 103.

30 Wyroki: Digital Rights, pkt 65; Tele2 Sverige i Watson, pkt 100.

31 Wyrok Tele2 Sverige i Watson, pkt 97. Wyróżnienie własne.

Dane te [32]

– „[…] pozwalają na odnalezienie i ustalenie źródła oraz odbiorcy połączenia, określenie daty, godziny i czasu trwania połączenia oraz jego rodzaju, określenie narzędzia komunikacji i identyfikację lokalizacji urządzenia komunikacji ruchomej” [33];

– „[…] pozwalają w szczególności ustalić, z jaką osobą i za pomocą jakiego środka komunikował się abonent lub zarejestrowany użytkownik, a także – czas połączenia oraz miejsce, z którego zostało ono nawiązane. Dzięki nim można też ustalić częstotliwość komunikowania się abonenta lub zarejestrowanego użytkownika z określonymi osobami w danym okresie” [34];

– „[…] mo[gą] dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, których dane są zatrzymywane, takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazyjnie pokonywane trasy, podejmowane czynności, relacje społeczne i środowiska społeczne, w których osoby te się obracają” [35].

– „[…] dają możność ustalenia profilu danych osób, która to informacja jest z punktu widzenia prawa do poszanowania życia prywatnego równie newralgiczna co sama treść komunikatów” [36].

44. Ingerencja ta może ponadto spowodować „powstanie po ich stronie wrażenia, iż ich prywatne życie podlega ciągłej obserwacji”, gdyż „użytkownicy usług łączności elektronicznej nie wiedzą o tym, że dane te są zatrzymywane” [37].

45. Ze względu na wagę tej ingerencji jedynie walka z poważną przestępczością mogłaby uzasadniać taki środek przechowywania danych [38]. Wspomniany środek nie może jednak stać się regułą, ponieważ „system ustanowiony przez dyrektywę 2002/58 ustanawia wymóg, by takie zatrzymywanie danych było wyjątkiem” [39].

46. Ponadto zdaniem Trybunału należy wyróżnić dwie cechy wynikające z okoliczności polegającej na tym, że sporny środek nie przewidywał „jakiegokolwiek zróżnicowania, ograniczenia ani wyjątku zależnego od zamierzonego celu” [40] oraz „nie wymaga istnienia żadnego związku między danymi, których zatrzymywanie nakazuje, a zagrożeniem dla bezpieczeństwa publicznego” [41]:

– po pierwsze, środek obejmuje „całościowo wszystkie korzystające z usług łączności elektronicznej osoby, nawet wtedy, gdy nie ma wobec nich żadnych podstaw, nawet pośrednich, do wszczęcia postępowania karnego. […] Ponadto dyrektywa nie przewiduje żadnych wyjątków, a więc w rezultacie ma zastosowanie nawet wobec tych osób, których łączność na gruncie przepisów prawa krajowego objęta jest tajemnicą zawodową” [42];

32 Do owych danych należą w szczególności nazwisko i imię oraz adres abonenta lub zarejestrowanego użytkownika, numer telefonu nadawcy i odbiorcy połączenia, a także, w przypadku usług internetowych, adres IP.

33 Wyrok Tele2 Sverige i Watson, pkt 98.

34 Ibidem, pkt 98.

35 Ibidem, pkt 99.

36 Ibidem, pkt 99 in fine.

37 Ibidem, pkt 100.

38 Ibidem, pkt 102.

39 Ibidem, pkt 104.

40 Ibidem, pkt 105.

41 Ibidem, pkt 106.

42 Ibidem, pkt 105.

– po drugie, „[n]ie zawiera […] 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” [43].

47. W tych okolicznościach analizowane uregulowanie krajowe przekraczało granice tego, co było ściśle konieczne. Nie można było zatem uznać go za uzasadnione w demokratycznym społeczeństwie, zgodnie z wymogami określonymi w art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty [44].

b) Dopuszczalność indywidualnego zatrzymywania danych

48. Trybunał uznał, że przepisy krajowe „dopuszczając[e] w ramach prewencji *indywidualne zatrzymywanie* danych dotyczących ruchu i danych o lokalizacji w celu zwalczania poważnej przestępczości” są zgodne z prawem Unii [45].

49. Ważność takiego indywidualnego przechowywania danych jest uzależniona od tego, czy „w zakresie dotyczącym kategorii danych podlegających zatrzymywaniu, stosowanych środków łączności, zaangażowanych w ten proces podmiotów oraz przyjętego okresu przechowywania danych – nie będzie wykraczać poza to, co jest absolutnie konieczne”.

50. Określone w wyroku Tele2 Sverige i Watson wskazówki umożliwiające stwierdzenie, kiedy przesłanki te zostały spełnione, nie są (być może nie mogły być) wyczerpujące i są sformułowane w sposób dość ogólny. Aby spełnić owe przesłanki, państwa członkowskie:

– muszą wprowadzić jasne i dokładne reguły dotyczące zakresu i sposobu stosowania danego środka związanego z przechowywaniem danych [46];

– muszą ustanowić „obiektywne kryteria określające związek między danymi, które mają być zatrzymywane, a realizowanym celem” [47]; oraz

– muszą „opierać się na obiektywnych elementach umożliwiających namierzenie osób, których dane mogą mieć związek, nawet pośredni, z poważną przestępczością, przyczyniać się w taki lub inny sposób do walki z ową przestępczością lub też zapobiegać powstawaniu poważnych zagrożeń dla bezpieczeństwa publicznego” [48].

51. W odniesieniu do tych obiektywnych elementów Trybunał podaje przykładowo możliwość zastosowania kryterium geograficznego w celu ograniczenia środka do kategorii ewentualnie objętych nim osób i sytuacji. Powołanie się na to kryterium, do którego niektóre państwa członkowskie odniosły się krytycznie, moim zdaniem nie ma na celu ograniczenia wyliczenia dopuszczalnych czynników dotyczących indywidualnego przetwarzania tylko do owego kryterium.

43 Ibidem, pkt 106.

44 Ibidem, pkt 107.

45 Ibidem, pkt 108. Wyróżnienie moje.

46 Ibidem, pkt 108. W szczególności państwa członkowskie powinny wskazywać „okoliczności i warunki, w których środek związany z zatrzymywaniem danych może zostać zastosowany tytułem prewencji, co pozwoli zagwarantować, by środek ów ograniczał się do tego, co jest absolutnie konieczne”.

47 Ibidem, pkt 110.

48 Ibidem, pkt 111.

4. Proporcjonalność dostępu do danych

a) Wyrok Tele2 Sverige i Watson

52. Trybunał rozpatruje *dostęp* organów krajowych do danych niezależnie od zakresu obowiązku *zatrzymywania* nałożonego na dostawców usług łączności elektronicznej, w szczególności niezależnie od uogólnionego lub indywidualnego charakteru przechowywania takich danych [49].

53. Choć bowiem logika zatrzymywania polega na ułatwieniu późniejszego uzyskania dostępu do danych, zarówno to zatrzymywanie, jak i uzyskiwanie dostępu mogą prowadzić do różnych naruszeń chronionych kartą praw podstawowych. Wprowadzenie tego rozróżnienia nie oznacza jednak, że niektóre uwagi dotyczące zatrzymywania danych nie mają również zastosowania do dostępu do przechowywanych danych.

54. Zgodnie z powyższym dostęp:

– „[…] powinien rzeczywiście odpowiadać wyłącznie jednemu z tych celów" określonych w art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58; realizowany cel powinien być także powiązany z wagą ingerencji. Jeżeli ingerencja jest uznawana za poważną, może być ona uzasadniona jedynie walką z poważną przestępczością [50];

– może być dozwolony tylko w zakresie, w jakim jest to absolutnie konieczne [51]; środki ustawodawcze powinny ustanawiać „jasne i dokładne reguły określające, w jakich okolicznościach i pod jakimi warunkami dostawcy usług łączności elektronicznej powinni udzielać właściwym organom władz krajowym dostępu do tych danych; ponadto tego rodzaju środek musi być prawnie wiążący w prawie krajowym" [52];

– w szczególności uregulowania krajowe powinny ustanawiać „materialne i proceduralne warunki regulujące dostęp odpowiednich organów władz krajowych do przechowywanych danych" [53].

55. Z powyższego można wywnioskować, iż „powszechny dostęp do zatrzymanych danych, niezależnie od jakiegokolwiek związku, nawet pośredniego, z realizowanym celem, nie może być uważany za ograniczony do tego, co absolutnie konieczne" [54].

56. Zdaniem Trybunału „rozpatrywane przepisy krajowe winny opierać się na obiektywnych kryteriach umożliwiających określenie okoliczności i warunków przyznania dostępu właściwym organom władz krajowych do danych abonentów lub zarejestrowanych użytkowników" [55]. W tym względzie, „biorąc pod uwagę cel polegający na zwalczaniu poważnej przestępczości, dostęp ten może co do zasady zostać przyznany jedynie w *odniesieniu do danych dotyczących osób podejrzewanych o planowanie, popełnianie czy też popełnienie już poważnego przestępstwa bądź też zaangażowanych w taki czy inny sposób w takie przestępstwo*" [56].

49 Ibidem, pkt 113.

50 Ibidem, pkt 115.

51 Ibidem, pkt 116.

52 Ibidem, pkt 117.

53 Ibidem, pkt 118.

54 Ibidem, pkt 119.

55 Idem.

56 Idem. Wyróżnienie własne.

57. Innymi słowy, przepisy krajowe, które zapewniają właściwym organom krajowym dostęp do zatrzymywanych danych, muszą mieć wystarczająco ograniczony zakres. Musi istnieć związek między osobami, których te dane dotyczą, a realizowanym celem tak, aby dostęp nie był udzielany w odniesieniu do znacznej liczby osób lub nawet wszystkich z nich, wszystkich środków łączności elektronicznej i wszystkich zatrzymywanych danych.

58. Zasady te mogą jednak zostać złagodzone w pewnych okolicznościach. Trybunał odnosi się do „szczególnych sytuacj[i], takich jak te, w których istotne interesy związane z bezpieczeństwem narodowym, obroną czy też bezpieczeństwem publicznym są zagrożone wskutek działań terrorystycznych". W takich sytuacjach „dostęp do danych dotyczących innych osób może zostać przyznany również wówczas, gdy istnieją obiektywne elementy pozwalające uznać, że dane te mogłyby w konkretnym przypadku rzeczywiście przyczynić się do zwalczania takich działań" [57].

59. To udzielone przez Trybunał wyjaśnienie umożliwia państwom członkowskim ustanowienie szerzej zakrojonego szczególnego systemu udzielania dostępu do danych wtedy, gdy jest to wyjątkowo konieczne do realizacji celu polegającego na walce z zagrożeniami dla nadrzędnych interesów państwa (bezpieczeństwo narodowe, obronność i bezpieczeństwo publiczne) [58], tak aby objąć nim nawet osoby pośrednio związane z takimi zagrożeniami.

60. Do tego, aby móc udzielić organom krajowym dostępu do zatrzymywanych danych, konieczne jest, niezależnie od rodzaju tych danych, spełnienie trzech warunków:

– musi być „co do zasady, z wyjątkiem należycie uzasadnionych pilnych przypadków, uzależniony od uprzedniej kontroli sądu lub niezależnego organu administracyjnego"; decyzja tego sądu lub organu musi zostać podjęta „na uzasadniony wniosek owych organów, złożony w szczególności w ramach postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw" [59];

– „[…] właściwe organy władz krajowych, którym przyznano dostęp do przechowywanych danych, informowały o tym zainteresowane osoby w trybie właściwego postępowania krajowego, [jeśli tylko] informacja taka nie będzie mogła narazić na szwank prowadzonych przez te organy postępowań dochodzeniowo-śledczych" [60];

– państwa członkowskie powinny przyjąć przepisy dotyczące bezpieczeństwa i ochrony danych będących w posiadaniu dostawców usług łączności w celu zapobieżenia niedozwolonemu użyciu i bezprawnemu dostępowi do danych [61].

b) Wyrok Ministerio Fiscal

61. W sprawie tej rozpatrywano, czy przepis krajowy, przewidujący dostęp właściwych organów do danych dotyczących tożsamości cywilnej posiadaczy niektórych kart SIM, jest zgodny z art. 15 ust. 1 dyrektywy 2002/58, interpretowanym w świetle art. 7 i 8 karty.

57 Idem.

58 Oprócz działań terrorystycznych ten wyjątkowy charakter mogłyby uzasadniać inne nieprzewidziane okoliczności, takie jak zakrojony na dużą skalę atak komputerowy na mającą krytyczne znaczenie infrastrukturę państwa lub zagrożenie związane z rozprzestrzenianiem broni jądrowej.

59 Wyrok Tele2 Sverige i Watson, pkt 120.

60 Ibidem, pkt 121.

61 Ibidem, pkt 122.

62. Trybunał orzekł, że art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 nie ogranicza celu polegającego na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu przestępstw wyłącznie do zwalczania poważnych przestępstw, lecz odnosi się ogólnie do „przestępstw kryminalnych” [62].

63. Trybunał dodał, że, aby uzasadnić uzyskanie dostępu do danych przez właściwe organy krajowe, waga ingerencji musi być powiązana z wagą danych przestępstw. W związku z tym:

– „[…] poważna ingerencja może […] być uzasadniona […] jedynie przez cel polegający na zwalczaniu przestępczości, którą można uznać za »poważną«” [63];

– „[j]eżeli natomiast ingerencja wynikająca z takiego dostępu nie jest poważna, to może być uzasadniona przez cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu ogółu »przestępstw kryminalnych«” [64].

64. Wychodząc z tego założenia i w odróżnieniu od wyroku Tele2 Sverige i Watson, Trybunał nie uznał za „poważną” ingerencji w prawa chronione na mocy art. 7 i 8 karty, ponieważ wniosek o udzielenie dostępu miał „na celu jedynie identyfikację posiadaczy kart SIM działających, w okresie dwunastu dni, z numerem IMEI skradzionego telefonu komórkowego” [65].

65. Aby podkreślić mniejszą wagę ingerencji, Trybunał wyjaśnił, iż „dane objęte wnioskiem o udzielenie dostępu rozpatrywanym w postępowaniu głównym pozwalają jedynie powiązać, w danym okresie, kartę lub karty SIM działające w skradzionym telefonie komórkowym z tożsamością cywilną posiadaczy owych kart SIM. Bez badania krzyżowego z danymi dotyczącymi komunikatów przekazanych przy użyciu wspomnianych kart SIM i z danymi dotyczącymi lokalizacji, dane te nie umożliwiają poznania ani daty, godziny, czasu trwania i odbiorców komunikatów przekazanych przy użyciu przedmiotowej karty lub przedmiotowych kart SIM, ani miejsc, w których łączność miała miejsce, lub częstotliwość komunikowania się z określonymi osobami w danym okresie. Rzeczone dane te nie pozwalają zatem na wyciągnięcie konkretnych wniosków dotyczących prywatnego życia osób, o których dane chodzi” [66].

66. Przedmiotem sprawy rozstrzygniętej wyrokiem Ministerio Fiscal nie było to, czy dane osobowe, których dotyczył wniosek o udzielenie dostępu, były zatrzymywane przez dostawców łączności elektronicznej zgodnie z przesłankami określonymi w art. 15 ust. 1 dyrektywy 2002/58, interpretowanymi w świetle art. 7 i 8 karty [67]. Nie była w niej także rozpatrywana kwestia, czy spełnione zostały inne wynikające ze wspomnianego artykułu warunki, których spełnienie jest niezbędne do udzielenia dostępu.

67. W związku z tym na podstawie wyroku Ministerio Fiscal nie można wyciągnąć wniosku o tym, że doszło do jakiejkolwiek zmiany w orzecznictwie Trybunału dotyczącym niezgodności z prawem Unii systemu krajowego, który zezwala na uogólnione i niezróżnicowane zatrzymywanie danych w rozumieniu wyroku Tele2 Sverige i Watson.

62 Wyrok Ministerio Fiscal, pkt 53.

63 Ibidem, pkt 56.

64 Ibidem, pkt 57.

65 Ibidem, pkt 59. Wniosek dotyczył dostępu „do numerów telefonu odpowiadających tym kartom SIM, a także do danych dotyczących tożsamości cywilnej posiadaczy owych kart, takich jak nazwisko, imię, oraz, w stosownych przypadkach, adres. Natomiast dane te nie dotyczą, jak potwierdziły na rozprawie zarówno rząd hiszpański, jak i prokuratura, komunikatów przekazanych przy użyciu skradzionego telefonu komórkowego ani jego lokalizacji”.

66 Ibidem, pkt 60.

67 Wyrok Ministerio Fiscal, pkt 49.

68. Uważam jednak, że, potwierdzając ważność obowiązywania systemu dostępu ograniczonego do niektórych danych osobowych (dotyczących tożsamości cywilnej posiadaczy kart SIM), Trybunał uznaje w sposób dorozumiany zatrzymywanie tych samych danych przez dostawców usługi.

C. Główne zarzuty dotyczące orzecznictwa Trybunału

69. Zarówno sąd odsyłający, jak i większość państw członkowskich, które przedstawiły uwagi, zwracają się do Trybunału o wyjaśnienie, uzupełnienie lub nawet ponowne rozważenie różnych aspektów jego orzecznictwa w tej dziedzinie, którego dotyczą ich zarzuty.

70. Większość tych zarzutów, dorozumianych lub wyraźnych, została już podniesiona w ramach wyroku Digital Rights i odrzucona w wyroku Tele2 Sverige i Watson. Zostały one ponownie podniesione w niniejszej sprawie, co świadczy w istocie o tym, że wystarczyłoby ustalenie rygorystycznych zasad dotyczących udzielania dostępu do danych będących w posiadaniu dostawców usług łączności elektronicznej, które mogłyby w pewien sposób zrównoważyć wagę ingerencji, jaką stanowi uogólnione i niezróżnicowane zatrzymywanie tych samych danych.

71. W niektórych z tych zarzutów podkreślono również konieczność podjęcia naprawdę skutecznych środków w walce z poważnymi zagrożeniami dla bezpieczeństwa i, ogólnie rzecz biorąc, z przestępczością oraz zwrócono się do Trybunału o wzięcie pod uwagę prawa do bezpieczeństwa osobistego (art. 6 karty), a także swobodnego uznania przysługującego państwom członkowskich w ramach realizacji celu polegającego na ochronie bezpieczeństwa narodowego. W każdym razie dodać należy, że Trybunał nie rozważył prewencyjnego charakteru interwencji służb bezpieczeństwa i służb wywiadowczych.

D. Moja ocena wspomnianych zarzutów, a także tego, jak można by doprecyzować orzecznictwo Trybunału

72. W mojej ocenie Trybunał powinien utrzymać zasadnicze stanowisko, jakie zajął w swoich poprzednich wyrokach: uogólniony i niezróżnicowany obowiązek zatrzymywania wszystkich danych dotyczących ruchu i lokalizacji wszystkich abonentów i zarejestrowanych użytkowników w nieproporcjonalny sposób narusza prawa podstawowe chronione na mocy art. 7, 8 i 11 karty.

73. *A contrario*, uregulowanie krajowe ustanawiające odpowiednie ograniczenia dotyczące zatrzymywania niektórych z owych danych generowanych w kontekście świadczenia usług łączności elektronicznej, mogłoby być zgodne z prawem Unii. Sedno tkwi zatem w *ograniczonym zatrzymywaniu* tych danych.

74. Jak wyjaśnię poniżej, takie ograniczone zatrzymywanie nie powinno dotyczyć tylko określonego obszaru geograficznego lub kategorii konkretnych osób: wyniki dyskusji prowadzonych na temat takich kryteriów zatrzymywania świadczą o tym, że owe kryteria mogłyby być niewykonalne lub nieskuteczne w odniesieniu do realizowanych celów, a nawet mogłyby stać się źródłem dyskryminacji.

75. Nie podzielam przede wszystkim argumentacji krytycznej opowiadającej się za przyjęciem „szerszego zakresu zatrzymywania w zamian za bardziej ograniczony dostęp”. Rozumowanie Trybunału, z którym się zgadzam, jest takie, że zatrzymywanie danych i uzyskiwanie do nich dostępu stanowią dwa różne rodzaje ingerencji. Nawet jeśli zatrzymywanie danych ma sens

w perspektywie ewentualnego późniejszego udzielania do nich dostępu przez właściwe organy, każda taka ingerencja powinna być uzasadniona oddzielnie, w ramach szczegółowego badania przeprowadzanego w świetle zamierzonego celu.

76. W związku z tym krajowy system przewidujący uogólnione i niezróżnicowane zatrzymywanie danych nie może być uzasadniony na tej podstawie, że odpowiednie normy ustanawiają jednocześnie rygorystyczne materialne i proceduralne przesłanki, których spełnienie jest wymagane do uzyskania dostępu do takich danych.

77. Muszą zatem istnieć zasady konkretnie związane z zatrzymywaniem danych, które uzależniają je od spełnienia pewnych warunków po to, aby zapobiec dokonywania tego zatrzymywania w uogólniony i niezróżnicowany sposób. Tylko w ten sposób można zapewnić, że będzie ono zgodne z art. 15 ust. 1 dyrektywy 2002/58 w świetle art. 7, 8, 11 i art. 52 ust. 1 karty.

78. Jest to ponadto podejście przyjęte przez grupy robocze zebrane w Radzie w celu określenia zasad zatrzymywania i udzielania dostępu zgodnych z orzecznictwem Trybunału, które jednocześnie badały oba te rodzaje ingerencji [68].

79. Poprzez zastosowanie ograniczeń w odniesieniu do każdego z tych dwóch rodzajów ingerencji będzie można ocenić, czy ich ewentualny łączny skutek, w połączeniu z silnymi zabezpieczeniami, jest tego rodzaju, że łagodzi on wpływ, jaki ma zatrzymywanie danych na prawa podstawowe chronione na mocy art. 7, 8 i 11 karty, przy jednoczesnym zapewnieniu skuteczności dochodzeń.

80. Aby chronić wspomniane prawa, system ten musi:

– przewidywać takie zatrzymywanie danych, które, w zależności od zamierzonego celu, podlega pewnym ograniczeniom i zróżnicowaniom;

– regulować udzielanie dostępu do takich danych tylko w zakresie ściśle niezbędnym do zamierzonego celu i pod kontrolą sądu lub niezależnego organu administracyjnego.

81. Uzasadnienie spoczywającego na dostawcach usług łączności elektronicznej obowiązku zatrzymywania niektórych danych, nie tylko w celu zarządzania ich zobowiązaniami umownymi wobec użytkowników, jest rozszerzane wraz z postępem technologicznym. Jeśli przyznamy, że takie zatrzymywanie jest przydatne do zapobiegania i zwalczania przestępczości (które to twierdzenie trudno jest obalić [69]), nie wydaje się logiczne ograniczenie jego zakresu do samego tylko wykorzystywania tych danych, które operatorzy zatrzymują w celu prowadzenia działalności gospodarczej i tylko przez okres niezbędny do prowadzenia takiej działalności.

82. Jeśli stwierdzimy użyteczność obowiązku zatrzymywania danych z punktu widzenia celu polegającego na ochronie bezpieczeństwa narodowego i zwalczaniu przestępczości, wychodzącego poza te, w którym operatorzy mogą dokonywać ich zatrzymywania dla swoich potrzeb technicznych i handlowych, konieczne jest określenie granic tego obowiązku.

[68] Od 2017 r. państwa członkowskie uczestniczą w grupie roboczej, której celem jest dostosowanie ich ustawodawstw do kryteriów określonych w orzecznictwie Trybunału w tej dziedzinie [Groupe Échange d'informations et protection des données (DAPIX)].

[69] W każdym razie określenie tych technik i ocena ich skuteczności wchodzą w zakres przysługującego państwom członkowskim swobodnego uznania.

83. Każdy system zatrzymywania musi być ściśle dostosowany do zamierzonego celu w taki sposób, aby nie było możliwości przekształcenia go w niezróżnicowane zatrzymywanie [70]. Należy również wykluczyć, że suma tych danych stanowi *obraz* osoby, której dane dotyczą (to znaczy jej zwykłych czynności i relacji społecznych), zbliżony lub podobny do tego, który zostałby uzyskany dzięki znajomości treści komunikatów.

84. Z punktu widzenia wyjaśnienia niektórych niejednoznaczności i nieporozumień istotne jest uwzględnienie tego, co Trybunał *nie stwierdził* w jego wyrokach Digital Rights oraz Tele2 Sverige i Watson. W wyrokach tych nie zakwestionowano jako takiego istnienia systemu zatrzymywania danych jako użytecznego narzędzia do walki z przestępczością. Przeciwnie, uznano zasadność celu polegającego na zapobieganiu przestępstwom i ich zwalczaniu, a także przydatność systemu przechowywania danych do osiągnięcia tego celu.

85. Natomiast – co pragnę podkreślić – w owych wyrokach odrzucono stanowczo twierdzenie, zgodnie z którym Unia lub jej państwa członkowskie mogą, powołując się na rzeczony cel, nałożyć obowiązek niezróżnicowanego zatrzymywania *wszystkich* danych generowanych w ramach świadczenia usług łączności elektronicznej oraz ogólnego dostępu do takich danych.

86. W związku z tym konieczne jest określenie takich form zatrzymywania danych, których nie można będzie zakwalifikować („uogólnione i niezróżnicowane") jako niezgodnych z ochroną wymaganą na mocy art. 7, 8 i 11 karty.

87. Jedną z tych form byłoby *indywidualne* zatrzymywanie danych odnoszących się albo do konkretnych osób (teoretycznie do tych, które są w pewien sposób, mniej lub bardziej bezpośredni, powiązane z najpoważniejszymi zagrożeniami), albo do określonego obszaru geograficznego.

88. Przyjęcie takiego podejścia wiąże się jednak z pewnymi trudnościami:

– identyfikacja grupy potencjalnych sprawców byłaby prawdopodobnie niewystarczająca w przypadku, gdy wykorzystują oni techniki anonimizacji lub wprowadzają w błąd co do ich tożsamości; dokonanie wyboru tych grup mogłoby również doprowadzić do ustanowienia ogólnego systemu podejrzeń dotyczących niektórych segmentów ludności i zostać uznane za dyskryminujące, w zależności od zastosowanego algorytmu;

– dokonanie wyboru według kryteriów geograficznych (które, aby było skuteczne, wymagałoby ograniczenia do dość dużych obszarów) wiąże się z tymi samymi problemami i prowadzi do, jak wskazał na rozprawie Europejski Inspektor Ochrony Danych, powstania kolejnych, ponieważ mogłoby ono postawić niektóre obszary w mniej korzystnej sytuacji.

89. Ponadto mogłaby istnieć pewna sprzeczność między prewencyjnym charakterem zatrzymywania ukierunkowanego na określone osoby lub na dany obszar geograficzny a okolicznością polegającą na tym, że sprawcy przestępstw nie są uprzednio znani, podobnie jak miejsce i czas ich popełnienia.

[70] Wyroki: Digital Rights, pkt 57; Tele2 Sverige i Watson, pkt 105.

90. W każdym razie nie można wykluczyć, że zostaną określone sposoby indywidualnego zatrzymywania oparte na wspomnianych kryteriach, które będą przydatne do osiągnięcia przedstawionych już celów. Opracowanie owych sposobów należy do uprawnień ustawodawczych każdego państwa członkowskiego lub całej Unii, z poszanowaniem ochrony praw podstawowych gwarantowanych przez Trybunał.

91. Błędem byłoby twierdzić, że indywidualne zatrzymywanie danych należących do określonego kręgu osób lub obszaru geograficznego jest jego jedynym sposobem, jaki Trybunał uznaje za zgodny z art. 15 ust. 1 dyrektywy 2002/58, interpretowanym w świetle art. 7 i 8 karty.

92. Pragnę podkreślić, że możliwe jest określenie sposobów indywidualnego zatrzymywania danych innych niż te skoncentrowanych na określonych grupach osób czy też na obszarach geograficznych. W rzeczywistości zostało to tak zrozumiane przez grupy robocze Rady, o których była mowa powyżej: rozważały one w szczególności, jako potencjalną metodę do wykorzystywania, ograniczenie kategorii zatrzymywanych danych [71]; pseudonimizację danych [72]; wprowadzenie ograniczonych okresów przechowywania [73]; wyłączenie niektórych kategorii dostawców usług łączności elektronicznej [74]; odnawialne zezwolenia na zatrzymywanie danych [75]; obowiązek przechowywania zatrzymywanych danych na terytorium Unii lub przeprowadzana systematyczna i regularna przez niezależny organ administracji kontrola gwarancji oferowanych przez dostawców usług łączności elektronicznej, zabezpieczających przed niedozwolonym wykorzystaniem danych.

93. Moim zdaniem, aby zachować zgodność z orzecznictwem Trybunału, należałoby przyznać pierwszeństwo tymczasowemu zatrzymywaniu niektórych *kategorii* danych dotyczących ruchu i lokalizacji, ograniczonych w zależności od ściśle określonych potrzeb w zakresie bezpieczeństwa, które nie umożliwiałyby, w swym całokształcie, uzyskania dokładnego i szczegółowego obrazu życia osób, których dane dotyczą.

94. W praktyce oznacza to, że, w przypadku dwóch głównych kategorii (dane dotyczące ruchu i dane dotyczące lokalizacji) zatrzymywane za pomocą odpowiednich filtrów powinny być jedynie *minimalne* dane uważane za absolutnie niezbędne dla skutecznego zapobiegania i kontroli przestępczości oraz w celu ochrony bezpieczeństwa narodowego.

71 Z obowiązku zatrzymywania byłyby wyłączone, które nie są ściśle niezbędne i obiektywnie konieczne do zapobiegania przestępstwom i ich ścigania oraz do ochrony bezpieczeństwa publicznego. W szczególności należałoby wskazać, w świetle zamierzonego celu, jakie rodzaje danych: tych dotyczących abonentów, ruchu i lokalizacji musiałyby być bezwzględnie zatrzymywane, aby go osiągnąć. W szczególności z obowiązku tego wyłączone byłyby te dane, które nie są uważane za niezbędne do prowadzenia dochodzenia i ścigania przestępstw.

72 Metoda zastępowania nazwisk pseudonimami, dzięki czemu dane nie są już powiązane z określonym nazwiskiem. W odróżnieniu od anonimizacji pseudonimizacja pozwala na ponowne powiązanie danych z nazwiskiem osoby, której dane dotyczą.

73 Można by rozważyć możliwość dostosowania okresów zatrzymywania w zależności od różnych kategorii danych, w zależności od ich mniej lub bardziej ingerującego w prywatne życie ludzi charakter. Ponadto należałoby ustanowić wymóg, że po upływie okresu zatrzymywania dane są trwale usuwane.

74 Można by rozważyć możliwość nienakładania obowiązku zatrzymywania danych na wszystkich dostawców usług łączności elektronicznej, lecz wprowadzenia tego obowiązku w zależności od ich wielkości i rodzaju oferowanych przez nich usług, z wyłączeniem na przykład tych, którzy oferują usługi wysoce wyspecjalizowane.

75 Systemy zezwoleń mogłyby się opierać na okresowych ocenach zagrożeń w każdym państwie członkowskim. Należy zapewnić, aby związek między zatrzymywanymi danymi a realizowanym celem powstawał i był dostosowywany do konkretnej sytuacji każdego państwa członkowskiego. W związku z tym możliwe byłoby, że zezwolenia na zatrzymywanie wydane dostawcom mogłyby doprowadzić do zatrzymywania niektórych rodzajów danych przez określony czas, w zależności od oceny zagrożenia. Te wydawane przez sąd lub niezależny organ administracyjny zezwolenia mogłyby by podstawę przeprowadzanej okresowo kontroli tego, czy to zatrzymywanie jest niezbędne.

95. To do państw członkowskich lub instytucji Unii należy dokonanie tego wyboru w drodze ustawodawczej (z pomocą ich własnych ekspertów), przy jednoczesnej rezygnacji z wszelkich prób narzucenia uogólnionego i niezróżnicowanego przechowywania wszystkich danych dotyczących ruchu i lokalizacji.

96. Oprócz tego ograniczenia ze względu na kategorię zatrzymane dane mogą być przechowywane tylko przez pewien okres, aby nie pozwalały na uzyskanie szczegółowego obrazu życia osób, których dane dotyczą. Ów okres zatrzymywania powinien ponadto być dostosowany do charakteru danych, tak aby dane dostarczające dokładniejszych informacji na temat stylu życia i nawyków tych osób były przechowywane przez krótszy okres [76].

97. Innymi słowy, należy zbadać kwestię zróżnicowania okresu przechowywania każdej kategorii danych, w zależności od ich przydatności do osiągnięcia celów w zakresie bezpieczeństwa. Poprzez określenie czasu, przez jaki różnego rodzaju kategorie danych są przechowywane jednocześnie (a zatem mogą być wykorzystane do stwierdzenia powiązań ujawniających styl życia osób, których dane dotyczą), zostaje rozszerzona ochrona prawa zagwarantowanego w art. 8 karty.

98. Takie też było stanowisko przedstawione przez Europejskiego Inspektora Ochrony Danych na rozprawie: im więcej kategorii metadanych jest przechowywanych i im dłuższy jest okres przechowywania, tym łatwiej będzie zdefiniować szczegółowy profil danej osoby i odwrotnie [77].

99. Ponadto, jak to zostało również podniesione na rozprawie, trudno jest wyznaczyć granicę między określonymi metadanymi połączeń elektronicznych a treścią tych połączeń. Niektóre metadane mogą ujawniać tyle samo lub więcej informacji niż treść tych połączeń: mogłoby się tak zdarzyć w przypadku adresów (URL) odwiedzanych stron internetowych [78]. Na tego rodzaju dane i podobne dane należałoby zatem zwrócić szczególną uwagę, maksymalnie ograniczając konieczność ich zatrzymywania i jego okres.

100. Znalezienie zrównoważonego rozwiązania nie jest łatwe, ponieważ technika krzyżowania i korelowania zatrzymywanych danych pozwala służbom dochodzeniowym i służbom nadzoru na identyfikację podejrzanego lub zagrożenia, w zależności od przypadku. Niemniej jednak istnieje różnica w stopniu natężenia między zatrzymywaniem danych w celu wykrycia wspomnianego podejrzanego lub zagrożenia a takim ich zatrzymywaniem, którego skutkiem jest przedstawienie szczegółowego obrazu życia danej osoby.

101. Do czasu przyjęcia wspólnego dla całej Unii uregulowania w tej konkretnej dziedzinie nie sądzę, aby możliwe było zwrócenie się do Trybunału o przejęcie funkcji regulacyjnych i szczegółowe określenie tego, jakie kategorie danych mogą być zatrzymywane i przez jaki czas. Po określeniu granic, które zdaniem Trybunału wynikają z karty, zadaniem instytucji Unii i państw członkowskich jest „umieszczenie kursora we właściwym miejscu" w celu znalezienia punktu równowagi między zachowaniem bezpieczeństwa a chronionymi na mocy karty prawami podstawowymi.

[76] Wydaje się, że jest to system stosowany w Republice Federalnej Niemiec, której rząd wskazał na rozprawie, iż zgodnie z jego ustawodawstwem okres przechowywania danych dotyczących ruchu wynosi dziesięć tygodni, a okres zatrzymywania danych dotyczących lokalizacji wynosi tylko cztery tygodnie. W przypadku Republiki Francuskiej w przypadku zatrzymywania danych dotyczących ruchu i lokalizacji wymagany jest okres jednego roku. Zdaniem tego państwa członkowskiego skrócenie wspomnianego okresu do mniej niż jednego roku doprowadziłoby do zmniejszenia skuteczności służb policji sądowej.

[77] Oczywiście należy zagwarantować, że dostawcy usług łączności elektronicznej po upływie okresu zatrzymywania trwale usuną dane (z wyjątkiem tych, które mogą oni nadal przechowywać w celach handlowych, zgodnie z dyrektywą 2002/58).

[78] Na rozprawie rząd francuski stwierdził, że adresy URL zostały wyłączone z danych dotyczących połączeń, w odniesieniu do których jego ustawodawstwo przewiduje ogólny obowiązek zatrzymywania.

102. Z pewnością rezygnacja z informacji wynikających z większej liczby przechowywanych danych mogłaby w niektórych przypadkach utrudnić walkę z potencjalnymi zagrożeniami. Jest to jednak jeden z kosztów, jakie władze publiczne muszą ponieść, gdy biorą na siebie obowiązek ochrony praw podstawowych.

103. Tak samo jak nikt nie opowiedziałby się za wprowadzeniem uogólnionego i niezróżnicowanego obowiązku *ex ante* zatrzymywania *treści* prywatnych komunikatów elektronicznych (nawet jeśli prawo gwarantowałoby późniejszy ograniczony dostęp do wspomnianych treści), metadane takich komunikatów, które mogą odzwierciedlać informacje tak samo wrażliwe jak ich treści, również nie powinny podlegać niezróżnicowanemu i uogólnionemu zatrzymywaniu.

104. Trudność legislacyjna – co przyznaję – polegająca na dokładnym określeniu przesłanek i warunków, na jakich można dokonać indywidualnego zatrzymywania, nie uzasadnia uznania przez państwa członkowskie, w drodze przyjęcia wyjątku za regułę, uogólnionego zatrzymywania danych osobowych za podstawową zasadę ich ustawodawstw. W takim przypadku doszłoby do bezterminowego istotnego naruszenia prawa do ochrony danych osobowych.

105. Należy dodać, że nic nie stoi na przeszkodzie temu, by w rzeczywiście *wyjątkowych* sytuacjach, charakteryzujących się nieuchronnym 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 przechowywania danych, jaki zostanie uznany za niezbędny.

106. W tym kontekście można by przyjąć uregulowanie, które wyraźnie umożliwia zatrzymywanie danych (i uzyskiwanie dostępu do nich) w szerszym zakresie, zgodnie z przesłankami i procedurami, które zapewniają tym środkom nadzwyczajny – pod względem ich przedmiotowego i czasowego zakresu stosowana charakter – jak również odpowiednie gwarancje sądowe.

107. Analiza porównawcza systemów normatywnych regulujących przewidziane w konstytucjach stany wyjątkowe wskazuje na to, że nie jest niemożliwe sformułowanie takich przesłanek faktycznych, które mogłyby doprowadzić do zastosowania szczególnego systemu normatywnego, określając, jaki organ może podjąć tę decyzję, na jakich warunkach i pod czyim nadzorem [79].

E. Szczegółowe odpowiedzi na trzy pytania prejudycjalne

1. Uwagi wstępne

108. Sąd odsyłający wnosi o dokonanie wykładni art. 15 ust. 1 dyrektywy 2002/58 w odniesieniu do różnego rodzaju praw zagwarantowanych w karcie: prawa do poszanowania życia prywatnego i rodzinnego (art. 7), prawa do ochrony danych osobowych (art. 8) oraz prawa do wolności wypowiedzi i informacji (art. 11).

109. Jak stwierdziłem w opinii w sprawach połączonych C-511/18 i C-512/18, są to prawa, które zdaniem Trybunału mogą się okazać naruszone w tych przypadkach.

[79] B. Ackerman, „The Emergency Constitution”, *Yale Law Journal*, vol. 113, 2004, s. 1029–1092; J. Ferejohn i P. Pasquino, „The Law of the Exception: A typology of Emergency Powers”, *International Journal of Constitutional Law*, vol. 2, 2004, s. 210–239.

110. Jednakże Cour constitutionnelle powołuje się również na art. 4 i 6 karty, których dotyczą odpowiednio drugie i pierwsze pytanie prejudycjalne.

111. Jeśli chodzi o art. 6 karty, który gwarantuje prawo do wolności i bezpieczeństwa osobistego, powołano się na niego również w sprawach połączonych C-511/18 i C-512/18, a co do jego znaczenia wypowiedziałem się w mojej opinii do tych spraw, do której odsyłam [80].

112. Jeśli chodzi o art. 4 karty, ze względu na to, że odpowiedź, jakiej należy udzielić, nie zależy w dużym stopniu od analizy ustawodawstwa krajowego, w celu porównania go z prawem Unii, lecz raczej od interpretacji tego przepisu, wydaje mi się, że na to pytanie należy odpowiedzieć w pierwszej kolejności.

2. W przedmiocie drugiego pytania prejudycjalnego

113. Odniesienie do zakazu tortur i nieludzkiego lub poniżającego traktowania albo karania, zagwarantowanego w art. 4 karty, w rzeczywistości dotyczy wyłącznie tego odesłania prejudycjalnego, wobec czego jestem zmuszony zwrócić na niego uwagę.

114. Powołując się na art. 4 karty, sąd odsyłający pragnie podkreślić, że przepis krajowy ma również na celu wywiązanie się z nałożonego na władzę publiczną *pozytywnego obowiązku* polegającego na ustanowieniu „ram prawnych, które umożliwiają skuteczne prowadzenie dochodzenia w sprawach karnych oraz skuteczne zwalczanie wykorzystywania seksualnego małoletnich, a także skuteczne zidentyfikowanie sprawcy czynu karalnego nawet w przypadku korzystania ze środków łączności elektronicznej” [81].

115. Moim zdaniem ten konkretny *pozytywny obowiązek* nie różni się znacząco od poszczególnych obowiązków, z jakimi wiąże się dla państwa przyjęcie katalogu praw podstawowych. Prawo do życia (art. 2 karty), prawo do integralności fizycznej (art. 3 karty) lub prawo do ochrony danych (art. 8 karty), a także wolność wypowiedzi (art. 11 karty) lub wolność myśli, sumienia i religii (art. 10 karty) nakładają na państwo obowiązek ustanowienia ram prawnych, w których zagwarantowane jest skuteczne korzystanie z owych praw, w razie potrzeby poprzez użycie zmonopolizowanego przez władzę publiczną przymusu wobec każdego, kto próbuje to uniemożliwić lub utrudnić [82].

116. W odniesieniu do wykorzystywania seksualnego małoletnich ETPC uznaje, że dzieci i inne osoby wymagające szczególnego traktowania mają kwalifikowane prawo do ochrony ze strony państwa, polegające na przyjęciu przepisów prawa karnego, które skutecznie i odstraszająco sankcjonują popełnianie takich przestępstw [83].

117. To kwalifikowane prawo do ochrony zostało ustanowione nie tylko w art. 4 karty, gdyż można by oczywiście powołać się na art. 1 (godność człowieka) lub art. 3 (prawo do integralności fizycznej i psychicznej).

80 Opinia w sprawach C-511/18 i C-512/18, pkt 95 i nast.

81 Pytanie drugie, *in fine*. To odniesienie do środków łączności elektronicznej wyjaśnia, że pytanie odnosi się do drugiego *pozytywnego obowiązku*, który spoczywa na państwach i został ustanowiony w art. 8 karty dotyczącym ochrony danych osobowych. Dwukrotne odniesienie do art. 8 karty świadczy o tym, że sąd odsyłający przypisuje dwa cele ustanowionym w karcie prawom, w zależności od ich charakteru: *ograniczenie* spornego obowiązku i *uzasadnienie* tego obowiązku.

82 Ten obowiązek skuteczności wiąże się z przyznaniem mandatu osiągnięcia rezultatu władzy publicznej w państwie socjalnym lub opiekuńczym, w którym, poza formalnym uznaniem praw, istotna jest praktyczna realizacja ich treści materialnej.

83 Wyrok ETPC z dnia 2 grudnia 2008 r. w sprawie K.U. przeciwko Finlandii, (ECHR:2008:1202JUD000287202, § 46).

118. Chociaż spoczywający na władzach publicznych pozytywny obowiązek polegający na zapewnieniu ochrony dzieciom i innym osobom wymagającym szczególnego traktowania nie może zostać zignorowany przy ocenie dóbr prawnych zagrożonych przepisami krajowymi [84], nie może on również wiązać się z „nadmiernymi obciążeniami" dla władzy publicznej [85], ani też nie może zostać spełniony z pominięciem legalności lub poszanowania innych praw podstawowych [86].

3. W przedmiocie pierwszego pytania prejudycjalnego

119. Sąd odsyłający zmierza zasadniczo do ustalenia, czy prawo Unii sprzeciwia się prawu krajowemu, w przedmiocie którego sąd ten ma wydać orzeczenie w ramach skargi konstytucyjnej.

120. Ze względu na to, iż Trybunał przedstawił już wykładnię dyrektywy 2002/58, która jest zgodna ze związanymi z nią postanowieniami karty, w odpowiedzi na pytanie prejudycjalne należy uwzględnić orzecznictwo zawarte w wyroku Tele2 Sverige i Watson, biorąc pod uwagę niuanse charakteryzujące niniejszą sprawę.

121. W oparciu o tę przesłankę wskazówki dotyczące wykładni, które można przedstawić Cour constitutionnelle po to, aby sam dokonał oceny zgodności przepisu krajowego z prawem Unii, powinny dotyczyć zatrzymywania i dostępu do danych oddzielnie, zgodnie z ich uregulowaniem we wspomnianym przepisie krajowym.

a) Warunki zatrzymywania danych

122. Rząd belgijski podkreśla, że zamierzał ustanowić wyraźne ramy prawne, które obejmowałyby niezbędne gwarancje ochrony życia prywatnego, zamiast opierać się na praktyce operatorów usług łączności elektronicznej w zakresie zatrzymywania danych w celu fakturowania i rozpatrywania wniosków klientów o udzielenie informacji.

123. Zdaniem tego rządu ogólny i prewencyjny obowiązek zatrzymywania danych służy nie tylko dochodzeniu, wykrywaniu i ściganiu poważnych przestępstw, lecz także ochronie bezpieczeństwa narodowego, obronie terytorium i bezpieczeństwa publicznego, dochodzeniu, wykrywaniu i ściganiu czynów innych niż poważne przestępstwa lub zapobieganiu zakazanemu używaniu systemów łączności elektronicznej [87] lub wszelkim innym celom określonym w art. 23 ust. 1 rozporządzenia 2016/679.

84 W tym względzie uważam, że do praw powołanych przez sąd odsyłający (jako o*graniczenie* spornego obowiązku, a nie – jako jego *uzasadnienie*) można by dodać prawo do skutecznego środka prawnego (art. 47 karty) lub prawo do obrony (art. 48 karty), których ewentualne naruszenie również było rozpatrywane w postępowaniach głównych. Sentencja postanowienia odsyłającego odnosi się jednak tylko do art. 7, 8, 11 i art. 52 ust. 1 karty.

85 Wyrok ETPC z dnia 28 października 1998 r. w sprawie Osman przeciwko Zjednoczonemu Królestwu (CE:ECHR:1998:1028JUD002345294, § 116).

86 Ibidem, § 116 in fine: „[konieczne jest] zapewnienie, aby policja wykonywała swoje uprawnienia w zakresie zwalczania i zapobiegania przestępczości przy pełnym poszanowaniu środków prawnych i innych gwarancji, które zgodnie z prawem ograniczają zakres jej czynności dochodzeniowych w sprawach karnych". Zobacz także wyrok ETPC z dnia 2 grudnia 2008 r. w sprawie K.U. przeciwko Finlandii (CE:ECHR:2008:1202JUD000287202, § 48). Podobnie w wyroku z dnia 29 lipca 2019 r., Gambino i Hyka (C-38/18, EU:C:2019:628, pkt 49), Trybunał orzekł, że prawa przyznane ofierze przestępstwa nie mogą wpływać na możliwość skutecznego korzystania przez oskarżonego z przysługujących mu praw.

87 Jest on również uzasadniony koniecznością reagowania na wezwanie służb ratowniczych lub poszukiwania osoby zaginionej, której integralność fizyczna jest w bezpośrednim niebezpieczeństwie.

124. W ocenie rządu belgijskiego:

– zatrzymywanie danych jako takie nie pozwala na wyciągnięcie bardzo precyzyjnych wniosków na temat życia prywatnego osób, których dane dotyczą: możliwość wyciągnięcia takich wniosków byłaby możliwa tylko w zakresie, w jakim udzielono by również dostępu do zatrzymywanych danych;

– środki ostrożności mające na celu ochronę życia prywatnego zostały przewidziane w przepisach ustawowych; między innymi, zatrzymywanie danych nie wpływa na treść komunikacji; w pełni stosowane są gwarancje dotyczące uzasadnienia zatrzymywania, prawa do uzyskania dostępu, prawa do sprostowania i inne; dostawcy i operatorzy muszą objąć zatrzymywane dane tymi samymi obowiązkami oraz środkami bezpieczeństwa i ochrony, które mają zastosowanie do danych w sieci, zapobiegając ich przypadkowemu lub bezprawnemu zniszczeniu, przypadkowej utracie lub zmianie;

– dane mogą być przechowywane przez dwanaście miesięcy (po upływie tego okresu muszą zostać zniszczone) i tylko na terytorium Unii;

– dostawcy i operatorzy muszą stosować technologiczne środki ochrony, dzięki którym zatrzymywane dane zaraz po zarejestrowaniu staną się niemożliwe do odczytania i bezużyteczne dla każdej osoby, która nie jest upoważniona do uzyskania do nich dostępu.

– w każdym razie operacje te są przeprowadzane pod nadzorem belgijskiego organu regulacyjnego ds. sektorów pocztowego i telekomunikacyjnego oraz organu ochrony danych.

125. Pomimo tych gwarancji ustawodawstwo belgijskie nakłada na operatorów i dostawców usług łączności elektronicznej ogólny i niezróżnicowany obowiązek zatrzymywania danych dotyczących ruchu i lokalizacji w rozumieniu dyrektywy 2002/58, przetwarzanych w kontekście świadczenia rzeczonych usług. Jak już wspomniano, okres ich zatrzymywania wynosi co do zasady dwanaście miesięcy: nie przewiduje się żadnego ograniczenia czasowego w zależności od kategorii przechowywanych danych.

126. Ów ogólny i niezróżnicowany obowiązek zatrzymywania ma trwały i ciągły charakter. Nawet jeśli jego celem jest zapobieganie, wykrywanie i ściganie wszelkiego rodzaju przestępstw (począwszy od przestępstw przeciwko bezpieczeństwu narodowemu, obronności lub szczególnie poważnych przestępstw, aż po przestępstwa zagrożone karą pozbawienia wolności poniżej jednego roku), obowiązek taki nie jest zgodny z orzecznictwem trybunału, w związku z czym nie można uznać go za zgodny z kartą.

127. Aby dostosować się do tego orzecznictwa, ustawodawca belgijski będzie musiał rozważyć inne środki (takie jak wspomniane powyżej), które ustanawiają sposoby bardziej ograniczonego zatrzymywania. Sposoby te, zróżnicowane w zależności od kategorii danych, muszą być zgodne z zasadą, że należy przechowywać tylko niezbędne *minimum* danych, zależnie od rodzaju ryzyka czy zagrożenia, i przez ograniczony czas, zależnie od charakteru przechowywanych informacji. W każdym razie zatrzymywanie to nie może umożliwiać dokładnego *odwzorowania* życia prywatnego, nawyków, zachowań lub relacji społecznych osób, których dane dotyczą.

b) Warunki, po spełnieniu których władze publiczne mogą uzyskać do zatrzymywanych danych

128. W mojej ocenie warunki wskazane w wyroku Tele2 Sverige i Watson [88] są również istotne w odniesieniu do uzyskiwania dostępu: uregulowanie krajowe powinno określać materialne i proceduralne przesłanki regulujące uzyskiwanie przez właściwe organy dostępu do przechowywanych danych [89].

129. Rząd belgijski wyjaśnia, że art. 126 ust. 2 ustawy z 2005 r. (o łączności elektronicznej) [90] określa ściśle organy krajowe, które mogą otrzymywać dane przechowywane zgodnie ust. 1 wspomnianego artykułu.

130. Do organów tych należą organy ściśle sądownicze i prokuratura; siły bezpieczeństwa państwa; główna służba wywiadowcza i bezpieczeństwa pod kontrolą dwóch niezależnych komisji; funkcjonariusze policji sądowej belgijskiego instytutu ds. usług pocztowych i telekomunikacji; służby ratownicze; funkcjonariusze policji sądowej komórki ds. osób zaginionych policji federalnej; służba mediacji w telekomunikacji i organ nadzorujący sektor finansowy.

131. Rząd belgijski stwierdza co do zasady, że te przepisy krajowe nie dają tym różnego rodzaju służbom możliwości uzyskania dostępu do danych w celu aktywnego ścigania niezidentyfikowanych zagrożeń lub bez konkretnych wskazówek. Te organy krajowe nie mogłyby zatem po prostu uzyskać dostępu do nieprzetworzonych danych dotyczących połączeń i automatycznie przetwarzać ich w celu uzyskania informacji i aktywnego zapobiegania zagrożeniom dla bezpieczeństwa.

132. Zdaniem wspomnianego rządu do uzyskania dostępu do tych danych wymagane jest spełnienie ściśle określonych warunków, w zależności od statusu każdego z właściwych organów krajowych.

133. Moim zdaniem odpowiedź na pierwsze pytanie prejudycjalne nie wymaga przeprowadzenia przez Trybunał wyczerpującej analizy warunków, po spełnieniu których każdy z tych organów może uzyskać zatrzymywane dane. Zadanie to należy raczej do sądu odsyłającego, który będzie musiał je wykonać w świetle wskazówek wynikających z orzecznictwa Tele2 Sverige i Watson oraz Ministerio Fiscal.

88 Zobacz pkt 60 niniejszej opinii.

89 Wyrok Tele2 Sverige i Watson, pkt 118.

90 Artykuł 126, w brzmieniu ustawy z dnia 29 maja 2016 r.

134. Ponadto, zgodnie z informacjami przedstawionymi przez rząd belgijski, istnieją znaczne różnice między warunkami udzielenia dostępu, które dotyczą organów sądowych lub prokuratury [91], do celów w zakresie badania, dochodzenia i ścigania przestępstw zgodnie z art. 46 bis [92] i 88 bis [93] kodeksu postępowania karnego, a warunkami mającymi zastosowanie do innych organów.

135. Jeśli chodzi o służby wywiadowcze i bezpieczeństwa, zgodnie z ustawą z 1998 r. wniosek o udzielenie dostępu do danych dotyczących ruchu i lokalizacji będących w posiadaniu operatorów musi się opierać na obiektywnych kryteriach, a to po to, aby zapewnić, że jest on ograniczony do tego, co jest ściśle konieczne, na podstawie zidentyfikowanego wcześniej zagrożenia [94]. Przewidziane są zróżnicowane okresy dostępu (sześć, dziewięć lub dwanaście miesięcy) w zależności od potencjalnego zagrożenia, a wniosek musi być zgodny z zasadami proporcjonalności i pomocniczości. Ustanowiono również mechanizm kontroli sprawowanej przez niezależny organ [95].

136. Jeśli chodzi o funkcjonariuszy policji sądowej belgijskiego instytutu ds. usług pocztowych i telekomunikacji (BIPT), uzyskanie przez nich dostępu do danych będących w posiadaniu operatorów telekomunikacyjnych jest możliwe pod nadzorem prokuratury, w bardzo ograniczonych szczególnych przypadkach [96], przy czym zdaniem rządu belgijskiego ich działalność nie obejmuje osób, których dane są zatrzymywane.

137. Jeśli chodzi o służby ratownicze, które udzielają pomocy na miejscu, mogą one zażądać danych osoby zgłaszającej, gdy po otrzymaniu zgłoszenia alarmowego służby te nie uzyskają od dostawcy lub operatora danych identyfikacyjnych wspomnianej osoby lub gdy są one niepełne lub nieprawidłowe.

138. Jeśli chodzi o funkcjonariuszy policji sądowej przydzielonych do komórki ds. osób zaginionych policji federalnej, mogą oni zażądać od operatora danych niezbędnych do odnalezienia osoby zaginionej, której integralność fizyczna jest w bezpośrednim niebezpieczeństwie. Dostęp, do udzielenia którego konieczne jest spełnienie ściśle określonych warunków, jest ograniczony do danych umożliwiających identyfikację użytkownika oraz danych

91 Możliwość przyjmowania takich środków przez prokuraturę jest przedmiotem sporu w zawisłej jeszcze sprawie dotyczącej odesłania prejudycjalnego C-746/18, HK/Prokuratur.

92 Prokuratura jest uprawniona do żądania od operatorów danych identyfikacyjnych w drodze uzasadnionej i pisemnej decyzji (ustnej w nagłych przypadkach), jeżeli wykaże proporcjonalność środka w odniesieniu do poszanowania życia prywatnego i jego pomocniczość w stosunku do wszelkich innych obowiązków w ramach dochodzenia. W przypadku przestępstw, które nie są zagrożone karą jednego roku pozbawienia wolności lub surowszą, prokuratura może zażądać danych tylko z okresu sześciu miesięcy poprzedzających wydanie przez nią decyzji.

93 Sędzia śledczy jest uprawniony do żądania od operatorów uzyskania wiadomości elektronicznych lub przechowywanych danych dotyczących ruchu i lokalizacji i może on przyjąć ten środek, jeżeli istnieją poważne przesłanki wskazujące na popełnienie przestępstwa zagrożonego określonymi karami, w drodze uzasadnionego i pisemnego postanowienia (ustnego w nagłych przypadkach) podlegającego tym samym wymogom proporcjonalności i pomocniczości, jakie obowiązują w odniesieniu do prokuratury. Pewne wyjątki ustanowione są w przypadku, gdy dany środek jest skierowany przeciwko niektórym chronionym kategoriom zawodowym (np. adwokatom lub lekarzom).

94 Decyzja ta, w zależności od przypadku, określa osoby fizyczne lub prawne, stowarzyszenia de facto lub grupy, przedmioty, miejsca, wydarzenia lub informacje podlegające określonej metodzie. Należy również wspomnieć o związku, jaki istnieje między celem, w jakim żąda się udzielenia dostępu do danych, a potencjalnym zagrożeniem uzasadniającym tę konkretną metodę.

95 Komisja administracyjna ds. nadzoru nad szczególnymi i wyjątkowymi metodami gromadzenia danych przez służby wywiadowcze i bezpieczeństwa (komisja BIM) oraz stały komitet kontroli służb wywiadowczych (komitet R). Rząd belgijski stwierdza, że komisja BIM jest odpowiedzialna za monitorowanie metod wyszukiwania stosowanych przez służby wywiadowcze i bezpieczeństwa, nad którymi sprawuje kontrolę pierwszej linii. Komisja ta, składająca się z sędziów, wykonuje swoje zadania w sposób całkowicie niezależny. Sprawowana jest również niezależna kontrola drugiego rzędu, dokonywana przez komitet R.

96 Dozwolony jest w przypadku badania, dochodzenia i ścigania naruszeń art. 114 (bezpieczeństwo sieci), 124 (poufność łączności elektronicznej) i 126 (zatrzymywanie i dostęp do danych) ustawy z dnia 13 czerwca 2005 r. o łączności elektronicznej.

związanych z dostępem i podłączeniem urządzeń końcowych do sieci i usługi, a także do lokalizacji takich urządzeń, i obejmuje dane przechowywane przez 48 godzin przed złożeniem wniosku.

139. Służba mediacji w telekomunikacji może zaś żądać jedynie danych identyfikacyjnych osoby, która w sposób niedozwolony korzystała z sieci lub usługi łączności elektronicznej. W tym przypadku brak jest przeprowadzenia uprzedniej kontroli przez niezależny organ sądowy lub administracyjny (odrębny od samej tej służby).

140. Wreszcie, w celu zwalczania przestępczości finansowej organ nadzorczy sektora finansowego może uzyskać dostęp do danych dotyczących ruchu i lokalizacji pod warunkiem uzyskania uprzedniej zgody sędziego śledczego.

141. Opis tych zasad i warunków uzyskiwania dostępu do zatrzymywanych danych, które obowiązują w odniesieniu do poszczególnych organów uprawnionych do uzyskiwania danych, świadczy o różnorodności przesłanek i zabezpieczeń, zaś szczegółowe zbadanie ich zgodności z kryteriami zastosowanymi przez Trybunał w jego orzecznictwie [97] jest zadaniem sądu odsyłającego.

142. Pragnę na przykład zauważyć, że w kontekście spornego uregulowania nie wydaje się, żeby właściwe organy krajowe miały obowiązek systematycznego informowania osób, których dane dotyczą (nie mający zastosowania wówczas, gdy informacje te zagrażają toczącym się dochodzeniom), o tym, że zapoznano się z ich danymi. Nie wydaje się również, że ustanawiane są, przynajmniej w niektórych przypadkach, takich jak te związane z naruszeniami finansowymi, z góry ustalone zasady dotyczące wagi takich naruszeń, uzasadniające udzielenie dostępu do odpowiednich danych. Związek między skalą ingerencji a wagą przestępstwa będącego przedmiotem dochodzenia, w rozumieniu wyroku Ministerio Fiscal, nie jest we wszystkich przypadkach oczywisty.

143. W każdym razie uważam, że uwagi dotyczące dostępu władz do danych mają drugorzędne znaczenie, skoro, w świetle tego, co już wskazano, uogólnione i niezróżnicowane zatrzymywanie tych danych jest głównym powodem, dla którego krajowe przepisy, których dotyczy niniejszej odesłanie, są niezgodne z prawem Unii.

4. W przedmiocie trzeciego pytania prejudycjalnego

144. Cour constitutionnelle zmierza do ustalenia, czy, w przypadku, gdyby w świetle odpowiedzi Trybunału stwierdzono, że przepisy krajowe są niezgodne z prawem Unii, mógłby on tymczasowo utrzymać skutki tych przepisów. Pozwoliłoby to uniknąć niepewności prawa oraz umożliwiłoby dalsze wykorzystywanie zatrzymanych i przechowywanych już danych do zamierzonych celów.

145. Zgodnie z utrwalonym orzecznictwem „jedynie Trybunał może, w drodze wyjątku oraz kierując się nadrzędnymi przesłankami pewności prawa, tymczasowo zawiesić skutki uchylenia przepisów prawa krajowego sprzecznych z podlegającym bezpośredniemu stosowaniu prawem Unii". „Powierzenie sądom krajowym prawa do przyznawania przepisom krajowym pierwszeństwa w stosunku do stojących im na przeszkodzie przepisów prawa Unii, nawet tymczasowo, godziłoby bowiem w zasadę jednolitego stosowania prawa Unii" [98].

[97] Odsyłam do pkt 60 niniejszej opinii.

[98] Wyrok z dnia 28 lipca 2016 r., Association France Nature Environnement (C-379/15, EU:C:2016:603, pkt 33).

146. Komisja uważa, że skoro Trybunał nie ograniczył w czasie skutków wykładni art. 15 ust. 1 dyrektywy 2002/58, odpowiedź na to pytanie sądu odsyłającego powinna być przecząca [99].

147. Jednakże w wyroku z dnia 28 lutego 2012 r., Inter-Environnement Wallonie i Terre wallonne [100] Trybunał orzekł, że dopuszczalne jest, by sąd krajowy, uwzględniając istnienie nadrzędnej przesłanki związanej z ochroną środowiska, posłużył się w drodze wyjątku przepisem krajowym pozwalającym na utrzymanie w mocy niektórych skutków krajowego aktu prawnego, którego nieważność stwierdzono w wyniku naruszenia przepisu prawa Unii [101].

148. Ta linia orzecznicza została potwierdzona wyrokiem z dnia 29 lipca 2019 r., Inter-Environnement Wallonie i Bond Beter Leefmilieu Vlaanderen [102]. Mimo iż wyrok ów został wydany w dziedzinie ochrony środowiska lub został oparty na bezpieczeństwie dostaw energii elektrycznej, nie znajduję powodu, aby nie zastosować go w innych obszarach prawa Unii, w szczególności w obszarze rozpatrywanym w niniejszej sprawie.

149. Jeżeli „nadrzędna przesłanka związana z ochroną środowiska" może uzasadniać, że w drodze wyjątku sądy krajowe utrzymają niektóre skutki przepisu krajowego niezgodnego z prawem Unii, wynika to z okoliczności, iż ochrona środowiska stanowi „jeden z podstawowych celów Unii, który ma przekrojowy i zasadniczy charakter" [103].

150. Jednym z celów Unii jest również stworzenie przestrzeni bezpieczeństwa (art. 3 TUE), która obejmuje poszanowanie podstawowych funkcji państwa, zwłaszcza tych, które mają na celu utrzymanie porządku publicznego i ochronę bezpieczeństwa narodowego (art. 4 ust. 2 TUE). Jest to cel nie mniej „przekrojowy i zasadniczy" niż ochrona środowiska, ponieważ jego realizacja jest niezbędnym warunkiem ustanowienia ram prawnych, które zagwarantują skuteczne korzystanie z podstawowych praw i wolności.

151. Moim zdaniem nadrzędne względy związane z ochroną bezpieczeństwa narodowego mogłyby uzasadniać to, aby w niniejszej sprawie Trybunał w drodze wyjątku zezwolił sądowi odsyłającemu na utrzymanie przynajmniej niektórych skutków spornej ustawy.

152. Wspomniane utrzymanie skutków wymagałoby, aby sąd odsyłający uznał, w świetle orzeczenia Trybunału, przepis krajowy za niezgodny z prawem Unii i ocenił, że konsekwencje, jakie natychmiastowe stwierdzenie nieważności owego przepisu (jeżeli w prawie krajowym skutkiem takiej niezgodności jest stwierdzenie nieważności) lub odstąpienie od jego stosowania mogłoby mieć dla bezpieczeństwa publicznego lub bezpieczeństwa państwa, są wyjątkowo niepokojące.

153. Tymczasowe utrzymanie (całości lub części) skutków przepisu krajowego wymagałoby również, aby:

– celem takiego utrzymania było uniknięcie luki prawnej o tak szkodliwych skutkach, jak te wynikające ze stosowania spornego uregulowania, której nie można byłoby usunąć innymi

99 Punkt 100 uwag Komisji.

100 Sprawa C-41/11, EU:C:2012:103.

101 Wyrok z dnia 28 lutego 2012 r., Inter-Environnement Wallonie i Terre wallonne (C-41/11, EU:C:2012:103, pkt 58). W wyroku z dnia 28 lipca 2016 r., Association France Nature Environnement (C-379/15, EU:C:2016:603, pkt 34), Trybunał wywiódł z powyższego stwierdzenia, że „zamiarem […] było przyznanie sądowi krajowemu, w konkretnym przypadku i w drodze wyjątku, prawa do dostosowania skutków uchylenia przepisu krajowego, który został uznany za sprzeczny z prawem Unii".

102 Sprawa C-411/17 (EU:C:2019:622, pkt 178).

103 Wyrok z dnia 28 lutego 2012 r., Inter-Environnement Wallonie i Terre wallonne (C-41/11, EU:C:2012:103, pkt 57).

środkami, a która pozbawiłaby władze krajowe cennego instrumentu gwarantującego bezpieczeństwo państwa; oraz

– miało ono miejsce wyłącznie przez czas ściśle niezbędny do przyjęcia środków pozwalających na usunięcie stwierdzonej niezgodności z prawem Unii [104].

154. Za przyjęciem tego rozwiązania przemawiają ponadto trudność związana z dostosowaniem przepisów krajowych do orzecznictwa ustanowionego w sprawie Tele2 Sverige i Watson [105] oraz okoliczność polegająca na tym, iż wola ustawodawcy belgijskiego znalazła wyraz w dostosowaniu do wyroku Digital Rights poprzez zmianę jego ustawodawstwa. Fakt ten pozwala sądzić, że ustawodawca belgijski dostosuje również ustawę z dnia 29 maja 2016 r. (przyjętą przed wydaniem wyroku Tele2 Sverige i Watson) do ustanowionego we wspomnianym wyroku orzecznictwa.

V. Wnioski

155. W świetle powyższych uwag proponuję, aby Trybunał Sprawiedliwości odpowiedział na pytania Cour constitutionnelle (trybunału konstytucyjnego, Belgia) w następujący sposób:

„1) Artykuł 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (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:

– sprzeciwia się on uregulowaniu krajowemu, które nakłada na operatorów i dostawców usług łączności elektronicznej obowiązek zatrzymywania w sposób uogólniony i niezróżnicowany danych dotyczących ruchu i lokalizacji wszystkich abonentów i użytkowników w odniesieniu do wszystkich środków łączności elektronicznej;

– powyższego nie wyklucza okoliczność polegająca na tym, że to uregulowanie krajowe zostało ustanowione nie tylko w celu prowadzenia dochodzenia, wykrywania i ścigania przestępstw poważnych lub o mniejszej wadze, lecz także w celu zapewnienia bezpieczeństwa narodowego, obrony terytorium, bezpieczeństwa publicznego, zapobiegania nieuprawnionemu korzystaniu z systemu łączności elektronicznej lub jakikolwiek inny cel określony w art. 23 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);

– powyższego nie wyklucza również okoliczność polegająca na tym, że udzielanie dostępu do zatrzymywanych danych podlega ściśle uregulowanym gwarancjom; to do sądu odsyłającego należy ustalenie, czy uregulowanie krajowe, które określa warunki uzyskiwania wspomnianego dostępu przez właściwe organy, ogranicza go jedynie do konkretnych przypadków, których waga uzasadnia konieczność ingerencji; z wyjątkiem nagłych przypadków, uzależnia udzielenie rzeczonego dostęp od przeprowadzenia przez sąd lub niezależny organ uprzedniej kontroli; oraz przewiduje, że osoby, których dane

104 Wyrok z dnia 28 lutego 2012 r., Inter-Environnement Wallonie i Terre wallonne (C-41/11; EU:C:2012:103, pkt 62).

105 Punkt 45 pisemnych uwag rządu duńskiego.

dotyczą, będą informowane o takim dostępie pod warunkiem, że powiadomienie to nie zagraża działaniu wymienionych organów.

2) Artykuły 4 i 6 Karty praw podstawowych Unii Europejskiej nie mają wpływu na wykładnię art. 15 ust. 1 dyrektywy 2002/58 w odniesieniu do pozostałych wyżej wymienionych artykułów karty w taki sposób, że nie dają one możliwości stwierdzenia niezgodności z prawem Unii uregulowania krajowego takiego jak to będące przedmiotem sporu w postępowaniu głównym.

3) Sąd krajowy, o ile zezwala na to prawo krajowe, może w drodze wyjątku i tymczasowo utrzymać skutki uregulowania takiego jak to będące przedmiotem sporu w postępowaniu głównym, nawet jeśli jest ono niezgodne z prawem Unii, jeżeli takie utrzymanie jest uzasadnione nadrzędnymi względami związanymi z zagrożeniami dla bezpieczeństwa publicznego lub bezpieczeństwa narodowego, którym nie można zaradzić za pomocą innych, alternatywnych środków. Takie utrzymanie może mieć miejsce jedynie przez czas ściśle niezbędny do usunięcia wspomnianej niezgodności z prawem Unii”.