Zbiór Orzeczeń

OPINIA RZECZNIKA GENERALNEGO
HENRIKA SAUGMANDSGAARDA ØE
przedstawiona w dniu 19 lipca 2016 r.[1]

Sprawy połączone C-203/15 i C-698/15

Tele2 Sverige AB
przeciwko
Post- och telestyrelsen (C-203/15)
i
Secretary of State for the Home Department
przeciwko
Tomowi Watsonowi,
Peterowi Brice'owi,
Geoffreyowi Lewisowi (C-698/15),
przy udziale
Open Rights Group,
Privacy International,
Law Society of England and Wales

{wnioski o wydanie orzeczenia w trybie prejudycjalnym, złożone przez Kammarrätten i Stockholm (administracyjny sąd apelacyjny w Sztokholmie, Szwecja) i Court of Appeal (England & Wales) (Civil Division) [sąd apelacyjny (Anglia i Walia) (wydział cywilny), Zjednoczone Królestwo]}

Odesłanie prejudycjalne — Dyrektywa 2002/58/WE — Przetwarzanie danych osobowych i ochrona prywatności w sektorze łączności elektronicznej — Ustawodawstwo krajowe przewidujące ogólny obowiązek zatrzymywania danych dotyczących łączności elektronicznej — Artykuł 15 ust. 1 — Karta praw podstawowych Unii Europejskiej — Artykuł 7 — Prawo do poszanowania życia prywatnego — Artykuł 8 — Prawo do ochrony danych osobowych — Poważna ingerencja — Uzasadnienie — Artykuł 52 ust. 1 — Warunki — Zgodny z prawem cel walki z poważnymi przestępstwami — Wymóg podstawy prawnej w prawie krajowym — Wymóg absolutnej konieczności — Wymóg proporcjonalności w demokratycznym społeczeństwie

Spis treści

1 — Język oryginału: francuski.

I – **Wprowadzenie**

1. W 1788 r. współtwórca konstytucji Stanów Zjednoczonych James Madison napisał: „If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself” [2].

2. Sedno niniejszych spraw stawia nas w samym centrum „największej trudności” wskazanej przez Madisona. Sprawy te dotyczą zgodności z prawem Unii systemów krajowych ustanawiających po stronie dostawców publicznie dostępnych usług łączności elektronicznej (zwanych dalej „dostawcami”) obowiązek zatrzymywania danych dotyczących łączności elektronicznej (zwanych dalej „danymi dotyczącymi komunikatów”) w odniesieniu do ogółu środków komunikacji i wszystkich użytkowników (zwany dalej „ogólnym obowiązkiem zatrzymywania danych”).

3. Z jednej strony zatrzymywanie danych dotyczących komunikatów daje „rządowi możność kontroli nad rządzonymi”, przyznając właściwym organom środek dochodzeniowy, który może mieć pewną użyteczność w walce z poważnymi przestępstwami, w szczególności w walce z terroryzmem. Zasadniczo zatrzymywanie tych danych daje bowiem władzom ograniczoną zdolność do „odtwarzania przeszłości” dzięki dostępowi do danych dotyczących komunikatów przekazywanych przez osobę, nawet zanim jeszcze stała się podejrzana o związek z poważnym przestępstwem [3].

2 — „Gdyby ludzie byli aniołami, żaden rząd nie byłby potrzebny. Gdyby ludźmi rządzili aniołowie, nie byłaby potrzebna ani zewnętrzna, ani wewnętrzna kontrola nad rządem. Przy tworzeniu rządu, w którym ludzie rządzą ludźmi, największa trudność polega na tym, że trzeba wpierw dać rządowi możność kontroli nad rządzonymi, a potem zobowiązać go do kontrolowania samego siebie”. J. Madison, Federalist No. 51, w: A. Hamilton, J. Madison, J. Jay, *The Federalist Papers*, ed. M.A. Genovese, Palsgrave Macmillan, New York 2009, s. 120 (wolny przekład). Madison był jednym z głównych autorów i jednym z 39 sygnatariuszy konstytucji Stanów Zjednoczonych (1787). Następnie został czwartym prezydentem Stanów Zjednoczonych (w latach 1809–1817).

3 — Ta ograniczona zdolność do „odtwarzania przeszłości” może okazać się bardzo przydatna do celów identyfikacji ewentualnych pomocników: zob. pkt 178–184 niniejszej opinii.

4. Jednakże z drugiej strony konieczne jest „zobowiązanie rządu do kontroli samego siebie" zarówno w zakresie zatrzymywania, jak i dostępu do zatrzymanych danych, z uwagi na poważne zagrożenia spowodowane istnieniem takich baz danych obejmujących całość komunikatów na terytorium krajowym. W istocie owe znacznych rozmiarów bazy danych oferują każdej osobie, która ma do nich dostęp, możliwość natychmiastowego katalogowania ogółu danej populacji [4]. Zagrożenia te powinny zostać skrupulatnie zanalizowane, w szczególności w drodze zbadania absolutnie koniecznego i proporcjonalnego charakteru ogólnego obowiązku zatrzymywania danych, takiego jak obowiązki rozpatrywane w postępowaniach głównych.

5. Tak więc w ramach niniejszych spraw Trybunał i sądy odsyłające zobowiązane są do określenia odpowiedniej równowagi między spoczywającym na państwach członkowskich obowiązkiem zapewnienia bezpieczeństwa osób znajdujących się na ich terytorium a przestrzeganiem praw podstawowych do poszanowania życia prywatnego oraz do ochrony danych osobowych ustanowionych w art. 7 i 8 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą").

6. To właśnie w świetle tej „największej trudności" zbadam pytania postawione Trybunałowi w niniejszych sprawach. Dotyczą one konkretnie zgodności systemów krajowych ustanawiających ogólny obowiązek zatrzymywania danych z dyrektywą 2002/58/WE [5] oraz z art. 7 i 8 karty. W celu udzielenia odpowiedzi na te pytania Trybunał będzie musiał w szczególności wyjaśnić, jaką należy – w kontekście krajowym – przyjąć wykładnię wyroku Digital Rights Ireland i in. (zwanego dalej „wyrokiem DRI") [6], w którym wielka izba Trybunału stwierdziła nieważność dyrektywy 2006/24/WE [7].

7. Z powodów, które przedstawię poniżej, wydaje mi się, że ogólny obowiązek zatrzymywania danych nałożony przez państwo członkowskie może być zgodny z prawami podstawowymi zagwarantowanymi prawem Unii, pod warunkiem ścisłego obwarowania go szeregiem gwarancji, które wskażę w moim rozumowaniu.

II – **Ramy prawne**

A – *Dyrektywa 2002/58*

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

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

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

4 — Zobacz pkt 252–261 niniejszej opinii.

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), zmieniona dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. (Dz.U. 2009, L 337, s. 11).

6 — Wyrok z dnia 8 kwietnia 2014 r., C-293/12 i C-594/12, EU:C:2014:238.

7 — 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).

3. Niniejsza dyrektywa nie ma zastosowania do działalności, która wykracza poza zakres [TFUE], takiej jak działalność określona w tytułach V i VI [TUE], ani, w żadnym wypadku do działalności dotyczącej bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając dobrobyt gospodarczy państwa, gdy działalność odnosi się do spraw bezpieczeństwa państwa) i działalności państwa w dziedzinie prawa karnego".

9. Artykuł 15 ust. 1 dyrektywy 2002/58, zatytułowany „Stosowanie niektórych przepisów dyrektywy [95/46]", ma następujące brzmienie:

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

B – *Prawo szwedzkie*

10. Dyrektywa 2006/24, obecnie nieważna, została transponowana do prawa szwedzkiego w drodze zmian do lagen (2003:389) om elektronisk kommunikation (szwedzkiej ustawy 2003:389 o łączności elektronicznej, zwanej dalej „LEK") i do förordningen (2003:396) om elektronisk kommunikation (rozporządzenia 2003:396 o łączności elektronicznej, zwanego dalej „FEK"), które weszły w życie w dniu 1 maja 2012 r.

1. W przedmiocie zakresu obowiązku zatrzymywania

11. Z rozdziału 6 §16 LEK wynika, że dostawcy są zobowiązani zatrzymywać dane dotyczące komunikatów niezbędne do identyfikacji ich źródła i odbiorcy, ustalenia daty, godziny i czasu trwania komunikatu, wskazania jego rodzaju, używanego narzędzia komunikacji i lokalizacji urządzenia komunikacji ruchomej używanego po rozpoczęciu i zakończeniu połączenia. Rodzaje danych, które mają być zatrzymywane, są przedmiotem bardziej szczegółowego uregulowania w §§ 38–43 FEK.

12. Ów obowiązek zatrzymywania danych obejmuje dane przetwarzane w ramach świadczenia usługi telefonii, usługi telefonii przy użyciu połączenia telefonii komórkowej, usługi poczty elektronicznej, usługi dostępu do Internetu oraz usługi zapewniania możliwości dostępu do Internetu.

13. Dane podlegające zatrzymywaniu obejmują nie tylko wszystkie dane, które miały być zatrzymywane w ramach dyrektywy 2006/24, ale także dane dotyczące nieudanych prób połączeń, a także dotyczące lokalizacji w momencie zakończenia połączenia komórkowego. Na wzór systemu przewidzianego w tej dyrektywie dane podlegające zatrzymywaniu nie obejmują treści komunikatów.

2. W przedmiocie dostępu do zatrzymywanych danych

14. Dostęp do zatrzymanych danych jest regulowany głównie przez trzy akty, mianowicie LEK, rättegångsbalken (kodeks postępowania sądowego, zwany dalej „RB") i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (szwedzką ustawę 2012:278 o przekazywaniu danych dotyczących łączności elektronicznej w ramach działań dochodzeniowo-śledczych prowadzonych przez organy ścigania).

a) LEK

15. Rozdział 6 § 22 akapit pierwszy pkt 2 LEK stanowi, że dostawca musi na żądanie przekazać dane dotyczące abonamentu prokuraturze, policji, Säkerhetspolisen (szwedzkiemu urzędowi ds. bezpieczeństwa, zwanemu dalej „Säpo") lub innemu publicznemu organowi odpowiedzialnemu za zwalczanie przestępczości, jeżeli wspomniane dane odnoszą się do domniemanego przestępstwa. Zgodnie z tymi przepisami nie ma wymogu, że musi chodzić o poważne przestępstwo.

16. Poprzez pojęcie danych dotyczących abonamentu rozumie się zasadniczo nazwisko, tytuł, adres, numer telefonu i adres IP abonenta.

17. Zgodnie z LEK przekazanie danych dotyczących abonamentu nie wymaga uprzedniej kontroli, lecz może być przedmiotem następczej kontroli administracyjnej. Ponadto krąg organów, które mogą mieć dostęp do danych, nie został ograniczony.

b) RB

18. RB reguluje niejawne obserwowanie łączności elektronicznej w trakcie postępowania przygotowawczego.

19. Niejawne obserwowanie łączności elektronicznej może co do zasady być przeprowadzone tylko wtedy, gdy istnieje uzasadnione podejrzenie, że określona osoba popełniła przestępstwo zagrożone karą co najmniej sześciu miesięcy pozbawienia wolności lub inne wyraźnie wymienione przestępstwa, jeśli środek ten ma szczególne znaczenie dla postępowania.

20. Poza tym takie niejawne obserwowanie łączności elektronicznej może być prowadzone na potrzeby dochodzenia dotyczącego przestępstwa zagrożonego karą co najmniej dwóch lat pozbawienia wolności w celu ustalenia osoby, co do której mogłoby istnieć uzasadnione podejrzenie popełnienia owego przestępstwa, jeśli środek ten ma szczególne znaczenie dla postępowania.

21. Zgodnie z rozdziałem 27 § 21 RB niejawne obserwowanie łączności elektronicznej wymaga co do zasady otrzymania przez prokuratora zezwolenia właściwego sądu.

22. Niemniej jednak, o ile istnieją podstawy, aby sądzić, że uzyskanie zgody sądu na niejawne obserwowanie łączności elektronicznej – środek absolutnie konieczny dla potrzeb postępowania – jest niezgodne z pilnym charakterem wdrożenia tego środka oraz skutkowałoby powstaniem przeszkód, o tyle pozwolenie na zastosowanie środka jest wydawane przez prokuratora w oczekiwaniu na decyzję właściwego sądu. Pisemne powiadomienie o zastosowaniu środka musi być natychmiast przesłane do sądu przez prokuratora. Właściwy sąd musi następnie szybko zbadać, czy istnieją podstawy do zastosowania środka.

c) Ustawa 2012:278

23. Zgodnie z § 1 ustawy 2012:278 policja krajowa, Säpo i Tullverket (szwedzki organ kontroli celnej) mogą, na warunkach określonych w tej ustawie, gromadzić w trakcie swoich dochodzeń, bez wiedzy dostawcy, dane dotyczące komunikatów.

24. Zgodnie z §§ 2 i 3 ustawy 2012:278 dane mogą być gromadzone, jeżeli okoliczności wskazują, że środek ten ma szczególne znaczenie dla prewencji, zapobiegania lub wykrywania działalności przestępczej, która obejmuje przestępstwo lub przestępstwa zagrożone karą od dwóch lat pozbawienia wolności lub czyny wymienione w § 3 (w tym w szczególności różne formy sabotażu i szpiegostwa).

25. Decyzja o gromadzeniu danych jest podejmowana przez szefa właściwego organu lub pracownika, któremu szef właściwego organu deleguje uprawnienia decyzyjne.

26. Decyzja musi określać działalność przestępczą, odnośny okres czasu, a także numer telefonu, inny adres, urządzenia łączności elektronicznej lub obszar geograficzny objęty środkiem. Okres, na jaki udziela się zezwolenia, nie może być dłuższy niż jest to konieczne i nie może, w odniesieniu do okresu po wydaniu decyzji w sprawie zezwolenia, przekraczać jednego miesiąca.

27. Tego rodzaju środek nie wymaga uprzedniej kontroli. Jednakże, zgodnie z § 6 ustawy 2012:278, Säkerhets- och integritetsskyddsnämnden (komisja ds. bezpieczeństwa i ochrony integralności, Szwecja) musi być informowana o każdej decyzji w sprawie zezwolenia na gromadzenie danych. Zgodnie z § 1 lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (ustawy 2007:980 o nadzorze nad niektórymi działaniami związanymi ze zwalczaniem przestępczości) organ ten powinien sprawować nadzór nad stosowaniem prawa przez organy ścigania.

3. W przedmiocie okresu przechowywania zatrzymanych danych

28. Rozdział 6 § 16d LEK stanowi, że dane, o których mowa w rozdziale 6 §16a, muszą być przechowywane przez okres sześciu miesięcy, liczonych od dnia zakończenia połączenia. Dane te muszą być następnie natychmiast usunięte, chyba że § 16d akapit drugi LEK (w rozdziale 6) stanowi inaczej. Zgodnie z tymi przepisami dane, o które wystąpiono przed upływem okresu zatrzymywania, ale jeszcze nieprzekazane, zostają usunięte natychmiast po przekazaniu.

4. W przedmiocie ochrony i bezpieczeństwa zatrzymanych danych

29. Paragraf 20 akapit pierwszy rozdziału 6 LEK zakazuje rozpowszechniania lub używania w sposób nieautoryzowany danych dotyczących komunikatów.

30. Paragraf §3 a rozdziału 6 LEK stanowi, że dostawcy muszą zastosować odpowiednie środki techniczne i organizacyjne niezbędne w celu zapewnienia ochrony danych w trakcie przetwarzania. Prace przygotowawcze nad tymi przepisami wskazują, że nie dopuszcza się określenia poziomu ochrony poprzez wyważenie względów związanych z technologią i kosztami w stosunku do względów związanych z ryzykiem naruszenia prywatności.

31. Inne przepisy dotyczące ochrony danych znajdują się w §37 FEK oraz w regulacjach i ogólnych wytycznych Post- och telestyrelsen (szwedzkiego organu nadzoru poczty i telekomunikacji, zwanego dalej „PTS”) na temat środków ochrony w ramach zatrzymywania i przetwarzania danych do celów walki z przestępczością (PTSFS nr 2012:4). Ze wspomnianych aktów wynika między innymi, że dostawcy muszą podjąć działania w celu ochrony danych przed przypadkowym lub bezprawnym zniszczeniem, przed bezprawnym przechowywaniem, przetwarzaniem lub dostępem i bezprawnym ich ujawnieniem. Dostawca musi również ciągle i systematycznie czuwać nad bezpieczeństwem danych, z uwzględnieniem szczególnych zagrożeń związanych z obowiązkiem zatrzymywania danych.

32. W prawie szwedzkim nie występują żadne przepisy regulujące kwestię miejsca, w którym zatrzymywane dane mają być przechowywane.

33. Zgodnie z rozdziałem 7 LEK w przypadku uchybienia przez dostawcę jego obowiązkom organ nadzoru ma uprawnienia do wydawania nakazów i zakazów oraz ewentualnego nakładania kar pieniężnych, a także do nakazania zaprzestania działalności w całości lub w części.

C – Prawo Zjednoczonego Królestwa

34. Przepisy dotyczące zatrzymywania danych znajdują się w Data Retention and Investigatory Powers Act 2014 (ustawie z 2014 r. o zatrzymywaniu danych i uprawnieniach dochodzeniowych, zwanej dalej „DRIPA"), w Data Retention Regulations 2014 (SI 2014/2042) (rozporządzeniu z 2014 r. dotyczącym zatrzymywania danych, zwanym dalej „rozporządzeniem z 2014 r.") oraz w Retention of Communications Data Code of Practice (kodeksie dobrej praktyki dotyczącym zatrzymywania danych dotyczących komunikatów).

35. Przepisy regulujące dostęp do danych znajdują się w części 1 rozdziału 2 Regulation of Investigatory Powers Act 2000 (ustawy z 2000 r. dotyczącej uregulowania uprawnień dochodzeniowo-śledczych, zwanej dalej „RIPA"), Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480) (dekrecie z 2015 r. dotyczącym uregulowania uprawnień dochodzeniowych w dziedzinie danych dotyczących łączności), zmienionym przez Regulation of Investigatory Powers (Communications Data) (Amendement) Order 2015 (SI 2015/228), oraz Acquisition and Disclosure of Communications Data Code of Practice (kodeksie dobrych praktyk w sprawie pozyskiwania i ujawniania danych dotyczących komunikatów, zwanym dalej „kodeksem w sprawie pozyskiwania danych").

1. W przedmiocie zakresu obowiązku zatrzymywania

36. Na podstawie sekcji 1 DRIPA Secretary of State for the Home Department (minister spraw wewnętrznych, Zjednoczone Królestwo, zwany dalej „ministrem") może nałożyć na dostawców obowiązek zatrzymywania wszystkich danych dotyczących komunikatów. Obowiązek ten może w istocie dotyczyć wszystkich danych generowanych w związku z komunikatem dostarczanym w ramach usługi pocztowej lub systemu telekomunikacyjnego, z wyjątkiem treści komunikatu. Informacje te obejmują w szczególności miejsce, w którym znajduje się użytkownik usługi, oraz dane pozwalające na ustalenie adresu IP (protokołu internetowego) lub innego identyfikatora należącego do nadawcy lub odbiorcy komunikatu.

37. Cele, jakie mogą uzasadnić przyjęcie takiego środka w zakresie zatrzymywania danych, obejmują interes bezpieczeństwa narodowego, zapobieganie przestępstwom lub wykrywanie ich, lub zapobieganie naruszeniom porządku publicznego, interes gospodarki Zjednoczonego Królestwa w zakresie, w jakim interes ten ma również znaczenie dla bezpieczeństwa państwa, interes bezpieczeństwa publicznego, ochronę zdrowia publicznego, wymiar lub pobór podatku, opłaty lub innej należności na rzecz administracji publicznej, zapobieżenie uszczerbkowi na zdrowiu fizycznym lub psychicznym w nagłych przypadkach, pomoc w czynnościach dochodzeniowo-śledczych w sprawach dotyczących pomyłek sądowych, ustalenie tożsamości osoby, która zmarła lub która jest niezdolna do podania swojej tożsamości z powodów innych niż przestępstwo (takich jak klęska żywiołowa lub wypadek), wykonywanie zadań związanych z nadzorem usług finansowych i rynków finansowych lub stabilności finansowej, a także każdy inny cel określony w nakazie wydanym przez ministra zgodnie z sekcją 22 ust. 2 DRIPA.

38. Przepisy krajowe nie wymagają, aby przyjęcie aktu nakazującego zatrzymywanie danych było uzależnione od uprzedniego zezwolenia wydanego przez sąd lub inny niezależny organ. Minister musi sprawdzić, czy obowiązek zatrzymywania danych jest „konieczny i proporcjonalny" dla jednego lub większej liczby celów, dla których mogą być zatrzymywane odnośne dane dotyczące komunikacji.

2. W przedmiocie dostępu do zatrzymywanych danych

39. Na mocy sekcji 22 ust. 4 RIPA organy władzy publicznej mogą w drodze określonych aktów zobowiązać dostawców, aby ujawniali tym organom dane dotyczące komunikatów. Formę i treść tych aktów reguluje sekcja 23 ust. 2 RIPA. Taki akt jest ograniczony w czasie na mocy przepisów dotyczących jego odwołania i przedłużenia.

40. Pozyskiwanie danych dotyczących łączności musi być konieczne i proporcjonalne do jednego lub większej liczby celów wymienionych w pkt 22 RIPA, które odpowiadają celom mogącym uzasadniać zatrzymywanie danych, opisanym w pkt 37 niniejszej opinii.

41. Z kodeksu w sprawie pozyskiwania danych wynika, że w przypadku wniosku o dostęp w celu wskazania źródła dziennikarskiego, a także w przypadku wniosku o dostęp złożonego przez władze lokalne wymagane jest postanowienie sądu.

42. W innych przypadkach dostęp organów władzy publicznej jest uzależniony od uzyskania zezwolenia udzielonego przez osoby wyznaczone w tym celu w danym organie władzy publicznej. Osoba wyznaczona to osoba pełniąca określoną funkcję, posiadająca określoną rangę lub zajmująca określone stanowisko w odnośnym organie władzy publicznej, która została wyznaczona jako osoba właściwa do celów pozyskania danych dotyczących komunikatów zgodnie z rozporządzeniem z 2015 r. dotyczącym unormowania uprawnień dochodzeniowo-śledczych w dziedzinie danych dotyczących komunikatów, ze zmianami.

43. Zgoda sądu ani niezależnego organu nie jest wyraźnie wymagana w odniesieniu do dostępu do danych dotyczących komunikatów chronionych ustawową tajemnicą zawodową ani do danych dotyczących komunikatów odnoszących się do lekarzy medycyny, członków Parlamentu czy też osób duchownych. Kodeks w sprawie pozyskiwania danych uściśla jedynie, że szczególną uwagę należy poświęcić niezbędności i proporcjonalności wniosku o udzielenie dostępu do takich danych.

3. W przedmiocie okresu przechowywania zatrzymanych danych

44. Sekcja 1 ust. 5 DRIPA i przepis 4 ust. 2 rozporządzenia z 2014 r. przewidują, że maksymalny okres przechowywania danych wynosi 12 miesięcy. Zgodnie z kodeksem dobrych praktyk w sprawie zatrzymywania danych długość tego okresu nie powinna przekraczać długości koniecznej i proporcjonalnej. Przepis 6 rozporządzenia z 2014 r. wymaga dokonania przez ministra przeglądu aktu nakazującego zatrzymywanie.

4. W przedmiocie ochrony i bezpieczeństwa zatrzymanych danych

45. Na podstawie sekcji 1 DRIPA dostawcy mają zakaz ujawniania zatrzymywanych danych, chyba że ujawnienie to jest zgodne z rozdziałem 2 części 1 RIPA, orzeczeniem sądowym lub innym zezwoleniem lub nakazem sądowym, lub też rozporządzeniem przyjętym przez ministra na podstawie sekcji 1 DRIPA.

46. Na podstawie przepisów art. 7 i 8 rozporządzenia z 2014 r. dostawcy muszą: zapewnić integralność i bezpieczeństwo zatrzymanych danych; chronić je przed przypadkowym lub bezprawnym zniszczeniem, utratą lub przypadkową zmianą, niedozwolonym lub bezprawnym zatrzymywaniem, przetwarzaniem, dostępem lub ujawnieniem; zniszczyć dane w celu uniemożliwienia dostępu do nich po wygaśnięciu zezwolenia na przechowywanie danych; wdrożyć odpowiednie systemy bezpieczeństwa. Przepis 9 rozporządzenia z 2014 r. powierza Information Commissioner (głównemu inspektorowi ochrony danych) obowiązek weryfikacji przestrzegania tych obowiązków przez dostawców.

47. Organy, którym dostawcy przekazują dane dotyczące komunikatów, powinny przetwarzać i zatrzymywać te dane, jak również ich kopie, wyciągi lub streszczenia, w sposób bezpieczny. Na mocy kodeksu w sprawie pozyskiwania danych wymogi zawarte w Data Protection Act (ustawie o ochronie danych, zwanej dalej „DPA"), która dokonuje transpozycji dyrektywy 95/46, powinny być przestrzegane.

48. RIPA ustanawia Interception of Communications Commissioner (głównego inspektora ds. przechwytywania komunikatów, zwanego dalej „inspektorem ds. przechwytywania"), który odpowiada za nadzorowanie w sposób niezależny wykonywania i realizacji uprawnień i obowiązków zawartych w rozdziale II części I RIPA. Inspektor ds. przechwytywania nie nadzoruje przypadków korzystania z uprawnień na podstawie sekcji 1 DRIPA. Przedstawia on regularnie sprawozdania skierowane do ogółu ludności i do Parlamentu (sekcja 57 ust. 2 i sekcja 58 RIPA) i opisuje, jakie dane są przechowywane i raportowane przez organy władzy publicznej (kodeks w sprawie pozyskiwania danych, pkt 6.1–6.8). Jeśli istnieje powód, aby sądzić, że dane zostały uzyskane w sposób niewłaściwy, skargi można również składać do Investigatory Powers Tribunal (sądu ds. uprawnień dochodzeniowych) (sekcja 65 RIPA).

49. Z kodeksu w sprawie pozyskiwania danych wynika, że inspektor ds. przechwytywania nie ma uprawnienia do odesłania sprawy do owego sądu. Jest on jedynie uprawniony do poinformowania danej osoby o podejrzeniu bezprawnego wykorzystania uprawnień, o ile może „wykazać, że dana osoba została poszkodowana wskutek uchybienia umyślnego lub lekkomyślnego". Jednakże nie jest on upoważniony do ujawnienia uchybienia, jeśli przez takie ujawnienie zagrożone byłoby bezpieczeństwo narodowe, nawet jeśli uważa, że doszło do uchybienia umyślnego lub lekkomyślnego.

III – **Postępowania główne i pytania prejudycjalne**

A – *Sprawa C-203/15*

50. W dniu 9 kwietnia 2014 r., czyli następnego dnia po ogłoszeniu wyroku DRI, Tele2 Sverige powiadomiło PTS o swej decyzji o zaprzestaniu zatrzymywania danych zgodnie z rozdziałem 6 LEK. Tele2 Sverige miało również usunąć dane, które zostały zatrzymane wcześniej zgodnie z tym rozdziałem. Tele2 Sverige stwierdziło, że szwedzkie przepisy prawne transponujące dyrektywę 2006/24 nie były zgodne z kartą.

51. W dniu 15 kwietnia 2014 r. Rikspolisstyrelsen (komenda główna policji, Szwecja, zwana dalej „RPS") zwróciła się ze skargą do PTS ze względu na to, że Tele2 Sverige przestało przekazywać dane dotyczące niektórych komunikatów elektronicznych. W swojej skardze RPS wyjaśnił, że odmowa Tele2 Sverige pociąga za sobą poważne konsekwencje dla działań policji związanych ze zwalczaniem przestępczości.

52. Decyzją z dnia 27 czerwca 2014 r. PTS nakazał Tele2 Sverige, aby spółka ta wznowiła zatrzymywanie danych zgodnie z rozdziałem 6 §16a LEK i z §§ 37–43 FEK najpóźniej od dnia 25 lipca 2014 r.

53. Tele2 Sverige zaskarżyło decyzję PTS do Förvaltningsrätten i Stockholm (sądu administracyjnego w Sztokholmie, Szwecja). Wyrokiem z dnia 13 października 2014 r. Förvaltningsrätten i Stockholm oddalił tę skargę.

54. Tele2 Sverige wniosło apelację od wyroku Förvaltningsrätten i Stockholm do sądu odsyłającego w celu uzyskania stwierdzenia nieważności zaskarżonej decyzji.

55. Stwierdzając, że istniały argumenty przemawiające zarówno za stanowiskiem, iż tak szeroki zakres obowiązku zatrzymywania, jaki został przewidziany w rozdziale 6 §16a LEK, jest zgodny z art. 15 ust. 1 dyrektywy 2002/58 i z art. 7, 8 i art. 52 ust. 1 karty, jak i przeciw temu stanowisku, Kammarrätten i Stockholm (administracyjny sąd apelacyjny w Sztokholmie, Szwecja) postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„1) Czy ogólny obowiązek zatrzymywania danych o ruchu obejmujący wszystkie osoby, wszystkie środki łączności elektronicznej i wszystkie dane o ruchu telekomunikacyjnym bez rozróżnienia, ograniczenia czy wyjątków do celów zwalczania przestępczości [taki jak opisany w pkt 13–18 postanowienia odsyłającego] jest zgodny z art. 15 ust. 1 dyrektywy 2002/58 z uwzględnieniem art. 7, 8 i art. 52 ust. 1 karty?

2) W przypadku odpowiedzi przeczącej na pytanie pierwsze, czy zatrzymywanie może być jednak dozwolone, gdy:

   a) dostęp organów krajowych do zatrzymanych danych jest określony w sposób opisany w pkt 19–36 [postanowienia odsyłającego] oraz

   b) wymogi w zakresie ochrony i bezpieczeństwa danych są regulowane w sposób opisany w pkt 38–43 [postanowienia odsyłającego], a także

   c) wszystkie dane o ruchu telekomunikacyjnym mają być przechowywane przez sześć miesięcy, licząc od dnia zakończenia połączenia, a następnie usuwane w sposób opisany w pkt 37 [postanowienia odsyłającego]?”.

B – *Sprawa C-698/15*

56. Tom Watson, P. Brice i G. Lewis wnieśli do High Court of Justice (England & Wales), Queen’s Bench Division (Administrative Court) [sądu wyższej instancji (Anglia i Walia), wydział Queen’s Bench Division (izba administracyjna)] środki prawne dotyczące kontroli zgodności z prawem („judicial review”) systemu zatrzymywania danych ustanowionego w sekcji 1 DRIPA, upoważniającego ministra do zobowiązania publicznych operatorów telekomunikacyjnych do zatrzymywania wszystkich danych dotyczących komunikatów na okres nieprzekraczający 12 miesięcy, z wykluczeniem zatrzymywania treści komunikatów.

57. Open Rights Group, Privacy International i Law Society of England and Wales zostały dopuszczone do sprawy w charakterze interwenienta w ramach każdej z tych skarg.

58. Wyrokiem dnia 17 lipca 2015 r. sąd ten stwierdził, że ów system nie był zgodny z prawem Unii w zakresie, w jakim nie spełniał wymogów ustanowionych w wyroku DRI, które sąd ów uznał za mające zastosowanie do przepisów państw członkowskich w dziedzinie zatrzymywania danych dotyczących komunikatów elektronicznych i dostępu do takich danych. Minister wniósł apelację od tego orzeczenia do sądu odsyłającego.

59. W wyroku z dnia 20 listopada 2015 r. Court of Appeal (England & Wales) (Civil Division) [sąd apelacyjny (Anglia i Walia) (wydział cywilny), Zjednoczone Królestwo] stwierdził wstępnie, że wyrok DRI nie ustanowił wiążących wymogów prawa Unii, z którymi muszą być zgodne uregulowania krajowe, lecz jedynie wskazał i opisał środki ochronne niezawarte w zharmonizowanym systemie Unii.

60. Jednakże uznając, że odpowiedzi na te pytania dotyczące prawa Unii nie były jasne, a były konieczne do orzekania w tych postępowaniach, Court of Appeal (England & Wales) (Civil Division) [sąd apelacyjny (Anglia i Walia) (wydział cywilny)] postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„1) Czy wyrok [DRI] (w tym w szczególności pkt 60 i 62 tego wyroku) ustanawia wiążące wymogi prawa Unii mające zastosowanie do prawa krajowego państwa członkowskiego normującego dostęp do danych zatrzymywanych zgodnie z ustawodawstwem krajowym, w celu zapewnienia zgodności z art. 7 i 8 [karty]?

2) Czy wyrok [DRI] rozszerza zakres stosowania art. 7 lub 8 karty w sposób wykraczający poza zakres art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności (»EKPC«) określony w orzecznictwie Europejskiego Trybunału Praw Człowieka (»ETPC«)?”.

IV – **Postępowanie przed Trybunałem**

61. Wnioski o wydanie orzeczenia w trybie prejudycjalnym zostały zarejestrowane w sekretariacie Trybunału w dniu 4 maja 2015 r. w sprawie C-203/15 i w dniu 28 grudnia 2015 r. w sprawie C-698/15.

62. Postanowieniem z dnia 1 lutego 2016 r. Trybunał postanowił o rozpoznaniu sprawy C-698/15 w trybie przyśpieszonym przewidzianym w art. 105 § 1 regulaminu postępowania przed Trybunałem.

63. W sprawie C-203/15 swoje uwagi na piśmie przedstawiły Tele2 Sverige, rządy belgijski, czeski, duński, niemiecki, estoński, hiszpański, francuski, węgierski, niderlandzki, szwedzki, Zjednoczonego Królestwa, Irlandia oraz Komisja Europejska.

64. W sprawie C-698/15 uwagi na piśmie przedstawili T. Watson, P. Brice i G. Lewis, Open Rights Group, Privacy International, Law Society of England and Wales, rządy czeski, duński, niemiecki, estoński, francuski, cypryjski, polski, fiński, Zjednoczonego Królestwa, Irlandia oraz Komisja.

65. Postanowieniem Trybunału z dnia 10 marca 2016 r. te dwie sprawy zostały połączone do celów ustnego etapu postępowania i wydania wyroku.

66. Na rozprawie w dniu 12 kwietnia 2016 r. stawili się i wygłosili uwagi przedstawiciele Tele2 Sverige, T. Watson, P. Brice i G. Lewis, Open Rights Group, Privacy International, Law Society of England and Wales, rządy czeski, duński, niemiecki, estoński, hiszpański, francuski, fiński, szwedzki, Zjednoczonego Królestwa, Irlandia oraz Komisja.

V – **Analiza pytań prejudycjalnych**

67. W pierwszym pytaniu postawionym w sprawie C-203/15 sąd odsyłający zwraca się do Trybunału o rozstrzygnięcie, czy w świetle wyroku DRI art. 15 ust. 1 dyrektywy 2002/58, jak również art. 7, 8 i art. 52 ust. 1 karty należy interpretować w ten sposób, że stoją one na przeszkodzie temu, aby państwo członkowskie nałożyło na dostawców ogólny obowiązek zatrzymywania danych, taki jak obowiązki rozpatrywane w postępowaniach głównych, i to niezależnie od ewentualnych gwarancji towarzyszących temu obowiązkowi.

68. W razie gdyby na pytanie to należało udzielić odpowiedzi przeczącej, pytanie drugie postawione w sprawie C-203/15 i pytanie pierwsze postawione w sprawie C-698/15 zmierzają do ustalenia, czy przepisy te powinny być interpretowane w ten sposób, że stoją one na przeszkodzie temu, aby państwo członkowskie nałożyło na dostawców ogólny obowiązek zatrzymywania danych, jeśli obowiązkowi temu nie towarzyszą wszystkie gwarancje ustanowione przez Trybunał w pkt 60–68 wyroku DRI w odniesieniu do dostępu do danych, okresu przechowywania oraz ochrony i bezpieczeństwa danych.

69. Ponieważ te trzy pytania są ściśle ze sobą związane, zbadam je łącznie w dalszej części mojego wywodu.

70. Natomiast pytanie drugie postawione w sprawie C-698/15 wymaga odrębnego potraktowania. Poprzez pytanie to sąd odsyłający zwraca się do Trybunału o rozstrzygnięcie, czy wyrok DRI rozszerzył zakres stosowania art. 7 lub 8 karty w sposób wykraczający poza zakres art. 8 EKPC. W dalszej części wyjaśnię powody, dla których uważam, że pytanie to należy odrzucić jako niedopuszczalne.

71. Uważam, że przed zbadaniem tych pytań stosowne będzie przypomnienie rodzaju danych objętych obowiązkami zatrzymywania rozpatrywanymi w postępowaniach głównych. Zgodnie z ustaleniami dokonanymi przez sądy odsyłające zakres tych obowiązków jest zasadniczo równoważny z zakresem obowiązku określonym w art. 5 dyrektywy 2006/24[8]. Dane dotyczące komunikatów będące przedmiotem obowiązków zatrzymywania mogą być z pewnym uproszczeniem zakwalifikowane do czterech kategorii[9]:

— dane pozwalające ustalić zarówno źródło, jak i odbiorcę komunikatu;

— dane pozwalające ustalić lokalizację zarówno źródła, jak i odbiorcy komunikatu,

— dane dotyczące daty, godziny i czasu trwania komunikatu;

— dane pozwalające na określenie rodzaju połączenia i rodzaju wykorzystywanego narzędzia komunikacji.

72. Treść komunikatów jest wyłączona z ogólnych obowiązków zatrzymywania danych rozpatrywanych w postępowaniach głównych, zgodnie z tym, co zostało przewidziane w art. 5 ust. 2 dyrektywy 2006/24.

A – *W przedmiocie dopuszczalności pytania drugiego postawionego w sprawie C-698/15*

73. W drugim pytaniu postawionym w sprawie C-698/15 zwrócono się do Trybunału o wyjaśnienie, czy wyrok DRI rozszerzył zakres stosowania art. 7 lub 8 karty w sposób wykraczający poza zakres art. 8 EKPC w świetle wykładni tego postanowienia dokonanej przez ETPC.

74. Pytanie to odzwierciedla w szczególności argument podniesiony przez ministra przed sądem odsyłającym, zgodnie z którym orzecznictwo ETPC nie wymaga, po pierwsze, aby dostęp do danych był uzależniony od uprzedniego zezwolenia niezależnego organu ani, po drugie, aby zatrzymywanie i dostęp do tych danych były ograniczone do walki z poważnymi przestępstwami.

8 — Równoważność ta jest zrozumiała, ponieważ owe systemy krajowe miały na celu transpozycję tej obecnie unieważnionej dyrektywy.

9 — Zobacz opis systemów krajowych rozpatrywanych w postępowaniach głównych w pkt 11–13 i 36 niniejszej opinii.

75. Jestem zdania, że pytanie to należy odrzucić jako niedopuszczalne z następujących powodów. Oczywiste jest, że decydujące znaczenie dla rozstrzygnięcia sporów w postępowaniach głównych mają uzasadnienie i rozstrzygnięcie przyjęte przez Trybunał w wyroku DRI. Natomiast okoliczność, że ów wyrok ewentualnie rozszerzył zakres stosowania art. 7 lub 8 karty w sposób wykraczający poza art. 8 EKPC, nie jest sama w sobie istotna dla rozstrzygnięcia tychże sporów.

76. W tym względzie należy przypomnieć, że zgodnie z art. 6 ust. 3 TUE prawa podstawowe zagwarantowane w EKPC stanowią część prawa Unii jako zasady ogólne prawa. Jednak do czasu przystąpienia Unii do tej konwencji nie stanowi ona aktu prawnego formalnie włączonego do porządku prawnego Unii [10].

77. Prawdą jest, że w art. 52 ust. 3 zdanie pierwsze karty ustanowiono regułę wykładni, zgodnie z którą w zakresie, w jakim karta zawiera prawa odpowiadające prawom zagwarantowanym w EKPC, „ich znaczenie i zakres są takie same jak praw przyznanych przez tę konwencję".

78. Jednakże zgodnie z art. 52 ust. 3 zdanie drugie karty „[n]iniejsze postanowienie nie stanowi przeszkody, aby prawo Unii przyznawało szerszą ochronę". W mojej ocenie ze zdania tego wynika, że Trybunał może, jeśli uzna to za niezbędne w kontekście prawa Unii, rozszerzyć zakres stosowania postanowień karty poza zakres odnośnych postanowień EKPC.

79. Tytułem ewentualnym dodam, że art. 8 karty, zinterpretowany przez Trybunał w wyroku DRI, ustanawia prawo, które nie odpowiada żadnemu prawu zagwarantowanemu przez EKPC, a mianowicie prawo do ochrony danych osobowych, co potwierdzają ponadto wyjaśnienia dotyczące art. 52 karty [11]. W konsekwencji zasada wykładni ustanowiona w art. 52 ust. 3 zdanie pierwsze karty nie może w każdym razie znaleźć zastosowania do wykładni art. 8 karty, jak wskazali P. Brice i G. Lewis, Open Rights Group i Privacy International, Law Society of England and Wales, a także rządy czeski, fiński i Irlandia.

80. Z powyższych rozważań wynika, że prawo Unii nie stoi na przeszkodzie temu, by art. 7 i 8 karty przyznawały szerszy zakres ochrony niż przewidziano w EKPC. Zatem okoliczność, że wyrok DRI ewentualnie rozszerzył zakres stosowania tych postanowień karty w sposób wykraczający poza art. 8 EKPC, nie jest sama w sobie istotna dla rozstrzygnięcia sporów w postępowaniach głównych. Sposób rozstrzygnięcia tych sporów zależy głównie od warunków, w jakich ogólny obowiązek zatrzymywania danych może być uznany za zgodny z art. 15 ust. 1 dyrektywy 2002/58, jak również z art. 7, 8 i art. 52 ust. 1 karty, interpretowanych w świetle wyroku DRI, co stanowi właśnie przedmiot trzech pozostałych pytań postawionych w niniejszych sprawach.

81. Zgodnie z utrwalonym orzecznictwem oddalenie wniosku sądu krajowego jest możliwe jedynie wtedy, gdy wykładnia prawa Unii, o którą sąd ten się zwrócił, pozostaje w sposób oczywisty bez związku ze stanem faktycznym czy z przedmiotem sporu w postępowaniu głównym, gdy problem ma charakter hipotetyczny lub gdy Trybunał nie dysponuje informacjami o okolicznościach faktycznych i prawnych niezbędnymi do udzielenia przydatnej odpowiedzi na postawione mu pytania [12].

10 — Opinia 2/13 z dnia 18 grudnia 2014 r., EU:C:2014:2454, pkt 179; wyrok z dnia 15 lutego 2016 r., N., C-601/15 PPU, EU:C:2016:84, pkt 45 i przytoczone tam orzecznictwo.

11 — Zgodnie z art. 6 ust. 1 akapit trzeci TUE i art. 52 ust. 7 karty wyjaśnienia dotyczące karty winny być brane pod uwagę przy jej wykładni (zob. wyroki: z dnia 26 lutego 2013 r., Åkerberg Fransson, C-617/10, EU:C:2013:105, pkt 20; z dnia 15 lutego 2016 r., N., C-601/15 PPU, EU:C:2016:84, pkt 47). Zgodnie z tymi wyjaśnieniami art. 7 karty odpowiada art. 8 EKPC, natomiast art. 8 karty nie odpowiada żadnemu prawu na gruncie EKPC.

12 — Zobacz w szczególności wyroki: z dnia 9 listopada 2010 r., Volker und Markus Schecke i Eifert, C-92/09 i C-93/09, EU:C:2010:662, pkt 40 i przytoczone tam orzecznictwo; a także z dnia 24 kwietnia 2012 r., Kamberaj, C-571/10, EU:C:2012:233, pkt 42 i przytoczone tam orzecznictwo.

82. W niniejszym przypadku, z przedstawionych wyżej powodów, pytanie drugie postawione w sprawie C-698/15 ma, jak mi się wydaje, jedynie charakter teoretyczny, zważywszy, że ewentualna odpowiedź na to pytanie nie pozwoliłaby na wywiedzenie elementów wykładni prawa Unii, które sąd odsyłający mógłby w sposób użyteczny zastosować w świetle tego prawa dla rozstrzygnięcia toczącego się przed nim postępowania [13].

83. W tych okolicznościach uważam, że wspomniane pytanie musi zostać odrzucone jako niedopuszczalne, jak słusznie zauważyli T. Watson, Law Society of England and Wales i rząd czeski.

B – *W przedmiocie zgodności ogólnego obowiązku zatrzymywania danych z systemem ustanowionym w dyrektywie 2002/58*

84. Niniejsza część dotyczy możliwości skorzystania przez państwa członkowskie z prawa przewidzianego w art. 15 ust. 1 dyrektywy 2002/58 w celu nałożenia ogólnego obowiązku zatrzymywania danych. Nie bada się w niej natomiast szczególnych wymogów, które powinny być przestrzegane przez państwa członkowskie chcące skorzystać z tego prawa; wymogi te zostaną obszernie przeanalizowane w dalszej części [14].

85. Open Rights Group i Privacy International podniosły bowiem, że obowiązek taki byłby niezgodny ze zharmonizowanym systemem ustanowionym w dyrektywie 2002/58, i to niezależnie od poszanowania wymogów wynikających z art. 15 ust. 1 dyrektywy 2002/58, ponieważ zniweczyłby istotę praw i systemu ustanowionych w tej dyrektywie.

86. Przed zbadaniem tego argumentu należy sprawdzić, czy ogólny obowiązek zatrzymywania danych mieści się w zakresie stosowania tej dyrektywy.

1. W przedmiocie objęcia ogólnego obowiązku zatrzymywania danych zakresem stosowania dyrektywy 2002/58

87. Żadna ze stron, które przedłożyły Trybunałowi uwagi, nie zakwestionowała faktu, że ogólny obowiązek zatrzymywania danych, taki jak obowiązki rozpatrywane w postępowaniach głównych, wchodzi w zakres pojęcia „przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności [w Unii]" w rozumieniu art. 3 dyrektywy 2002/58.

88. Jednakże rządy czeski, francuski, polski oraz Zjednoczonego Królestwa twierdziły, że ogólny obowiązek zatrzymywania danych jest objęty wyłączeniem przewidzianym w art. 1 ust. 3 dyrektywy 2002/58. Po pierwsze, krajowe przepisy regulujące dostęp do danych i ich wykorzystywanie przez organy policji lub sądy państw członkowskich dotyczą bezpieczeństwa publicznego, obronności lub bezpieczeństwa narodowego, a przynajmniej należą do dziedziny prawa karnego. Po drugie, wyłącznym celem zatrzymywania danych jest umożliwienie owym organom policji lub sądom dostępu do nich i ich wykorzystania. Co za tym idzie, na podstawie przywołanego przepisu obowiązek zatrzymywania danych jest wyłączony z zakresu stosowania tej dyrektywy.

89. Rozumowanie to mnie nie przekonuje, a to z następujących powodów.

13 — Zobacz w szczególności wyrok z dnia 16 września 1982 r., Vlaeminck, 132/81, EU:C:1982:294, pkt 13; postanowienie z dnia 24 marca 2011 r., Abt i in., C-194/10, EU:C:2011:182, pkt 36, 37 i przytoczone tam orzecznictwo; wyrok z dnia 24 października 2013 r., Stoiłow i Ko, C-180/12, EU:C:2013:693, pkt 46 i przytoczone tam orzecznictwo.

14 — Zobacz pkt 126–262 niniejszej opinii.

90. W pierwszej kolejności brzmienie art. 15 ust. 1 dyrektywy 2002/58 potwierdza, że nałożone przez państwa członkowskie obowiązki zatrzymywania są objęte zakresem stosowania tej dyrektywy. Zgodnie z tym przepisem bowiem „[p]aństwa członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie". Wydaje mi się, że co najmniej trudno jest twierdzić, iż obowiązek zatrzymywania jest wyłączony z zakresu stosowania tej dyrektywy, gdyż art. 15 ust. 1 wspomnianej dyrektywy bezpośrednio reguluje prawo do przyjęcia takich obowiązków.

91. W rzeczywistości, jak wskazali T. Watson, P. Brice i G. Lewis, rządy belgijski, duński, niemiecki, fiński oraz Komisja, ogólny obowiązek zatrzymywania danych, taki jak obowiązki rozpatrywane w postępowaniach głównych, stanowi wprowadzenie w życie art. 15 ust. 1 dyrektywy 2002/58.

92. W drugiej kolejności fakt, że przepisy regulujące dostęp mogłyby być objęte wyłączeniem przewidzianym w art. 1 ust. 3 dyrektywy 2002/58 [15], nie oznacza, że jest nim również objęty obowiązek zatrzymywania danych i, co za tym idzie, że znajduje się on poza zakresem stosowania tej dyrektywy.

93. W tym względzie Trybunał miał już okazję wyjaśnić, że działalność wymieniona w art. 3 ust. 2 tiret pierwsze dyrektywy 95/46/WE [16], którego treść ma zakres równoważny art. 1 ust. 3 dyrektywy 2002/58, jest działalnością właściwą państwom lub władzom państwowym, odmienną od dziedzin działalności jednostek [17].

94. Tymczasem, jak wskazała Komisja, obowiązki zatrzymywania rozpatrywane w postępowaniach głównych są nałożone na podmioty prywatne w ramach prywatnej działalności świadczenia usług łączności elektronicznej. Ponadto obowiązki te są wiążące niezależnie od jakichkolwiek wniosków o dostęp ze strony organów policji lub sądów oraz – bardziej ogólnie – jakichkolwiek działań władz państwowych wchodzących w zakres bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego lub prawa karnego.

95. W trzeciej kolejności rozwiązanie przyjęte przez Trybunał w wyroku Irlandia/Parlament i Rada potwierdza, że ogólny obowiązek zatrzymywania danych nie należy do dziedziny prawa karnego [18]. Trybunał orzekł bowiem, że dyrektywa 2006/24, która ustanawiała taki obowiązek, należała nie do dziedziny prawa karnego, lecz do funkcjonowania rynku wewnętrznego, wobec czego art. 95 WE (obecnie art. 114 TFUE) stanowił właściwą podstawę prawną dla przyjęcia tejże dyrektywy.

96. Aby dojść do takiego wniosku, Trybunał stwierdził w szczególności, że przepisy tej dyrektywy były zasadniczo ograniczone do działalności dostawców i nie regulowały dostępu do danych ani ich wykorzystywania przez organy policji lub organy sądowe państw członkowskich [19].Wnioskuję z tego, że przepisy prawa krajowego ustanawiające obowiązek zatrzymywania podobny do obowiązku przewidzianego w dyrektywie 2006/24 również nie należą do dziedziny prawa karnego.

97. Mając na uwadze powyższe rozważania, jestem zdania, że ogólny obowiązek zatrzymywania danych nie jest objęty wyłączeniem, o którym mowa w art. 1 ust. 3 dyrektywy 2002/58 i, co za tym idzie, mieści się w zakresie stosowania tej dyrektywy.

15 — Zobacz pkt 123–125 niniejszej opinii.

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).

17 — Wyrok z dnia 6 listopada 2003 r., Lindqvist, C-101/01, EU:C:2003:596, pkt 43, 44.

18 — Wyrok z dnia 10 lutego 2009 r., C-301/06, EU:C:2009:68.

19 — Wyrok z dnia 10 lutego 2009 r., Irlandia/Parlament i Rada, C-301/06, EU:C:2009:68, pkt 80.

2. W przedmiocie możliwości odstępstwa od systemu ustanowionego przez dyrektywę 2002/58 poprzez ustanowienie ogólnego obowiązku zatrzymywania danych

98. Należy obecnie ustalić, czy ogólny obowiązek zatrzymywania danych jest zgodny z systemem ustanowionym przez dyrektywę 2002/58.

99. Pytanie, jakie pojawia się w tym względzie, dotyczy tego, czy możliwe jest, aby państwo członkowskie skorzystało z prawa przewidzianego w art. 15 ust. 1 dyrektywy 2002/58 w celu nałożenia takiego obowiązku.

100. Przeciw takiej możliwości zostały przedstawione, w szczególności przez Open Rights Group i Privacy International, cztery argumenty.

101. Według pierwszego argumentu przyznanie państwom członkowskim uprawnienia do przyjęcia ogólnego obowiązku zatrzymywania danych podważa cel harmonizacji, który stanowi podstawę przyjęcia dyrektywy 2002/58. Dyrektywa ta przewiduje bowiem, zgodnie z jej art. 1 ust. 1, harmonizację przepisów krajowych wymaganych do zapewnienia równoważnego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do prywatności i poufności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej oraz w celu zapewnienia swobodnego przepływu w Unii tego typu danych oraz urządzeń i usług łączności elektronicznej.

102. Tym samym art. 15 ust. 1 dyrektywy 2002/58 nie można interpretować w ten sposób, że daje on państwom członkowskim uprawnienie do przyjęcia odstępstwa od systemu ustanowionego przez ową dyrektywę o takim zakresie, który pozbawiłby wysiłek na rzecz harmonizacji wszelkiej skuteczności (effet utile).

103. Zgodnie z drugim argumentem brzmienie art. 15 ust. 1 dyrektywy 2002/58 również sprzeciwia się tak szerokiej wykładni uprawnienia państw członkowskich do odstąpienia od systemu ustanowionego przez dyrektywę. Zgodnie bowiem z tym przepisem „[p]aństwa członkowskie mogą uchwalić środki ustawodawcze w celu *ograniczenia zakresu* praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4 i art. 9 tej dyrektywy” (wyróżnienie moje).

104. Tymczasem ogólny obowiązek zatrzymywania danych nie sprowadza się do „ograniczenia zakresu” praw i obowiązków, o których mowa w tym przepisie, lecz prowadzi do zredukowania owych praw i obowiązków do zera. Dotyczy to zatem:

— obowiązku zapewnienia poufności danych o ruchu i obowiązku otrzymania zgody użytkownika na przechowywanie informacji, przewidzianych, odpowiednio, w art. 5 ust. 1 i 3 dyrektywy 2002/58;

— obowiązku usunięcia lub anonimizacji danych o ruchu, ustanowionego w art. 6 ust. 1 tej dyrektywy, oraz

— obowiązku anonimizacji danych dotyczących lokalizacji lub uzyskania zgody użytkownika na przetwarzanie tych danych, ustanowionego w art. 9 ust. 1 rzeczonej dyrektywy.

105. Wydaje mi się, że te dwa pierwsze argumenty muszą zostać oddalone z następujących powodów.

106. Z jednej strony brzmienie art. 15 ust. 1 dyrektywy 2002/58 przewiduje możliwość, by państwa członkowskie przyjęły „środki ustawodawcze przewidujące przechowywanie danych przez określony czas”. To wyraźne odniesienie do obowiązków zatrzymywania danych potwierdza, że obowiązki te nie są same w sobie niezgodne z systemem ustanowionym w dyrektywie 2002/58. O ile takie sformułowanie nie przewiduje wyraźnie możliwości przyjęcia *ogólnego* obowiązku zatrzymywania danych, o tyle należy stwierdzić, że również się temu nie sprzeciwia.

107. Z drugiej strony motyw 11 dyrektywy 2002/58 stanowi, że dyrektywa ta nie zmienia „istniejącej równowagi między prawem do prywatności osoby fizycznej a [przysługującą państwom członkowskim] możliwością podejmowania środków, określonych w art. 15 ust. 1 [tejże] dyrektywy, niezbędnych do ochrony bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając gospodarczy dobrobyt państwa, gdy działania dotyczą zagadnień bezpieczeństwa państwa) i wykonywania prawa karnego". Wskutek tego „[rzeczona] dyrektywa nie wpływa na [przysługujące państwom członkowskim] możliwości zgodnego z prawem przejmowania danych w łączności elektronicznej lub podejmowania innych środków, jeżeli jest to konieczne dla któregokolwiek z tych celów i zgodne z [EKPC]".

108. Moim zdaniem z przytoczonego motywu 11 wynika, że intencją prawodawcy Unii było nie naruszenie przysługującego państwom członkowskim prawa do przyjmowania środków, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, lecz obwarowanie tego prawa pewnymi wymogami, dotyczącymi w szczególności celów i proporcjonalności tych środków. Innymi słowy, ogólny obowiązek zatrzymywania danych nie jest moim zdaniem niezgodny z systemem ustanowionym przez tę dyrektywę, pod warunkiem że spełnia określone warunki.

109. Zgodnie z trzecim argumentem art. 15 ust. 1 dyrektywy 2002/58 powinien, jako odstępstwo od systemu ustanowionego przez dyrektywę, stanowić przedmiot ścisłej wykładni dokonanej na podstawie reguły wykładni wynikającej z utrwalonego orzecznictwa Trybunału. Owa reguła ścisłej wykładni sprzeciwia się interpretowaniu tego przepisu w ten sposób, że uprawnia on do nałożenia ogólnego obowiązku zatrzymywania danych.

110. Sądzę w tym względzie, że prawo przewidziane w art. 15 ust. 1 dyrektywy 2002/58 nie może być zakwalifikowane jako odstępstwo i w konsekwencji, jak słusznie podnosi Komisja, nie może podlegać ścisłej interpretacji. Wydaje mi się bowiem, że trudno jest zakwalifikować owo prawo jako odstępstwo w świetle przywołanego wyżej motywu 11, zgodnie z którym dyrektywa ta nie wpływa na prawo przyjmowania przez państwa członkowskie środków, o których mowa w tym przepisie. Pragnę zauważyć ponadto, że art. 15 tej dyrektywy jest zatytułowany „Stosowanie niektórych przepisów dyrektywy 95/46/WE", natomiast art. 10 tej dyrektywy jest wyraźnie zatytułowany „Wyjątki". Tytuły te utwierdzają mnie w przekonaniu, że prawo przewidziane w art. 15 nie może być zakwalifikowane jako „wyjątek [odstępstwo]".

111. Zgodnie z czwartym i ostatnim argumentem za niezgodnością ogólnego obowiązku zatrzymywania danych z systemem ustanowionym w dyrektywie 2002/58 przemawia dodanie art. 15 ust. 1a tej dyrektywy przy przyjmowaniu dyrektywy 2006/24, unieważnionej wyrokiem DRI. Zgodnie z tym argumentem to właśnie owa niezgodność skłoniła prawodawcę Unii do uznania, że art. 15 ust. 1 dyrektywy 2002/58 nie ma zastosowania do systemu ogólnego zatrzymywania ustanowionego przez dyrektywę 2006/24.

112. Wydaje mi się, że argument ten wynika z błędnego rozumienia zakresu art. 15 ust. 1a dyrektywy 2002/58. Zgodnie z tym przepisem „[art. 15 ust. 1 dyrektywy 2002/58] nie stosuje się do danych, których zatrzymywanie jest wyraźnie wymagane na mocy dyrektywy [2006/24] dla celów określonych w art. 1 ust. 1 tej dyrektywy".

113. Moja wykładnia tego przepisu jest następująca. W odniesieniu do danych, których zatrzymywanie było wymagane na mocy dyrektywy 2006/24 i do celów ustanowionych przez tę dyrektywę, państwa członkowskie utraciły określone w art. 15 ust. 1 dyrektywy 2002/58 prawo do dalszego ograniczenia zakresu praw i obowiązków, o których mowa w tym przepisie, w szczególności poprzez dodatkowe obowiązki w dziedzinie zatrzymywania danych. Innymi słowy, art. 15 ust. 1a przewidywał pełną harmonizację w odniesieniu do danych, których zatrzymywanie było wymagane na mocy dyrektywy 2006/24 i do celów ustanowionych przez tę dyrektywę.

114. Potwierdzenie tej interpretacji znajduję w motywie 12 dyrektywy 2006/24, zgodnie z którym „[a]rtykuł 15 ust. 1 dyrektywy [2002/58] *powinien być stosowany w dalszym ciągu* w odniesieniu do danych, w szczególności [w tym] tych dotyczących nieudanych prób uzyskania połączenia, co do których nie istnieje szczególny wymóg zatrzymywania w świetle niniejszej dyrektywy i *z tego względu nie zostały w niej ujęte*, a także w odniesieniu do [zatrzymywania danych do innych] *celów, które nie zostały uwzględnione w niniejszej dyrektywie* [zwłaszcza do celów sądowych]" (wyróżnienie moje).

115. Tak więc dodanie art. 15 ust. 1a dyrektywy 2002/58 świadczy nie o niezgodności ogólnego obowiązku zatrzymywania danych z systemem ustanowionym przez tę dyrektywę, lecz o woli prawodawcy Unii, aby przy przyjęciu dyrektywy 2006/24 dokonać pełnej harmonizacji.

116. Mając na uwadze powyższe rozważania, uważam, że ogólny obowiązek zatrzymywania danych jest zgodny z systemem ustanowionym przez dyrektywę 2002/58 i co za tym idzie, państwo członkowskie może skorzystać z prawa przewidzianego w art. 15 ust. 1 tej dyrektywy w celu nałożenia takiego obowiązku [20]. Prawo to należy jednak uzależnić od spełnienia restrykcyjnych wymogów wynikających nie tylko z tego przepisu, lecz również z odpowiednich postanowień karty interpretowanych w świetle wyroku DRI, które zostaną zbadane w dalszej części [21].

C – *W przedmiocie możliwości stosowania karty do ogólnego obowiązku zatrzymywania danych*

117. Przed zbadaniem treści wymogów, jakie karta przewiduje w związku z art. 15 ust. 1 dyrektywy 2002/58, w przypadku gdy państwo postanawia wprowadzić ogólny obowiązek zatrzymywania danych, należy sprawdzić, czy karta ma zastosowanie do takiego obowiązku.

118. Możliwość zastosowania karty do ogólnego obowiązku zatrzymywania danych zależy zasadniczo od stosowalności dyrektywy 2002/58 do takiego obowiązku.

119. Zgodnie bowiem z art. 51 ust. 1 zdanie pierwsze karty „postanowienia [karty] mają zastosowanie […] do państw członkowskich wyłącznie w zakresie, w jakim stosują one prawo Unii". W wyjaśnieniach do art. 51 karty odsyłano w tym względzie do orzecznictwa Trybunału, zgodnie z którym wymóg poszanowania praw podstawowych określonych w kontekście Unii jest wiążący dla państw członkowskich wyłącznie wtedy, gdy działają one w zakresie stosowania prawa Unii [22].

120. Rządy czeski, francuski, polski i Zjednoczonego Królestwa, które zakwestionowały możliwość stosowania dyrektywy 2002/58 do ogólnego obowiązku zatrzymywania danych [23], stwierdziły również, że karta nie ma zastosowania do takiego obowiązku.

121. Wskazałem już powody, dla których uważam, że ogólny obowiązek zatrzymywania danych stanowi wykonanie prawa przewidzianego w art. 15 ust. 1 dyrektywy 2002/58 [24].

20 — Biorąc pod uwagę, że dyrektywę 2002/58 można uznać za lex specialis w stosunku do dyrektywy 95/46 (zob. w tym względzie art. 1 ust. 2 dyrektywy 2002/58), nie uważam za konieczne, by zbadać zgodność ogólnego obowiązku zatrzymywania danych z systemem ustanowionym przez dyrektywę 95/46, która zresztą nie stanowi przedmiotu pytań skierowanych do Trybunału. W trosce o pełność opinii chciałbym jednak uściślić, że brzmienie art. 13 ust. 1 dyrektywy 95/46 daje większą swobodę państwom członkowskim, niż proponuje to art. 15 ust. 1 dyrektywy 2002/58, który określa jej zakres w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej. Ponieważ prawo przewidziane w art. 15 ust. 1 dyrektywy 2002/58 pozwala na przyjęcie przez państwo członkowskie ogólnego obowiązku zatrzymywania danych, wnioskuję stąd, że art. 13 ust. 1 dyrektywy 95/46 również na to pozwala.

21 — Zobacz pkt 126–262 niniejszej opinii.

22 — Z utrwalonego orzecznictwa Trybunału wynika bowiem, że prawa podstawowe chronione w porządku prawnym Unii znajdują zastosowanie we wszystkich sytuacjach podlegających prawu Unii, ale nie poza takimi sytuacjami. Z tego względu Trybunał przypomniał już, że nie jest władny oceniać zgodności z kartą przepisów krajowych, które nie mieszczą się w zakresie zastosowania prawa Unii. Natomiast jeżeli przepisy takie wchodzą w zakres zastosowania tego prawa, Trybunał, rozpatrując pytanie prejudycjalne, powinien udzielić wszelkich wyjaśnień interpretacyjnych koniecznych do oceny przez sąd krajowy zgodności tych przepisów z prawami podstawowymi, których ochronę zapewnia (zob. wyrok z dnia 26 lutego 2013 r., Åkerberg Fransson, C-617/10, EU:C:2013:105, pkt 19 i przytoczone tam orzecznictwo).

23 — Zobacz pkt 88 niniejszej opinii.

24 — Zobacz pkt 90–97 niniejszej opinii.

122. W konsekwencji jestem zdania, że postanowienia karty mają zastosowanie do środków krajowych ustanawiających taki obowiązek, zgodnie z art. 51 ust. 1 karty, jak podnieśli T. Watson, P. Brice i G. Lewis, Open Rights Group i Privacy International, rządy duński, niemiecki, fiński oraz Komisja [25].

123. Wniosku tego nie podważa fakt, że krajowe przepisy regulujące dostęp do zatrzymanych danych nie mieszczą się, jako takie, w dziedzinie stosowania karty.

124. Prawdą jest, że w zakresie, w jakim dotyczą one „działalności państwa w dziedzinie prawa karnego", przepisy krajowe regulujące dostęp do zatrzymywanych danych przez organy policji lub sądy w celu walki z poważnymi przestępstwami podlegają moim zdaniem wyłączeniu przewidzianemu w art. 1 ust. 3 dyrektywy 2002/58 [26]. W konsekwencji takie przepisy krajowe nie stanowią stosowania prawa Unii, wobec czego karta nie ma do nich zastosowania.

125. Niemniej jednak przyczyną ustanowienia obowiązku zatrzymywania danych jest umożliwienie organom ścigania dostępu do zatrzymanych danych, wobec czego problematyka związana z ich ochroną i dostępem do nich nie jest zagadnieniem całkowicie odrębnym. Jak słusznie zauważyła Komisja, przepisy regulujące dostęp mają decydujące znaczenie dla oceny zgodności z kartą przepisów ustanawiających ogólny obowiązek zatrzymywania danych, które wprowadzają w życie art. 15 ust. 1 dyrektywy 2002/58. Ściślej rzecz ujmując, przepisy regulujące dostęp powinny być brane pod uwagę przy ocenie konieczności i proporcjonalności takiego obowiązku [27].

D – *W przedmiocie zgodności ogólnego obowiązku zatrzymywania danych z wymogami ustanowionymi w art. 15 ust. 1 dyrektywy 2002/58, a także w art. 7, 8 i art. 52 ust. 1 karty*

126. Pozostaje mi teraz zająć się trudną kwestią zgodności ogólnego obowiązku zatrzymywania danych z wymogami ustanowionymi w art. 15 ust. 1 dyrektywy 2002/58, a także w art. 7, 8 i art. 52 ust. 1 karty rozpatrywanych w związku z wyrokiem DRI. Pytanie to dotyczy, w sposób bardziej ogólny, konieczności dostosowania przepisów regulujących możliwości prowadzenia przez państwa niejawnych obserwacji, których liczba znacznie wzrosła dzięki obecnemu postępowi technologicznemu [28].

127. Pierwszy etap analizy polega w tym kontekście na stwierdzeniu ingerencji w prawa ustanowione przez dyrektywę 2002/58 i w prawa podstawowe ustanowione w art. 7 i 8 karty.

128. Obowiązek taki stanowi bowiem poważną ingerencję w prawo do poszanowania życia prywatnego ustanowione w art. 7 karty i w prawo do ochrony danych osobowych zagwarantowane w art. 8 karty. Nie sądzę, abym musiał rozwodzić się nad ustaleniem owej ingerencji, która została wyraźnie stwierdzona przez Trybunał w pkt 32–37 wyroku DRI [29]. Tym samym ogólny obowiązek zatrzymywania danych stanowi ingerencję w szereg praw ustanowionych w dyrektywie 2002/58 [30].

25 — Ściślej rzecz ujmując, art. 51 ust. 1 zdanie drugie karty stanowi, że państwa członkowskie są zobowiązane do poszanowania praw gwarantowanych przez kartę w zakresie, w jakim państwa te stosują prawo Unii.

26 — W przedmiocie zakresu tego wykluczenia zob. pkt 90–97 niniejszej opinii.

27 — Zobacz pkt 185–262 niniejszej opinii.

28 — Zobacz w szczególności Rada Praw Człowieka ONZ, sprawozdanie specjalnego sprawozdawcy ds. wolności opinii i wypowiedzi, 17 kwietnia 2013 r., A/HRC/23/40, nr 33: „Postęp technologiczny umożliwia państwom prowadzenie działań w zakresie niejawnej obserwacji, które nie są już ograniczone kryteriami skali lub czasu trwania […]. W konsekwencji państwo posiada obecnie jeszcze większą gamę środków do równoczesnego prowadzenia szeregu działań w zakresie niejawnej obserwacji, naruszających życie prywatne, ukierunkowanych i na dużą skalę […]". Zobacz również nr 50: „Mówiąc w sposób ogólny, ustawodawstwo nie dotrzymało kroku zmianom technologicznym. W większości państw normy prawne albo w ogóle nie istnieją, albo są nieodpowiednie do tego, aby sprostać nowoczesnym warunkom niejawnej obserwacji komunikatów […]" [tłumaczenie nieoficjalne].

29 — Powrócę jednak do szczególnych zagrożeń, jakie wynikają z tworzenia baz danych o takiej wielkości w kontekście wymogu proporcjonalności, w demokratycznym społeczeństwie, ogólnego obowiązku zatrzymywania danych, takiego jak obowiązki rozpatrywane w postępowaniach głównych: zob. pkt 252–261 niniejszej opinii.

30 — Zobacz w tym względzie argument podniesiony przez Open Rights Group i Privacy International, streszczony w pkt 104 niniejszej opinii.

129. Drugi etap analizy polega na ustaleniu, czy i na jakich warunkach owa poważna ingerencja w prawa ustanowione w dyrektywie 2002/58, jak również w prawa podstawowe ustanowione w art. 7 i 8 karty, może być uzasadniona.

130. Dwa przepisy określają warunki, jakie muszą zostać spełnione, aby ta podwójna ingerencja była uzasadniona: art. 15 ust. 1 dyrektywy 2002/58, który normuje prawo państw członkowskich do ograniczenia zakresu pewnych praw określonych w tej dyrektywie, i art. 52 ust. 1 karty, interpretowany w związku z wyrokiem DRI, który normuje wszelkie ograniczenia w korzystaniu z praw ustanowionych przez kartę.

131. Chciałbym podkreślić, że wymogi te są *kumulatywne*. Przestrzeganie wymogów ustanowionych w art. 15 ust. 1 dyrektywy 2002/58 nie oznacza bowiem samo w sobie, że spełnione są wymogi przewidziane w art. 52 ust. 1 karty, i odwrotnie [31]. W konsekwencji, jak podkreśliło Law Society of England and Wales [32], ogólny obowiązek zatrzymywania danych może zostać uznany za zgodny z prawem Unii, jedynie jeśli jednocześnie spełnia wymogi określone w art. 15 ust. 1 dyrektywy 2002/58 i określone w art. 52 ust. 1 karty.

132. Te dwa przepisy łącznie ustanawiają sześć wymogów, które muszą zostać spełnione, aby ingerencja spowodowana ogólnym obowiązkiem zatrzymywania danych była uzasadniona:

— obowiązek zatrzymywania danych musi być oparty na podstawie prawnej;

— musi szanować istotę praw ustanowionych przez kartę;

— musi dążyć do osiągnięcia celu interesu ogólnego;

— musi być właściwy do realizacji tego celu;

— musi być konieczny do realizacji tego celu;

— musi być, w ramach społeczeństwa demokratycznego, proporcjonalny do osiągnięcia tego celu.

133. Wiele z tych przesłanek zostało już przywołanych przez Trybunał w wyroku DRI. W trosce o zapewnienie jasności i biorąc pod uwagę specyfikę niniejszych spraw w porównaniu do sprawy DRI, pragnę jednak powrócić do każdej z nich i zbadać w sposób bardziej szczegółowy wymogi odnoszące się do podstawy prawnej, do koniecznego oraz proporcjonalnego charakteru ogólnego obowiązku zatrzymywania danych w społeczeństwie demokratycznym.

1. W przedmiocie wymogu istnienia podstawy prawnej w prawie krajowym

134. Zarówno art. 52 ust. 1 karty, jak i art. 15 ust. 1 dyrektywy 2002/58 określają wymogi w odniesieniu do podstawy prawnej, z której państwo członkowskie powinno skorzystać w celu nałożenia ogólnego obowiązku zatrzymywania danych.

31 — Potwierdzenie owego kumulatywnego charakteru znajduję w ostatnim zdaniu art. 15 ust. 1 dyrektywy 2002/58, zgodnie z którym „wszystkie środki określone w [tym] ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 TUE". Na mocy art. 6 ust. 1 TUE „Unia uznaje prawa, wolności i zasady określone w [karcie], która ma taką samą moc prawną jak traktaty".

32 — Logiczną konsekwencją owego charakteru kumulatywnego jest to, że ponieważ wymogi ustanowione przez te dwa przepisy częściowo się pokrywają, należy zastosować wymóg najbardziej surowy lub, innymi słowy, wymóg najszerzej chroniący rozpatrywane prawa.

135. W pierwszej kolejności każde ograniczenie w korzystaniu z praw uznanych w karcie musi być „przewidziane ustawą" zgodnie z jej art. 52 ust. 1. Chciałbym wyjaśnić, że wymóg ten nie został formalnie zbadany przez Trybunał w wyroku DRI, który dotyczył ingerencji przewidzianej w dyrektywie.

136. Do czasu niedawnego wyroku WebMindLicenses [33] Trybunał nigdy nie wypowiedział się na temat dokładnego zakresu tego wymogu, i to nawet jeżeli wyraźnie stwierdził, że wymóg ten był [34] albo nie był [35] spełniony. W pkt 81 tego wyroku trzecia izba Trybunału orzekła, co następuje:

„W tym względzie należy podkreślić, że wymóg, aby wszelkie ograniczenia w korzystaniu z tego prawa były przewidziane ustawą, oznacza, że podstawa prawna umożliwiająca wykorzystanie dowodów wskazanych w poprzednim punkcie przez organ podatkowy musi być wystarczająco jasna i precyzyjna oraz że w zakresie, w jakim definiuje ona sama zakres ograniczenia w wykonywaniu prawa zagwarantowanego w art. 7 karty, zapewnia ona pewną ochronę przed ewentualnymi arbitralnymi działaniami tego organu (zob. w szczególności wyroki ETPC: z dnia 2 sierpnia 1984 r. w sprawie Malone przeciwko Zjednoczonemu Królestwu, seria A, nr 82, § 67; a także z dnia 12 stycznia 2010 r. w sprawie Gillan i Quinton przeciwko Zjednoczonemu Królestwu, nr 4158/05, § 77, ETPC 2010)".

137. Chciałbym zaproponować wielkiej izbie Trybunału, aby w niniejszych sprawach potwierdziła tę interpretację, z następujących powodów.

138. Jak słusznie zauważa rzecznik generalny P. Cruz Villalón w opinii przedstawionej w sprawie Scarlet Extended [36], ETPC wypracował bogate orzecznictwo dotyczące tego wymogu w kontekście EKPC, które charakteryzuje się materialnym, a nie formalnym pojmowaniem terminu „ustawy" [37].

139. Zgodnie z tym orzecznictwem wyrażenie „przewidziane ustawą" oznacza, że podstawa prawna jest wystarczająco przystępna i przewidywalna, czyli przedstawiona na tyle dokładnie, aby umożliwić jednostce dostosowanie jej postępowania, w razie potrzeby po zasięgnięciu fachowej porady. Rzeczona podstawa prawna powinna również oferować odpowiednią ochronę przed arbitralnością i w konsekwencji określać w sposób wystarczająco jasny zakres i warunki wykonywania uprawnienia powierzonego właściwym organom (zasada rządów prawa) [38].

140. Otóż moim zdaniem wyrażeniu „przewidziane ustawą", o którym mowa w art. 52 ust. 1 karty, trzeba przypisać zakres podobny do zakresu tego pojęcia w kontekście EKPC, a to z następujących powodów.

33 — Wyrok z dnia 17 grudnia 2015 r., C-419/14, EU:C:2015:832.

34 — Zobacz w szczególności wyroki: z dnia 17 października 2013 r., Schwarz, C-291/12, EU:C:2013:670, pkt 35 (ingerencja przewidziana przez rozporządzenie europejskie); z dnia 27 maja 2014 r., Spasic, C-129/14 PPU, EU:C:2014:586, pkt 57 (ingerencja przewidziana w Konwencji wykonawczej do układu z Schengen z dnia 14 czerwca 1985 r. między rządami państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach, podpisana w Schengen w dniu 19 czerwca 1990 r., która weszła w życie w dniu 26 marca 1995 r.); z dnia 6 października 2015 r., Delvigne, C-650/13, EU:C:2015:648, pkt 47 (ingerencja przewidziana ordynacją wyborczą i francuskim kodeksem karnym); z dnia 17 grudnia 2015 r., Neptune Distribution C-157/14, EU:C:2015:823, pkt 69 (ingerencja przewidziana przez europejskie rozporządzenie i dyrektywę).

35 — Wyrok z dnia 1 lipca 2010 r., Knauf Gips/Komisja, C-407/08 P, EU:C:2010:389, pkt 87–92 (ingerencja pozbawiona podstawy prawnej).

36 — C-70/10, EU:C:2011:255, pkt 94–100.

37 — Zobacz w szczególności wyrok ETPC z dnia 14 września 2010 r. w sprawie Sanoma Uitgevers B.V. przeciwko Niderlandom, CE:ECHR:2010:0914JUD003822403, § 83.

38 — Zobacz w szczególności wyroki ETPC: z dnia 26 marca 1987 r. w sprawie Leander przeciwko Szwecji, CE:ECHR:1987:0326JUD000924881, §§ 50, 51; z dnia 26 października 2000 r. w sprawie Hassan i Tchaouch przeciwko Bułgarii, CE:ECHR:2000:1026JUD003098596, § 84; z dnia 4 grudnia 2008 r. w sprawie S. i Marper przeciwko Zjednoczonemu Królestwu, CE:ECHR:2008:1204JUD003056204, § 95; z dnia 14 września 2010 r. w sprawie Sanoma Uitgevers B.V. przeciwko Niderlandom, CE:ECHR:2010:0914JUD003822403, §§ 81–83; z dnia 31 marca 2016 r. w sprawie Stoyanov i in. przeciwko Bułgarii, CE:ECHR:2016:0331JUD005538810, §§ 124–126.

141. Po pierwsze, zgodnie z art. 53 karty i wyjaśnieniami dotyczącymi tego artykułu poziom ochrony zapewniany na gruncie karty nigdy nie może być niższy od zagwarantowanego w EKPC. Ów zakaz zejścia poniżej „progu EKPC" oznacza, że przyjmowana przez Trybunał wykładnia wyrażenia „przewidziane ustawą", o którym mowa w art. 52 ust. 1 karty, powinna być przynajmniej tak ścisła, jak ta przyjęta przez ETPC w kontekście EKPC [39].

142. Po drugie, zważywszy na horyzontalny charakter tego wymogu, który może mieć zastosowanie do wielu rodzajów ingerencji zarówno w kontekście karty, jak i na gruncie EKPC [40], niewłaściwe byłoby poddawanie państw członkowskich różnym kryteriom w zależności od tego, czy ingerencja rozpatrywana jest w świetle jednego czy drugiego z tych instrumentów [41].

143. W związku z tym uważam, że – jak podnoszą rząd estoński oraz Komisja – zawarte w art. 52 ust. 1 karty wyrażenie „przewidziane ustawą", należy interpretować w świetle orzecznictwa ETPC streszczonego w pkt 139 niniejszej opinii, w ten sposób, że ogólny obowiązek zatrzymywania danych, taki jak obowiązki rozpatrywane w postępowaniach głównych, musi zostać ustanowiony w oparciu o podstawę prawną, która, po pierwsze, jest wystarczająco przystępna i przewidywalna, a po drugie, zapewnia odpowiednią ochronę przed arbitralnością.

144. W drugiej kolejności należy określić treść wymogów ustanowionych w art. 15 ust. 1 dyrektywy 2002/58 w odniesieniu do podstawy prawnej, która powinna zostać wykorzystana przez państwo członkowskie pragnące skorzystać z prawa przysługującego na mocy tego przepisu.

145. Wydaje się, iż należy zaznaczyć w tym względzie istnienie rozbieżności między wersjami językowymi pierwszego zdania tego przepisu.

146. W wersjach angielskiej („legislative measures"), francuskiej („mesures législatives"), włoskiej („disposizioni legislative"), portugalskiej („medidas legislativas"), rumuńskiej („măsuri legislative") i w szwedzkiej („genom lagstiftning vidta åtgärder") art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 wymaga moim zdaniem przyjęcia środków pochodzących od władzy ustawodawczej.

147. Natomiast wersje duńska („retsforskrifter"), niemiecka („Rechtsvorschriften"), niderlandzka („wettelijke maatregele") i hiszpańska („medidas legales") tego zdania mogą być interpretowane jako wymagające przyjęcia albo środków pochodzących od władzy ustawodawczej, albo przepisów wykonawczych wydanych przez władzę wykonawczą.

148. Zgodnie z utrwalonym orzecznictwem konieczność jednolitego stosowania, a w związku z tym jednolitej wykładni aktu Unii wyklucza jego rozpatrywanie w jednej – w oderwaniu od innych – wersji, ale wymaga ustalenia wykładni w zależności zarówno od rzeczywistej woli autora tego aktu, jak i przyświecającego mu celu, a zwłaszcza w świetle wszystkich innych oficjalnych wersji językowych. W wypadku wystąpienia rozbieżności między nimi sporny przepis należy interpretować z uwzględnieniem ogólnej systematyki i celu uregulowania, którego przepis ten jest częścią [42].

39 — Ściślej rzecz ujmując, Trybunał nie może moim zdaniem przyjąć takiej wykładni tego wymogu, która byłaby bardziej permisywna niż wykładnia przyjęta przez ETPC, jako że prowadziłoby to do umożliwienia szeregu ingerencji idących dalej niż ingerencja, która wynikałaby z wykładni tego wymogu przez ETPC.

40 — Wyrażenie „przewidziane ustawą" jest użyte w art. 8 ust. 2 (prawo do poszanowania życia prywatnego i rodzinnego), art. 9 ust. 2 (wolność myśli, sumienia i wyznania), art. 10 ust. 2 (wolność wyrażania opinii) i art. 11 ust. 2 (wolność zgromadzeń i stowarzyszenia się) EKPC. Zgodnie z kartą art. 52 ust. 1 stosuje się do wszelkich ograniczeń w korzystaniu z ustanowionych w niej praw, o ile ograniczenie jest w ogóle dopuszczalne.

41 — Zobacz podobnie S. Peers, Article 52 – Scope of guaranteed rights, w: S. Peers i in., *The EU Charter of Fundamental Rights: a Commentary*, Oxford, OUP, 2014, nr 52.39.

42 — Zobacz w szczególności wyroki: z dnia 30 maja 2013 r., Asbeek Brusse i de Man Garabito, C-488/11, EU:C:2013:341, pkt 26; z dnia 24 czerwca 2015 r., Hotel Sava Rogaška, C-207/14, EU:C:2015:414, pkt 26; z dnia 26 lutego 2015 r., Christie's France, C-41/14, EU:C:2015:119, pkt 26.

149. W niniejszym przypadku art. 15 ust. 1 dyrektywy 2002/58 reguluje prawa państw członkowskich do wprowadzenia odstępstw od praw podstawowych ustanowionych w art. 7 i 8 karty, których ochrona jest realizowana przez tę dyrektywę. Uważam zatem za konieczne, aby interpretować wymóg podstawy prawnej nałożony przez art. 15 ust. 1 dyrektywy 2002/58 w świetle karty, a w szczególności jej art. 52 ust. 1.

150. Tak więc „środki" wymagane przez art. 15 ust. 1 dyrektywy 2002/58 muszą bezwzględnie posiadać cechy przystępności, przewidywalności i odpowiedniej ochrony przed arbitralnością, przytoczone w pkt 143 niniejszej opinii. Jak wynika w szczególności z tych cech, a zwłaszcza z wymogu odpowiedniej ochrony przed arbitralnością, środki te powinny być *wiążące* dla władz krajowych, które otrzymują prawo dostępu do zatrzymanych danych. W szczególności nie byłoby wystarczające ustanowienie gwarancji dotyczących dostępu do tych danych w wewnętrznych kodeksach lub wytycznych, nieposiadających takiego wiążącego charakteru, jak słusznie podkreśliło to Law Society of England and Wales.

151. Ponadto wyrażenie „państwa członkowskie mogą uchwalić środki", które jest wspólne dla wszystkich wersji językowych art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58, wyklucza, jak mi się wydaje, możliwość, aby orzecznictwo krajowe, nawet utrwalone, mogło stanowić podstawę prawną wystarczającą do wdrożenia tego przepisu. Podkreślam, że w tym zakresie przepis ten wykracza poza wymogi wynikające z orzecznictwa ETPC[43].

152. Dodam, że wydaje mi się pożądane, aby ze względu na wagę ingerencji, jaką stanowi ogólny obowiązek zatrzymywania danych, w prawa podstawowe ustanowione w art. 7 i 8 karty, istota spornego systemu, a w szczególności istota gwarancji związanych z tym obowiązkiem, została określona w środku przyjętym przez władzę ustawodawczą, przy czym do władzy wykonawczej należy dokładne określenie warunków jego wykonywania.

153. Mając na uwadze powyższe rozważania, jestem zdania, że art. 15 ust. 1 dyrektywy 2002/58 i art. 52 ust. 1 karty należy interpretować w ten sposób, iż system ustanawiający ogólny obowiązek zatrzymywania danych, taki jak obowiązki rozpatrywane w postępowaniach głównych, powinien zostać ustanowiony na podstawie przepisów ustawowych lub wykonawczych odznaczających się cechami przystępności, przewidywalności i odpowiedniej ochrony przed arbitralnością.

154. Ustalenie poszanowania tego wymogu należy do sądów odsyłających ze względu na ich uprzywilejowaną pozycję w zakresie oceny swojego systemu krajowego.

2. W przedmiocie poszanowania istoty praw uznanych w art. 7 i 8 karty

155. Zgodnie z art. 52 ust. 1 wszelkie ograniczenia w korzystaniu z praw uznanych w karcie muszą „szanować istotę tych praw"[44]. Aspekt ten, który został zbadany przez Trybunał w pkt 39 i 40 wyroku DRI w kontekście dyrektywy 2006/24, nie wydaje mi się stanowić szczególnego problemu w ramach niniejszych spraw, jak podniosły rząd hiszpański, Irlandia oraz Komisja.

156. W pkt 39 wyroku DRI Trybunał orzekł, że dyrektywa ta nie naruszała istoty prawa do poszanowania życia prywatnego i innych praw zawartych w art. 7 karty, ponieważ nie pozwalała na zapoznanie się z samą treścią komunikatów elektronicznych.

43 — Zobacz w szczególności wyrok ETPC z dnia 14 września 2010 r. w sprawie Sanoma Uitgevers B.V. przeciwko Niderlandom, CE:ECHR:2010:0914JUD003822403, § 83: „[pojęcie »ustawy« zawarte w art. 8–11 EKPC obejmuje] zarówno »prawo stanowione«, obejmujące też przepisy o randze niższej niż ustawa, oraz akty wykonawcze przyjęte przez samorząd zawodowy na podstawie delegacji ustawowej w ramach jego niezależnych uprawnień normatywnych, jak i »prawo niepisane«. Termin »ustawa« należy rozumieć w ten sposób, że obejmuje on akty prawa stanowionego oraz »prawo wypracowane« przez sądy" [tłumaczenie nieoficjalne].

44 — Tego rodzaju wymóg nie wynika ani z brzmienia art. 15 ust. 1 dyrektywy 2002/58, ani z systematyki tej dyrektywy, ze względów przedstawionych w pkt 99–116 niniejszej opinii.

157. Ocenę tę według mnie można zastosować do systemów krajowych będących przedmiotem sporu w postępowaniach głównych, zważywszy, że systemy te również nie pozwalają na zapoznanie się z samą treścią komunikatów elektronicznych [45].

158. W pkt 40 wyroku DRI Trybunał uznał, że dyrektywa 2006/24 nie narusza zasadniczej istoty ustanowionego w art. 8 karty prawa podstawowego do ochrony danych osobowych w świetle zasad ochrony i bezpieczeństwa danych, które powinny być przestrzegane przez dostawców na mocy art. 7 tej dyrektywy, przy czym państwa członkowskie mają obowiązek zapewnienia właściwych środków technicznych i organizacyjnych w celu ochrony danych przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą.

159. Również w tym przypadku uważam, że ocenę tę można zastosować także do systemów krajowych będących przedmiotem sporu w postępowaniach głównych, zważywszy, że przewidują one, jak mi się wydaje, gwarancje porównywalne odnośnie do ochrony i bezpieczeństwa danych zatrzymanych przez dostawców, gdyż takie gwarancje powinny umożliwiać skuteczną ochronę danych osobowych przed ryzykiem nadużyć i przed jakimkolwiek bezprawnym dostępem do tych danych i korzystaniem z nich [46].

160. Do sądu odsyłającego należy jednak ustalenie, czy przepisy krajowe będące przedmiotem postępowań głównych rzeczywiście zachowują, w świetle powyższych rozważań, istotę praw uznanych w art. 7 i 8 karty.

3. W przedmiocie istnienia uznanego przez Unię celu interesu ogólnego, który może uzasadniać ogólny obowiązek zatrzymywania danych

161. Zarówno art. 15 ust. 1 dyrektywy 2002/58, jak i art. 52 ust. 1 karty wymagają, aby wszelka ingerencja w prawa w nich ustanowione służyła celowi interesu ogólnego.

162. W pkt 41–44 wyroku DRI Trybunał orzekł, po pierwsze, że ogólny obowiązek zatrzymywania danych nałożony przez dyrektywę 2006/24 przyczynia się do „walki z poważną przestępczością, co w ostatecznym rozrachunku przekłada się na zapewnienie bezpieczeństwa publicznego", a po drugie, że walka ta stanowi cel interesu ogólnego Unii.

163. Z orzecznictwa Trybunału wynika bowiem, że walka z terroryzmem międzynarodowym w celu utrzymania międzynarodowego pokoju i bezpieczeństwa stanowi cel interesu ogólnego Unii. Podobnie rzecz ma się w przypadku walki z poważną przestępczością, w celu zapewnienia bezpieczeństwa publicznego. Należy też w tym względzie zauważyć, że art. 6 karty gwarantuje każdemu prawo nie tylko do wolności, ale też do bezpieczeństwa osobistego [47].

164. Ocena ta ma zastosowanie do ogólnych obowiązków zatrzymywania danych będących przedmiotem sporu w postępowaniach głównych, które mogą być uzasadnione celem walki z poważnymi przestępstwami.

165. Niemniej jednak, zważywszy na niektóre argumenty przedstawione Trybunałowi, należy ustalić, czy taki obowiązek może być uzasadniony celem interesu ogólnego innym niż walka z poważnymi przestępstwami.

166. W tym względzie treść art. 52 ust. 1 karty odwołuje się w sposób ogólny do „celów interesu ogólnego uznawanych przez Unię" i „potrzeb ochrony praw i wolności innych osób".

45 — Zobacz opis systemów krajowych będących przedmiotem postępowań głównych, w szczególności w pkt 13 i 36 niniejszej opinii.

46 — Wyrok DRI, pkt 54. Zobacz opis systemów krajowych rozpatrywanych w postępowaniach głównych w pkt 29–33, 45 i 46 niniejszej opinii.

47 — Wyrok DRI, pkt 42 i przytoczone tam orzecznictwo.

167. Brzmienie art. 15 ust. 1 dyrektywy 2002/58 jest bardziej precyzyjne co do celów mogących uzasadniać ingerencję w prawa ustanowione w tej dyrektywie. Zgodnie z tym przepisem sporne środki powinny bowiem przyczyniać się 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]".

168. Ponadto w wyroku Promusicae [48] Trybunał orzekł, że przepis ten należy interpretować w świetle art. 13 ust. 1 dyrektywy 95/46, która dopuszcza odstępstwa od praw ustanowionych w tej dyrektywie, jeżeli są uzasadnione dla „zabezpieczenia praw i wolności innych osób". W konsekwencji Trybunał orzekł, że na podstawie art. 15 ust. 1 dyrektywy 2002/58 państwom członkowskim przysługiwało prawo ustanowienia spoczywającego na dostawcy obowiązku ujawnienia danych osobowych w celu ustalenia, w ramach postępowania cywilnego, istnienia naruszenia praw autorskich dotyczącego nagrań muzycznych i audiowizualnych.

169. Rząd Zjednoczonego Królestwa oparł na tym wyroku argument, że ogólny obowiązek zatrzymywania danych może być uzasadniony każdym celem, określonym albo w art. 15 ust. 1 dyrektywy 2002/58, albo w art. 13 ust. 1 dyrektywy 95/46. Zdaniem tego rządu obowiązek taki może być uzasadniony użytecznością zatrzymanych danych w walce z przestępstwami „pospolitymi" (w przeciwieństwie do „poważnych") lub nawet w związku z postępowaniami niemającymi charakteru karnego, lecz pozostającymi w związku z celami, o których mowa w tych przepisach.

170. Argument ten nie przekonuje mnie z następujących powodów.

171. W pierwszej kolejności, jak słusznie podkreślili T. Watson oraz Open Rights Group i Privacy International, podejście przyjęte przez Trybunał w wyroku Promusicae [49] nie ma zastosowania do niniejszej sprawy, ponieważ wyrok ten dotyczył złożonego przez stowarzyszenie właścicieli praw autorskich wniosku o udzielenie dostępu do danych zatrzymanych z własnej inicjatywy przez dostawcę, to jest przedsiębiorstwo Telefónica de España. Innymi słowy, wyrok ten nie dotyczył celów, które mogłyby uzasadniać poważne ingerencje w prawa podstawowe, jakie pociąga za sobą ogólny obowiązek zatrzymywania danych, taki jak obowiązki rozpatrywane w postępowaniach głównych.

172. W drugiej kolejności uważam, że wymóg proporcjonalności w społeczeństwie demokratycznym wyklucza, aby walka z przestępstwami pospolitymi lub sprawny przebieg postępowań niemających charakteru karnego mógł uzasadniać ogólny obowiązek zatrzymywania danych. Znaczne zagrożenia, jakie rodzi taki obowiązek, są bowiem nadmierne w stosunku do korzyści, jakie przyniósłby on w walce z pospolitymi przestępstwami lub też w kontekście postępowań niemających charakteru karnego [50].

173. Mając na uwadze powyższe rozważania, jestem zdania, że art. 15 ust. 1 dyrektywy 2002/58 i art. 52 ust. 1 karty należy interpretować w ten sposób, że walka z poważnymi przestępstwami stanowi cel interesu ogólnego, który może uzasadniać ogólny obowiązek zatrzymywania danych, w przeciwieństwie do walki z przestępstwami pospolitymi lub ze sprawnym przebiegiem postępowań niemających charakteru karnego.

174. W konsekwencji należy zbadać odpowiedni, konieczny i proporcjonalny charakter takiego obowiązku w świetle celu walki z poważnymi przestępstwami.

48 — Wyrok z dnia 29 stycznia 2008 r., C-275/06, EU:C:2008:54, pkt 50–54.

49 — Wyrok z dnia 29 stycznia 2008 r., C-275/06, EU:C:2008:54.

50 — Zobacz pkt 252–261 niniejszej opinii.

4. W przedmiocie odpowiedniego charakteru ogólnego obowiązku zatrzymywania danych w świetle walki z poważnymi przestępstwami

175. Wymogi dotyczące charakteru odpowiedniego, koniecznego [51] i proporcjonalnego [52] wypływają zarówno z art. 15 ust. 1 dyrektywy 2002/58, jak i z art. 52 ust. 1 karty.

176. Zgodnie z pierwszym z tych wymogów ogólny obowiązek zatrzymywania danych, taki jak obowiązki rozpatrywane w postępowaniach głównych, powinien móc przyczyniać się do realizacji wskazanego wyżej celu interesu ogólnego, a mianowicie do walki z poważnymi przestępstwami.

177. Wymóg ten nie stwarza szczególnych trudności w kontekście niniejszych spraw. Jak Trybunał wskazał zasadniczo w pkt 49 wyroku DRI, zatrzymane dane pozwalają organom krajowym właściwym w sprawach karnych dysponować dodatkowym środkiem dochodzeniowo-śledczym w celu zapobiegania poważnym przestępstwom lub wyjaśniania ich. W rezultacie obowiązek taki przyczynia się do walki z poważnymi przestępstwami.

178. Chciałbym jednak uściślić, w jaki sposób ogólny obowiązek zatrzymywania danych może być użyteczny do celów walki z poważnymi przestępstwami. Jak słusznie podnosi rząd francuski, obowiązek taki w pewnym stopniu pozwala organom ścigania na „odtwarzanie przeszłości" dzięki badaniu zatrzymanych danych, w odróżnieniu od środków ukierunkowanej obserwacji niejawnej.

179. Środek ukierunkowanej obserwacji niejawnej dotyczy osób, które zostały wcześniej zidentyfikowane jako mogące mieć związek, nawet pośredni lub odległy, z poważnym przestępstwem. Takie środki ukierunkowane pozwalają właściwym organom na dostęp do danych dotyczących komunikatów przekazywanych przez te osoby, a wręcz do treści owych komunikatów. Jednakże taki dostęp może dotyczyć jedynie komunikatów przekazywanych przez takie osoby *po* ich identyfikacji.

180. Natomiast ogólny obowiązek zatrzymywania danych obejmuje wszystkie komunikaty przekazywane przez ogół użytkowników, przy czym nie jest wymagane jakiekolwiek powiązanie z poważnym przestępstwem. Obowiązek taki pozwala właściwym organom na dostęp do historii komunikatów przekazywanych przez osobę przed jej zidentyfikowaniem jako mającej takie powiązanie. To właśnie w ten sposób ów obowiązek daje organom ścigania ograniczoną zdolność do odtwarzania przeszłości, przyznając im dostęp do komunikatów przekazywanych przez takie osoby *przed* identyfikacją tych osób [53].

181. Innymi słowy, użyteczność ogólnego obowiązku zatrzymywania danych do celów walki z poważnymi przestępstwami polega na owej ograniczonej zdolności do odtwarzania przeszłości na podstawie danych ukazujących historię komunikatów przekazywanych przez daną osobę, nawet zanim jeszcze stała się ona podejrzana o związek z poważnym przestępstwem [54].

51 — W przedmiocie charakteru koniecznego zob. pkt 185–245 niniejszej opinii.

52 — W przedmiocie charakteru proporcjonalnego sensu stricto zob. pkt 246–262 niniejszej opinii.

53 — Komisja wskazała ponadto, że wartość dodana ogólnego obowiązku zatrzymywania danych, w porównaniu do indywidualnego zatrzymywania danych, polega na owej ograniczonej zdolności do odtwarzania przeszłości: zob. dokument roboczy służb Komisji przedstawiony w załączniku do wniosku dotyczącego dyrektywy, który doprowadził do przyjęcia dyrektywy 2006/24, SEC(2005) 1131, 21 września 2005 r., nr 3.6, „Data Preservation versus Data Retention": „[W]ith only data preservation as a tool, it is impossible for investigators to go back in time. Data preservation is only useful as of the moment when suspects have been identified – data retention is indispensable in many cases to actually identify those suspects".

54 — Rząd francuski powołał się w tym względzie na sprawozdanie Conseil d'État (rady państwa, Francja), *Le numérique et les droits fondamentaux*, 2014, s. 209, 210. Conseil d'État podkreśla, że mechanizm środków ukierunkowanej obserwacji niejawnej „byłby zdecydowanie mniej skuteczny niż systematyczne zatrzymywanie danych z punktu widzenia bezpieczeństwa narodowego i wykrywania sprawców naruszenia. Nie pozwala on bowiem na dostęp retrospektywny do komunikatów, które miały miejsce przed zidentyfikowaniem przez organ zagrożenia lub przestępstwa: jego przydatność operacyjna zależy zatem od zdolności organów do przewidywania tożsamości osób, których dane o ruchu mogą być przydatne, co jest niemożliwe w policji sądowej. Jeśli chodzi na przykład o przestępstwo, organ sądowy nie może mieć dostępu do połączeń, które miały miejsce przed jego popełnieniem, informacji cennej, a czasem nawet koniecznej do identyfikacji jego sprawcy i jego pomocników, jak pokazało kilka niedawnych spraw dotyczących zamachów terrorystycznych. W dziedzinie zapobiegania naruszeniom bezpieczeństwa narodowego nowe programy techniczne opierają się na zdolności wykrywania słabych sygnałów, która jest sprzeczna z koncepcją wcześniejszej identyfikacji osób niebezpiecznych".

182. W trakcie prezentacji wniosku w sprawie dyrektywy, który doprowadził do przyjęcia dyrektywy 2006/24, Komisja zilustrowała ową użyteczność za pomocą konkretnych przykładów postępowań dotyczących w szczególności aktów terrorystycznych, zabójstw, porwań i pornografii dziecięcej [55].

183. Szereg podobnych przykładów zostało przedstawionych Trybunałowi w ramach niniejszych spraw, w szczególności przez rząd francuski, który podkreślił ciążący na państwach członkowskich pozytywny obowiązek zapewnienia bezpieczeństwa osób znajdujących się na ich terytorium. Zdaniem tego rządu w postępowaniach dotyczących rozbicia siatki organizującej wyjazdy rezydentów francuskich do stref konfliktu w Iraku lub w Syrii dostęp do zatrzymanych danych odgrywa decydującą rolę w identyfikacji osób, które pomagały w tych wyjazdach. Rząd ten dodaje, że dostęp do dotyczących komunikatów danych związanych z osobami zaangażowanymi w ostatnie ataki terrorystyczne mające miejsce w styczniu i listopadzie 2015 r. we Francji był szczególnie użyteczny dla osób prowadzących postępowania przy wykrywaniu pomocników sprawców tychże ataków. Podobnie, w poszukiwaniach osoby zaginionej dane dotyczące lokalizacji tej osoby w czasie przekazywania komunikatów przed jej zaginięciem mogą odgrywać decydującą rolę w postępowaniu.

184. Mając na względzie powyższe rozważania, jestem zdania, że ogólny obowiązek zatrzymywania danych jest w stanie przyczynić się do walki z poważnymi przestępstwami. Pozostaje jednak ustalić, czy taki obowiązek jest jednocześnie konieczny i proporcjonalny do osiągnięcia tego celu.

5. W przedmiocie koniecznego charakteru ogólnego obowiązku zatrzymywania danych w świetle walki z poważnymi przestępstwami

185. Zgodnie z utrwalonym orzecznictwem środek może zostać uznany za konieczny wyłącznie w braku jakiegokolwiek innego środka, który byłby równie odpowiedni, będąc jednocześnie mniej dolegliwy [56].

186. Wymóg dotyczący odpowiedniości sprowadza się do oceny skuteczności „bezwzględnej" – niezależnie od jakiegokolwiek innego możliwego środka – ogólnego obowiązku zatrzymywania danych w odniesieniu do walki z poważnymi przestępstwami. Wymóg konieczności prowadzi natomiast do oceny skuteczności – albo skuteczności „względnej", to znaczy w porównaniu z innym możliwym środkiem – takiego obowiązku [57].

187. W kontekście niniejszej sprawy test konieczności wymaga, po pierwsze, sprawdzenia, czy inne środki mogłyby być równie skuteczne, jak ogólny obowiązek zatrzymywania danych w ramach walki z poważnymi przestępstwami, i po drugie, czy te ewentualne środki byłyby mniej szkodliwe dla praw ustanowionych w dyrektywie 2002/58 i w art. 7 i 8 karty [58].

55 — Commission Staff Working Document przedstawiony w załączniku do wniosku dotyczącego dyrektywy, który doprowadził do przyjęcia dyrektywy 2006/24, SEC(2005) 1131, 21 września 2005 r., nr 1.2, „The importance of traffic data for law enforcement".

56 — Zobacz w szczególności wyroki: z dnia 22 stycznia 2013 r., Sky Österreich, C-283/11, EU:C:2013:28, pkt 54–57; z dnia 13 listopada 2014 r., Reindl, C-443/13, EU:C:2014:2370, pkt 39; z dnia 16 lipca 2015 r., CEZ Razpredelenie Bŭlgarija, C-83/14, EU:C:2015:480, pkt 120–122. W doktrynie zob. w szczególności B. Pirker, *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, s. 29: „Under a necessity test, the adjudicator examines whether there exists an alternative measure which achieves the same degree of satisfaction for the first value while entailing a lower degree of non-satisfaction of the second value".

57 — Zobacz J. Rivers, Proportionality and variable intensity of review, 65(1) *Cambridge Law Journal* (2006) 174, s. 198: „The test of necessity thus expresses the idea of efficiency or Pareto-optimality. A distribution is efficient or Pareto-optimal if no other distribution could make at least one person better off without making any one else worse off. Likewise an act is necessary if no alternative act could make the victim better off in terms of rights-enjoyment without reducing the level of realisation of some other constitutional interest".

58 — W przedmiocie istnienia tych dwóch elementów w ramach testu dotyczącego konieczności zob. A. Barak, *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press 2012, s. 323–331.

188. Przypominam ponadto utrwalone orzecznictwo, przywołane w pkt 52 wyroku DRI, zgodnie z którym ochrona prawa podstawowego do prywatności wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia trzymały się w granicach tego, co „absolutnie konieczne” [59].

189. Strony, które przedstawiły uwagi Trybunałowi, omówiły dogłębnie dwa zagadnienia odnoszące się do wymogu absolutnej konieczności w kontekście niniejszych spraw, odpowiadające zasadniczo dwóm pytaniom postawionym przez sąd odsyłający w sprawie C-203/15:

— po pierwsze, czy w świetle pkt 56–59 wyroku DRI należy uznać, że ogólny obowiązek zatrzymywania danych sam w sobie wykracza poza granice tego, co absolutnie konieczne do walki z poważnymi przestępstwami, i to niezależnie od gwarancji towarzyszących temu obowiązkowi;

— po drugie, zakładając, że taki obowiązek sam w sobie mógłby zostać uznany za nieprzekraczający granic tego, co absolutnie konieczne, czy powinien on zostać obwarowany wszystkimi gwarancjami ustanowionymi przez Trybunał w pkt 60–68 wyroku DRI, w celu ograniczenia naruszenia praw ustanowionych w dyrektywie 2002/58 i w art. 7 i 8 karty do tego, co absolutnie konieczne?

190. Zanim zajmę się tymi zagadnieniami, pragnę zauważyć, że należy oddalić podniesiony przez rząd Zjednoczonego Królestwa argument, zgodnie z którym kryteria określone w wyroku DRI są pozbawione znaczenia w kontekście niniejszych spraw ze względu na to, że wyrok ten dotyczy nie systemu krajowego, lecz systemu ustanowionego przez prawodawcę Unii.

191. W tym względzie podkreślam, że w wyroku DRI dokonano wykładni art. 7, 8 i art. 52 ust. 1 karty oraz że postanowienia te są również przedmiotem pytań postawionych w postępowaniach głównych. Otóż nie jest moim zdaniem możliwe, aby wykładnia postanowień karty była odmienna w zależności od tego, czy sporny system został ustanowiony na poziomie Unii, czy na poziomie krajowym, jak słusznie podkreślili P. Brice i G. Lewis oraz Law Society of England and Wales. Jeżeli stwierdzono, że karta znajduje zastosowanie, jak ma to miejsce w przypadku niniejszych spraw [60], powinna ona być stosowana w taki sam sposób, niezależnie od spornego systemu. Co za tym idzie, kryteria określone przez Trybunał w wyroku DRI są istotne do celów oceny systemów krajowych będących przedmiotem sporu w niniejszych sprawach, jak wskazały w szczególności rząd duński i Irlandia oraz Komisja.

a) W przedmiocie absolutnie koniecznego charakteru ogólnego obowiązku zatrzymywania danych

192. Zgodnie z pierwszym podejściem, bronionym przez Tele2 Sverige oraz Open Rights Group i Privacy International, należy uznać, w następstwie wyroku DRI, że ogólny obowiązek zatrzymywania danych sam w sobie wykracza poza granice tego, co absolutnie konieczne do walki z poważnymi przestępstwami, i to niezależnie od ewentualnych gwarancji, którymi obwarowany jest ten obowiązek.

193. Zgodnie z drugim stanowiskiem, popieranym przez większość pozostałych stron, które przedłożyły uwagi Trybunałowi, obowiązek taki nie wykracza poza granice tego, co absolutnie konieczne, pod warunkiem że jest obwarowany pewnymi gwarancjami dotyczącymi dostępu do danych, okresu przechowywania oraz ochrony i bezpieczeństwa danych.

194. Następujące powody skłaniają mnie do przyjęcia tego drugiego podejścia.

59 — Zobacz w szczególności wyroki: z dnia 9 listopada 2010 r., Volker und Markus Schecke i Eifert, C-92/09 i C-93/09, EU:C:2010:662, pkt 77, 86; wyrok z dnia 7 listopada 2013 r., IPI, C-473/12, EU:C:2013:715, pkt 39.

60 — Zobacz pkt 117–125 niniejszej opinii.

195. W pierwszej kolejności, zgodnie z moim rozumieniem wyroku DRI, Trybunał orzekł, że ogólny obowiązek zatrzymywania danych wykracza poza granice tego, co jest absolutnie konieczne, w przypadku gdy *nie jest obwarowany* rygorystycznymi gwarancjami dotyczącymi dostępu do danych, okresu przechowywania oraz ochrony i bezpieczeństwa danych. Natomiast Trybunał nie wypowiedział się w przedmiocie zgodności z prawem Unii ogólnego obowiązku zatrzymywania danych, który jest *obwarowany* takimi gwarancjami, ponieważ system taki nie stanowił przedmiotu pytań skierowanych do Trybunału w tej sprawie.

196. W tym względzie podkreślam, że pkt 56–59 wyroku DRI nie zawierają żadnego stwierdzenia Trybunału wskazującego, że ogólny obowiązek zatrzymywania danych sam w sobie wykracza poza granice tego, co absolutnie konieczne.

197. W pkt 56 i 57 tego wyroku Trybunał stwierdza, że ustanowiony w dyrektywie 2006/24 obowiązek zatrzymywania danych obejmuje wszystkie środki łączności elektronicznej, wszystkich użytkowników i wszystkie dane o ruchu, przy czym nie przewidziano jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku ze względu na cel walki z poważnymi przestępstwami.

198. W pkt 58 i 59 tego wyroku Trybunał wskazuje w sposób bardziej szczegółowy praktyczne skutki wspomnianego braku zróżnicowania. Po pierwsze, obowiązek zatrzymywania dotyczy nawet tych osób, co do których brak jest dowodów mogących sugerować, że ich zachowanie może mieć związek, nawet pośredni lub daleki, z poważnymi przestępstwami. Po drugie, dyrektywa ta nie wymaga istnienia żadnego związku między danymi, które mają być zatrzymywane, a zagrożeniem dla bezpieczeństwa publicznego; w szczególności dyrektywa nie ogranicza się do zatrzymywania danych związanych z określonym okresem czasu, określonym obszarem geograficznym lub określonym kręgiem osób mogących, w taki czy inny sposób, mieć związek z poważnym przestępstwem.

199. W konsekwencji Trybunał stwierdza, że ogólny obowiązek zatrzymywania danych charakteryzuje się brakiem zróżnicowania ze względu na cel walki z poważnymi przestępstwami. Nie orzekł on jednak, że ów brak zróżnicowania oznacza, iż obowiązek taki sam w sobie przekracza granice tego, co absolutnie konieczne.

200. W rzeczywistości dopiero zbadawszy system przewidziany przez dyrektywę 2006/24 i stwierdziwszy brak pewnych gwarancji, które przeanalizuję poniżej [61], Trybunał orzekł w pkt 69 wyroku DRI:

„*Z powyższych względów* należy uznać, że przyjmując dyrektywę 2006/24, prawodawca Unii *przekroczył granice*, które wyznacza poszanowanie zasady proporcjonalności na gruncie art. 7, 8 i art. 52 ust. 1 karty” (wyróżnienie moje).

201. Jak wskazały rządy niemiecki i niderlandzki, gdyby samo generalne zatrzymywanie danych było wystarczające do stwierdzenia nieważności dyrektywy 2006/24, Trybunał nie miałby potrzeby badania, i to w sposób szczegółowy, braku gwarancji określonych w pkt 60–68 tego wyroku.

202. Co za tym idzie, ogólny obowiązek zatrzymywania danych ustanowiony w dyrektywie 2006/24 nie przekraczał sam w sobie granic tego, co absolutnie konieczne. Dyrektywa ta przekroczyła granice tego, co absolutnie konieczne, ze względu na *połączony skutek* generalnego zatrzymywania danych i braku gwarancji służących ograniczeniu naruszenia praw uznanych w art. 7 i 8 karty do tego, co absolutnie konieczne. W związku z tym skutkiem połączonym dyrektywa powinna zostać uznana za nieważną w całości [62].

61 — Zobacz pkt 216–245 niniejszej opinii.

62 — Zobacz wyrok DRI, pkt 65: „Należy w rezultacie stwierdzić, że dyrektywa ta wyjątkowo szeroko i mocno ingeruje w te podstawowe dla porządku prawnego Unii prawa, przy czym przepisy mające zagwarantować to, że ingerencja ta nie będzie rzeczywiście wykraczać poza to, co ściśle niezbędne, *nie regulują* precyzyjnie tej kwestii” (wyróżnienie moje).

203. W drugiej kolejności taka wykładnia znajduje potwierdzenie w pkt 93 wyroku Schrems [63], który przytaczam poniżej:

„W ten sposób uregulowanie umożliwiające generalnie przechowywanie wszelkich danych osobowych wszystkich osób fizycznych, których dane zostały przekazane z Unii do Stanów Zjednoczonych *bez* jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w zależności od zamierzonego celu *i bez* przewidzenia obiektywnych kryteriów, które pozwoliłyby na ograniczenie dostępu władz publicznych do danych oraz na ich późniejsze wykorzystanie do określonych celów, ściśle ograniczonych, które mogą uzasadnić ingerencję, jaką stanowi zarówno dostęp, jak i wykorzystanie tych danych, nie ogranicza się do tego, co absolutnie konieczne [zob. podobnie, w odniesieniu do dyrektywy 2006/24, wyrok DRI, pkt 57–61]" (wyróżnienie moje).

204. Ponownie, Trybunał nie orzekł, że sporny w tej sprawie system przekracza granice tego, co absolutnie konieczne, jedynie na tej podstawie, że zezwalał on na generalne zatrzymywanie danych osobowych. W niniejszej sprawie granice tego, co absolutnie konieczne, zostały przekroczone ze względu na połączony skutek możliwości dokonania takiego generalnego zatrzymywania danych i braku gwarancji w zakresie dostępu zmierzającej do ograniczenia ingerencji do tego, co absolutnie konieczne.

205. Z powyższego wnioskuję, że nie można uznać, iż ogólny obowiązek zatrzymywania danych sam w sobie zawsze przekracza granice tego, co jest absolutnie konieczne do walki z poważnymi przestępstwami. Natomiast taki obowiązek zawsze przekracza granice tego, co jest absolutnie konieczne, w przypadku gdy nie jest obwarowany gwarancjami dotyczącymi dostępu do danych, okresu przechowywania oraz ochrony i bezpieczeństwa danych.

206. W trzeciej kolejności moje przekonanie w tym względzie potwierdza konieczność ustalenia w konkretnych przypadkach, czy poszanowany został wymóg dotyczący charakteru absolutnie koniecznego w obrębie systemów krajowych rozpatrywanych w postępowaniach głównych.

207. Jak wskazałem w pkt 187 niniejszej opinii, wymóg absolutnie koniecznego charakteru wymaga zbadania, czy inne środki mogłyby być równie skuteczne, jak ogólny obowiązek zatrzymywania danych w ramach walki z poważnymi przestępstwami, będąc jednocześnie mniej szkodliwe dla praw ustanowionych w dyrektywie 2002/58 i w art. 7 i 8 karty.

208. Tymczasem taka ocena powinna zostać dokonana w szczególnym kontekście każdego systemu krajowego przewidującego ogólny obowiązek zatrzymywania danych. Po pierwsze, ocena ta wymaga porównania skuteczności tego obowiązku ze skutecznością każdego innego możliwego na gruncie krajowym środka, biorąc pod uwagę fakt, że wspomniany obowiązek zapewnia właściwym organom ograniczoną zdolność do odtwarzania przeszłości na podstawie zatrzymanych danych [64].

209. Mając na względzie wymóg ścisłej konieczności, nieodzowne jest, aby sądy te nie ograniczyły się do weryfikacji samej li tylko użyteczności ogólnego obowiązku zatrzymywania danych, ale by rygorystycznie sprawdziły też, czy żaden inny środek lub kombinacja środków, a w szczególności obowiązek indywidualnego zatrzymywania danych wraz z innymi narzędziami

63 — Wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650.

64 — Zobacz pkt 178–183 niniejszej opinii.

dochodzeniowo-śledczymi, nie może zapewnić takiej samej skuteczności w walce z poważnymi przestępstwami. W tym względzie podkreślam, że szereg badań zaprezentowanych Trybunałowi podważa konieczność wprowadzenia tego rodzaju obowiązku do celów walki z poważnymi przestępstwami [65].

210. Po drugie, zakładając, że inne środki mogą być równie skuteczne w walce z poważnymi przestępstwami, do sądów odsyłających należeć będzie jeszcze ustalenie, czy w myśl utrwalonego orzecznictwa przypomnianego w pkt 185 niniejszej opinii są one dla rozpatrywanych praw podstawowych mniej szkodliwe niż ogólny obowiązek zatrzymywania danych.

211. W świetle pkt 59 wyroku DRI sądy krajowe będą miały za zadanie zastanowić się w szczególności nad możliwością ograniczenia zakresu materialnego obowiązku zatrzymywania danych przy jednoczesnym zachowaniu skuteczności tego środka w walce z poważnymi przestępstwami [66]. Obowiązki takie mogą mieć bowiem zasięg materialny szerzy lub węższy, w zależności od użytkowników, obszarów geograficznych i środków komunikacji, których dotyczą [67].

212. W mojej ocenie w szczególności pożądane byłoby, o ile pozwala na to technologia, wykluczenie z obowiązku zatrzymywania danych szczególnie wrażliwych w świetle praw podstawowych rozpatrywanych w niniejszych sprawach, takich jak dane objęte tajemnicą zawodową lub też dane pozwalające na zidentyfikowanie źródła dziennikarskiego.

213. Należy jednak mieć na uwadze fakt, że znaczne ograniczenie zakresu ogólnego obowiązku zatrzymywania danych wiąże się z ryzykiem istotnego ograniczenia użyteczności, jaką taki system posiada w walce z poważnymi przestępstwami. Po pierwsze, szereg rządów podkreśliło trudności, a wręcz brak możliwości określenia z góry danych, które mogłyby mieć związek z poważnym przestępstwem. Co za tym idzie, ograniczenie takie może wykluczyć zatrzymywanie danych, które mogłyby okazać się istotne w walce z poważnymi przestępstwami.

214. Z drugiej strony, jak to podniósł rząd estoński, poważna przestępczość jest zjawiskiem dynamicznym i posiada zdolność dostosowania się do narzędzi dochodzeniowych, którymi dysponują organy ścigania. Tak więc ograniczenie do określonego obszaru geograficznego lub określonego środka komunikacji mogłoby spowodować przeniesienie działalności związanej z poważną przestępczością do obszaru geograficznego lub środka komunikacji nieobjętych tym systemem.

215. Uważam, że ocena ta, jako wymagająca przeprowadzenia złożonego badania krajowych systemów rozpatrywanych w postępowaniach głównych, powinna zostać przeprowadzona przez sądy krajowe, jak to podkreśliły rządy czeski, estoński, francuski, niderlandzki, Irlandia oraz Komisja.

65 — Zobacz Komisarz Praw Człowieka Rady Europy, „Issue paper on the rule of law on the Internet and in the wider digital world", grudzień 2014, CommDH/IssuePaper (2014) 1, s. 115; Rada Praw Człowieka ONZ, Sprawozdanie wysokiego komisarza Narodów Zjednoczonych do spraw praw człowieka na temat prawa do poszanowania życia prywatnego w dobie łączności cyfrowej, 30 czerwca 2014 r., A/HRC/27/37, nr 26; Zgromadzenie Ogólne ONZ, Sprawozdanie specjalne sprawozdawcy Narodów Zjednoczonych dotyczące wspierania i ochrony praw człowieka i podstawowych wolności w ramach walki z terroryzmem, 23 września 2014 r., A/69/397, nr 18, 19 [tłumaczenia nieoficjalne].

66 — Uwaga ta dotyczy jedynie ogólnych obowiązków zatrzymywania danych (które mogą dotyczyć każdej osoby, niezależnie od jakiegokolwiek jej związku z poważnym przestępstwem), a nie środków ukierunkowanej obserwacji niejawnej (odnoszących się do osób, które zostały wcześniej zidentyfikowane jako mające związek z poważnym przestępstwem): w przedmiocie tego rozróżnienia zob. pkt 178–183 niniejszej opinii.

67 — Rząd niemiecki wyjaśnił między innymi podczas rozprawy, że parlament niemiecki wykluczył z zakresu obowiązku zatrzymywania danych, nałożonego przez ustawodawstwo niemieckie, korespondencję elektroniczną, ale że system ten obejmuje wszystkich użytkowników i całość terytorium krajowego.

b) W przedmiocie wiążącego charakteru gwarancji ustanowionych przez Trybunał w pkt 60–68 wyroku DRI w świetle wymogu absolutnej konieczności

216. Zakładając, że ogólny obowiązek zatrzymywania danych może być uznany za absolutnie konieczny w ramach rozpatrywanego systemu krajowego, czego ocena należy do sądu krajowego, należy ponadto ustalić, czy obowiązek taki powinien zostać obwarowany całością gwarancji ustanowionych przez Trybunał w pkt 60–68 wyroku DRI, w celu ograniczenia naruszenia praw przyznanych w dyrektywie 2002/58 i w art. 7 i 8 karty do tego, co absolutnie konieczne.

217. Gwarancje te dotyczą zasad regulujących dostęp do zatrzymanych danych i ich wykorzystywania przez właściwe organy (pkt 60–62 wyroku DRI), okresu przechowywania danych (pkt 63 i 64 tego wyroku) oraz bezpieczeństwa i ochrony danych zatrzymanych przez dostawców (pkt 66–68 wyroku).

218. W uwagach przedłożonych Trybunałowi przedstawiono dwie przeciwstawne koncepcje dotyczące charakteru tych gwarancji.

219. Zgodnie z pierwszą koncepcją, bronioną przez T. Watsona, P. Brice'a i G. Lewisa oraz Open Rights Group i Privacy International, gwarancje wymienione przez Trybunał w pkt 60–68 wyroku DRI mają wiążący charakter. Zgodnie z tą koncepcją Trybunał ustalił minimalne gwarancje, z których *wszystkie* muszą być spełnione przez sporny system krajowy, aby naruszenie praw podstawowych było ograniczone do tego, co absolutnie konieczne.

220. Zgodnie z drugą koncepcją, wysuniętą przez rządy niemiecki, estoński, francuski, Zjednoczonego Królestwa i Irlandię gwarancje wymienione przez Trybunał w pkt 60–68 wyroku DRI mają jedynie charakter orientacyjny. Trybunał dokonał „oceny całości" gwarancji, których brak było w systemie przewidzianym przez dyrektywę 2006/24, przy czym żadna z tych gwarancji nie może w sposób autonomiczny zostać uznana za wiążącą z punktu widzenia wymogu absolutnej konieczności. Dla zilustrowania tej koncepcji rząd niemiecki posłużył się mechanizmem „naczyń połączonych", zgodnie z którym podejście bardziej elastyczne w odniesieniu do jednego z trzech aspektów wskazanych przez Trybunał (na przykład dostępu do zatrzymywanych danych) może zostać skompensowane przez podejście bardziej rygorystyczne w odniesieniu do dwóch pozostałych aspektów (okresu przechowywania oraz bezpieczeństwa i ochrony danych).

221. Żywię przekonanie, że koncepcja „naczyń połączonych" powinna zostać odrzucona i że należy uznać, iż *wszystkie* gwarancje wymienione przez Trybunał w pkt 60–68 wyroku DRI mają wiążący charakter, a to z następujących powodów.

222. W pierwszej kolejności nie podlegają takiej wykładni sformułowania użyte przez Trybunał w ramach badania absolutnie koniecznego charakteru systemu wprowadzonego przez dyrektywę 2006/24. W szczególności Trybunał nigdzie w pkt 60–68 wspomnianego wyroku nie daje do zrozumienia, że istnieje jakakolwiek możliwość „skompensowania" podejścia bardziej elastycznego w odniesieniu do jednego z trzech aspektów wskazanych przez Trybunał przez podejście bardziej rygorystyczne w odniesieniu do dwóch pozostałych aspektów.

223. W rzeczywistości koncepcja „naczyń połączonych", jak mi się wydaje, wynika z pomylenia wymogu konieczności i wymogu proporcjonalności sensu stricto, który nie został zbadany przez Trybunał w wyroku DRI. Jak już bowiem wskazałem w pkt 186 niniejszej opinii, wymóg konieczności polega na odrzuceniu wszelkich środków nieskutecznych. Nie można w tym kontekście mówić o „ocenie całościowej", „skompensowaniu" ani „wyważeniu", ponieważ elementy te występują dopiero

na etapie proporcjonalności sensu stricto [68].

224. W drugiej kolejności owa koncepcja „naczyń połączonych" niweczy skuteczność gwarancji ustanowionych przez Trybunał w pkt 60–68 wyroku DRI, przez co osoby, których dane zostały zatrzymane, zostają pozbawione wystarczających gwarancji rzeczywistej ochrony ich danych osobowych przed ryzykiem nadużyć oraz ich bezprawnym udostępnianiem i wykorzystywaniem, czego wymaga pkt 54 owego wyroku.

225. Destrukcyjny skutek takiej koncepcji można łatwo zilustrować za pomocą następujących przykładów. System krajowy, który ściśle limituje dostęp jedynie do celów walki z terroryzmem i ogranicza okres przechowywania do trzech miesięcy (podejście rygorystyczne w odniesieniu do dostępu i okresu przechowywania), ale który nie zobowiązuje dostawców do przechowywania danych na danym terytorium krajowym i w postaci zaszyfrowanej (podejście elastyczne w odniesieniu do bezpieczeństwa), naraża ogół ludności na wysokie ryzyko niezgodnego z prawem dostępu do zatrzymanych danych. Tak samo system krajowy, który ustala okres przechowywania na trzy miesiące oraz wymaga przechowywania danych na swoim terytorium krajowym w postaci zaszyfrowanej (podejście rygorystyczne w odniesieniu do okresu przechowywania i bezpieczeństwa), lecz który umożliwia wszystkim pracownikom wszystkich organów władzy publicznej dostęp do zatrzymanych danych (podejście elastyczne w odniesieniu do dostępu), narażałby ogół ludności na wysokie ryzyko nadużycia ze strony organów krajowych.

226. W mojej ocenie z przykładów tych wynika, że zachowanie skuteczności gwarancji ustanowionych przez Trybunał w pkt 60–68 wyroku DRI wymaga uznania *każdej* z tych gwarancji za wiążącą. ETPC podkreślił również fundamentalne znaczenie tych gwarancji w niedawnym wyroku Szabó i Vissy przeciwko Węgrom, odnosząc się wyraźnie do wyroku DRI [69].

227. W trzeciej kolejności wprowadzenie w życie tych gwarancji przez państwa członkowskie, które zamierzają nałożyć ogólny obowiązek zatrzymywania danych, nie powinno, jak mi się wydaje, sprawiać większych trudności praktycznych. W rzeczywistości gwarancje te wydają mi się pod wieloma względami „minimalne", jak podniósł T. Watson.

228. Wiele z tych gwarancji było przedmiotem dyskusji przed Trybunałem ze względu na możliwy ich brak w krajowych systemach będących przedmiotem sporu w postępowaniach głównych.

229. Po pierwsze, jak wynika z pkt 61 i 62 wyroku DRI, dostęp do zatrzymanych danych i ich późniejsze wykorzystanie powinny być ściśle ograniczone do celów zapobiegania i wykrywania dokładnie określonych poważnych przestępstw lub ich ścigania na gruncie prawa karnego.

230. Zdaniem Tele2 Sverige i Komisji szwedzki system będący przedmiotem sprawy C-203/15, który pozwala na dostęp do zatrzymanych danych w celu walki z przestępstwami pospolitymi, nie spełnia tego wymogu. Z podobnym zarzutem spotkał się ze strony P. Brice'a i G. Lewisa oraz T. Watsona będący przedmiotem sprawy C-698/15 system Zjednoczonego Królestwa, który zezwala na dostęp w celu walki z przestępstwami pospolitymi, a nawet w wypadku braku przestępstwa.

68 — Zobacz A. Barak, *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge 2012, s. 344: „The first three components of proportionality deal mainly with the relation between the limiting law's purpose and the means to fulfil that purpose […]. Accordingly, those tests are referred to as means-end analysis. *They are not based on balancing*. The test of proportionality stricto sensu is different […]. It focuses on the relation between the benefit in fulfilling the law's purpose and the harm caused by limiting the constitutional right. *It is based on balancing*" (wyróżnienie moje).

69 — Wyrok ETPC z dnia 12 stycznia 2016 r. w sprawie Szabó i Vissy przeciwko Węgrom, CE:ECHR:2016:0112JUD003713814, §68: „Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information".

231. Chociaż to nie do Trybunału należy orzekanie w przedmiocie treści tych systemów krajowych, do niego należy jednak określenie celów interesu ogólnego, które mogą uzasadnić poważną ingerencję w prawa ustanowione w dyrektywie i w art. 7 i 8 karty. W niniejszej sprawie przedstawiłem już powody, dla których uważam, że taką ingerencję może uzasadniać *wyłącznie* walka z poważnymi przestępstwami [70].

232. Po drugie, zgodnie z pkt 62 wyroku DRI, uzyskanie dostępu do danych powinno podlegać uprzedniej kontroli sądu lub niezależnego organu administracyjnego, które pilnowałyby, aby udostępnianie i wykorzystywanie danych ograniczało się do przypadków, gdy jest to absolutnie konieczne do realizacji zamierzonego celu. Owa uprzednia kontrola powinna ponadto mieć miejsce na uzasadniony wniosek owych organów, złożony w ramach postępowań mających na celu zapobieganie przestępstwom na gruncie prawa karnego, ich wykrywanie lub ściganie.

233. Jak wynika z uwag Tele2 Sverige i Komisji, owej gwarancji niezależnej i uprzedniej kontroli dostępu częściowo brak jest w systemie szwedzkim będącym przedmiotem sprawy C-203/15. To samo stwierdzenie, którego prawdziwość nie jest kwestionowana przez rząd Zjednoczonego Królestwa, zostało sformułowane przez P. Brice'a i G. Lewisa, T. Watsona oraz Open Rights Group i Privacy International w odniesieniu do systemu Zjednoczonego Królestwa będącego przedmiotem sprawy C-698/15.

234. Nie widzę żadnego powodu, by osłabić ów wymóg przeprowadzenia uprzedniej kontroli przez niezależny organ, który to wymóg bez wątpienia wynika ze sformułowań użytych przez Trybunał w pkt 62 wyroku DRI [71]. Przede wszystkim wymóg ten jest podyktowany wagą ingerencji i zagrożeń spowodowanych przez utworzenie baz danych obejmujących niemal ogół ludności [72]. Pragnę zauważyć, że wielu ekspertów w dziedzinie ochrony praw człowieka w walce z terroryzmem skrytykowało obecną tendencję do zastępowania tradycyjnych procedur niezależnego udzielania zezwoleń i skutecznego nadzoru systemami „wewnętrznych" zezwoleń na dostęp do danych, które służby wywiadowcze i policja wydają same sobie [73].

235. Poza tym niezależna i uprzednia kontrola dostępu do danych jest konieczna w celu umożliwienia indywidualnego traktowania szczególnie wrażliwych w świetle praw podstawowych rozpatrywanych w niniejszych sprawach danych, takich jak dane objęte tajemnicą zawodową lub też dane pozwalające na zidentyfikowanie źródła dziennikarskiego, co podkreśliły Law Society of England and Wales, a także rządy francuski i niemiecki. Owa uprzednia kontrola, następująca przed przyznaniem dostępu, jest tym bardziej niezbędna w przypadku, gdy technicznie trudno jest wykluczyć wszystkie takie dane na etapie zatrzymywania [74].

70 — Zobacz pkt 170–173 niniejszej opinii.

71 — Wskazuję jednak, że ów wymóg uprzedniej i niezależnej kontroli nie znajduje moim zdaniem swego źródła w art. 8 ust. 3 karty, ponieważ karta jako taka nie jest stosowana do przepisów krajowych regulujących dostęp do zatrzymanych danych: zob. pkt 123–125 niniejszej opinii.

72 — Zobacz pkt 252–261 niniejszej opinii.

73 — Rada Praw Człowieka ONZ, sprawozdanie specjalnego sprawozdawcy Narodów Zjednoczonych dotyczące wspierania i ochrony praw człowieka i podstawowych wolności w ramach walki z terroryzmem, 28 grudnia 2009 r., A/HRC/13/37, nr 62: „[N]ie powinien istnieć żaden system niejawnego obserwowania połączeń, który nie znajduje się pod skutecznym nadzorem organu kontroli, ani żadna ingerencja, która nie jest przedmiotem zezwolenia wydanego przez niezależny organ" (zob. także nr 51). Zobacz także Zgromadzenie Ogólne ONZ, sprawozdanie specjalnego sprawozdawcy Narodów Zjednoczonych dotyczące wspierania i ochrony praw człowieka i podstawowych wolności w ramach walki z terroryzmem, 23 września 2014 r., A/69/397, nr 61.

74 — Zobacz pkt 212 niniejszej opinii. W odniesieniu do źródeł dziennikarskich ETPC podkreślił konieczność uzyskania uprzedniego zezwolenia od niezależnego organu, ponieważ kontrola następcza nie pozwala na przywrócenie poufności tych źródeł: zob. wyrok ETPC: z dnia 22 listopada 2012 r. w sprawie Telegraaf Media Nederland Landelijke Media B.V. i in. przeciwko Niderlandom, CE:ECHR:2012:1122JUD003931506, § 101; z dnia 12 stycznia 2016 r. w sprawie Szabó i Vissy przeciwko Węgrom, CE:ECHR:2016:0112JUD003713814, §77. W wyroku Kopp przeciwko Szwajcarii, który dotyczył niejawnego obserwowania linii telefonicznych adwokata, ETPC zakwestionował to, że urzędnikowi będącemu częścią administracji powierzono, bez kontroli przez niezależny sąd, selekcjonowanie informacji objętych zakresem tajemnicy zawodowej: zob. wyrok ETPC z dnia 25 marca 1998 r. w sprawie Kopp przeciwko Szwajcarii, CE:ECHR:1998:0325JUD002322494, § 74.

236. Wreszcie pragnę dodać, że z praktycznego punktu widzenia żaden z trzech podmiotów, których dotyczy wniosek o dostęp, nie jest w stanie sprawować skutecznej kontroli nad dostępem do zatrzymanych danych. Organy ścigania potrzebują przedstawić żądanie możliwie najszerszego dostępu do tych danych. Dostawcy, którzy nie znają akt dochodzenia lub śledztwa, nie mogą ustalić, czy wniosek o dostęp jest ograniczony do tego, co absolutnie konieczne. W odniesieniu do osób, których dane są przeglądane, nie mają one żadnej możliwości dowiedzenia się, że są przedmiotem takiego środka dochodzeniowo-śledczego, i to nawet w przypadku nadużycia lub działania bezprawnego, co zostało podkreślone przez T. Watsona, P. Brice'a i G. Lewisa. Taki układ wchodzących w grę interesów wymaga w mojej ocenie, aby przed przyznaniem możliwości zapoznania się z zatrzymanymi danymi nastąpiła interwencja niezależnego organu w celu ochrony osób, których dane są przechowywane, przed nadużyciem dostępu przez właściwe organy.

237. Niezależnie od tego wydaje mi się rozsądne, aby sytuacje doraźne, niecierpiące zwłoki, o których mówił rząd Zjednoczonego Królestwa, mogły uzasadniać natychmiastowy dostęp organów ścigania do zatrzymanych danych, bez uprzedniej kontroli, w celu zapobieżenia popełnieniu ciężkiego przestępstwa lub w celu ścigania sprawców takich przestępstw[75]. Konieczne jest, aby, jeśli to tylko możliwe, utrzymać wymóg uprzedniego zezwolenia poprzez ustanowienie w ramach niezależnego organu pilnej procedury służącej rozpatrywaniu tego rodzaju wniosków o dostęp. Jednakże gdyby samo nawet zwrócenie się do tego organu z wnioskiem o dostęp było niezgodne z niezwykle pilnym charakterem sytuacji, dostęp i wykorzystanie danych powinny być przedmiotem kontroli następczej przeprowadzonej przez ten organ w możliwie najkrótszym terminie.

238. Po trzecie, w pkt 68 wyroku DRI ustanowiono spoczywający na dostawcach obowiązek zatrzymywania danych na terytorium Unii w celu zagwarantowania kontroli poszanowania wymogów ochrony i bezpieczeństwa, o których mowa w pkt 66 i 67 tego wyroku, przez niezależny organ, czego wymaga art. 8 ust. 3 karty.

239. Tele2 Sverige i Komisja podniosły, że system szwedzki, będący przedmiotem sprawy C-203/15, nie gwarantuje, iż dane będą przechowywane na terytorium krajowym. Z takim samym zarzutem spotkał się ze strony P. Brice'a i G. Lewisa oraz T. Watsona system Zjednoczonego Królestwa, będący przedmiotem sprawy C-698/15.

240. W tym względzie, po pierwsze, nie widzę żadnego powodu, by ów wymóg, ustanowiony w pkt 68 wyroku DRI, osłabić, ponieważ przechowywanie danych poza terytorium Unii nie pozwoliłoby zagwarantować osobom, których dane są przechowywane, poziomu ochrony zapewnionego przez dyrektywę 2002/58 oraz art. 7, 8 i art. 52 ust. 1 karty[76].

241. Wydaje mi się, po drugie, że rozsądne byłoby dostosowanie tego wymogu, opisanego przez Trybunał w kontekście dyrektywy 2006/24, do kontekstu systemów krajowych poprzez wprowadzenie obowiązku przechowywania danych na terytorium krajowym, jak podnoszą rządy niemiecki i francuski oraz Komisja. Zgodnie bowiem z art. 8 ust. 3 karty każde państwo członkowskie ma obowiązek zapewnić, by niezależny organ dokonał kontroli przestrzegania wymogów ochrony i bezpieczeństwa przez dostawców objętych systemem krajowym. Tymczasem w braku koordynacji na szczeblu Unii taki organ krajowy mógłby zostać pozbawiony możliwości wypełniania swoich zadań kontrolnych na terytorium innego państwa członkowskiego.

75 — Zobacz w tym względzie mechanizm opisany w pkt 22 niniejszej opinii. Podkreślam, że problematyka ta nie została poruszona przez Trybunał w wyroku DRI.

76 — Zobacz w tym względzie wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650.

242. Po czwarte, w odniesieniu do okresu przechowywania, sądy odsyłające powinny zastosować kryteria określone przez Trybunał w pkt 63 i 64 wyroku DRI. Z jednej strony sądy te powinny ustalić, czy zatrzymywane dane można rozróżnić ze względu na ich użyteczność oraz, jeśli tak jest, czy okres przechowywania został dostosowany zgodnie z tym kryterium. Z drugiej strony sądy te muszą ustalić, czy okres przechowywania jest oparty na obiektywnych kryteriach pozwalających na zapewnienie, by był on ograniczony do tego, co absolutnie konieczne.

243. Podkreślam, że ETPC w niedawnym wyroku Roman Zakharov przeciwko Rosji orzekł, iż okres przechowywania o długości nieprzekraczającej sześciu miesięcy jest rozsądny, lecz jednocześnie skrytykował brak obowiązku niszczenia na miejscu danych, które nie mają związku z celem, dla którego zostały zebrane[77]. Dodam w tym względzie, że systemy krajowe będące przedmiotem postępowań głównych powinny przewidywać obowiązek nieodwracalnego zniszczenia zatrzymanych danych, o ile nie są one już absolutnie konieczne do walki z poważnymi przestępstwami. Obowiązek ten musi być przestrzegany nie tylko przez dostawców, którzy dokonują zatrzymywania danych, lecz również przez organy mające dostęp do zatrzymanych danych.

244. Mając na względzie powyższe rozważania, uważam, że wszystkie gwarancje ustanowione przez Trybunał w pkt 60–68 wyroku DRI mają wiążący charakter i powinny zatem towarzyszyć ogólnemu obowiązkowi zatrzymywania danych w celu ograniczenia naruszenia praw przyznanych w dyrektywie 2002/58 i w art. 7 i 8 karty do tego, co absolutnie konieczne.

245. Do sądów odsyłających należy ustalenie, czy systemy krajowe będące przedmiotem postępowań głównych obejmują każdą z tych gwarancji.

6. W przedmiocie proporcjonalnego charakteru, w demokratycznym społeczeństwie, ogólnego obowiązku zatrzymywania danych w świetle celu walki z poważnymi przestępstwami

246. Po ustaleniu, czy systemy krajowe sporne w postępowaniach głównych mają konieczny charakter, sądy odsyłające powinny jeszcze zbadać ich proporcjonalny charakter w demokratycznym społeczeństwie w świetle celu walki z poważnymi przestępstwami. Kwestia ta nie została zbadana przez Trybunał w wyroku DRI, zważywszy, że system ustanowiony przez dyrektywę 2006/24 przekroczył granice tego, co jest absolutnie konieczne do walki z poważnymi przestępstwami.

247. Ów wymóg proporcjonalności w społeczeństwie demokratycznym – lub proporcjonalności „sensu stricto” – wynika zarówno z art. 15 ust. 1 dyrektywy 2002/58, z art. 52 ust. 1 karty, jak i z utrwalonego orzecznictwa. Zgodnie z tym utrwalonym orzecznictwem przepis naruszający prawa podstawowe może być uważany za proporcjonalny tylko wówczas, gdy niedogodności, które powoduje, nie są nadmierne w stosunku do zamierzonych celów[78].

248. W odróżnieniu od wymogów dotyczących odpowiedniego i koniecznego charakteru rozpatrywanego przepisu, w przypadku których dokonuje się oceny skuteczności tego przepisu w świetle zamierzonego celu, wymóg proporcjonalności sensu stricto polega na wyważeniu z jednej strony korzyści wynikających z tego przepisu w świetle zgodnego z prawem zamierzonego celu,

77 — Zobacz w tym względzie wyrok ETPC z dnia 4 grudnia 2015 r. w sprawie Roman Zakharov przeciwko Rosji, CE:ECHR:2015:1204JUD004714306, §§ 254, 255. Według prawa rosyjskiego zniszczenie przejętych elementów powinno nastąpić w terminie sześciu miesięcy od ich zatrzymania, jeżeli dana osoba nie została oskarżona o przestępstwo. ETPC orzekł, że maksymalna długość okresu zatrzymywania, to jest sześć miesięcy, ustalona w prawie rosyjskim w odniesieniu do takich danych, jest rozsądna. Niemniej jednak skrytykował on brak obowiązku zniszczenia na miejscu danych, które nie mają związku z celem, dla którego zostały zebrane, wyjaśniając, że automatyczne zatrzymywanie na okres sześciu miesięcy danych w sposób oczywisty pozbawionych znaczenia nie może być postrzegane jako uzasadnione w świetle art. 8 EKPC.

78 — Zobacz w szczególności wyroki: z dnia 15 lutego 2016 r., N., C-601/15 PPU, EU:C:2016:84, pkt 54 (charakter konieczny został zbadany w pkt 56–67, charakter proporcjonalny w pkt 68 i 69); z dnia 16 lipca 2015 r., CEZ Razpredelenie Byłgarija, C-83/14, EU:C:2015:480, pkt 123 (charakter konieczny został zbadany w pkt 120–122, charakter proporcjonalny w pkt 123–127); z dnia 22 stycznia 2013 r., Sky Österreich, C-283/11, EU:C:2013:28, pkt 50 (charakter konieczny został zbadany w pkt 54–57, charakter proporcjonalny w pkt 58–67).

a z drugiej strony wynikających z niego niedogodności w świetle praw podstawowych ustanowionych w społeczeństwie demokratycznym [79]. Wymóg ten otwiera tym samym dyskusję na temat wartości, jakie należy przyjąć w demokratycznym społeczeństwie, i ostatecznie na temat modelu społeczeństwa, w jakim pragniemy żyć [80].

249. W rezultacie, jak wskazałem w pkt 223 niniejszej opinii, to właśnie na etapie badania proporcjonalności sensu stricto, a nie na etapie badania konieczności, jak podnosili zwolennicy koncepcji „naczyń połączonych", należy dokonać oceny całości spornego systemu [81].

250. W myśl orzecznictwa przypomnianego w pkt 247 niniejszej opinii należy wyważyć korzyści i niedogodności ogólnego obowiązku zatrzymywania danych w demokratycznym społeczeństwie. Owe korzyści i niedogodności są ściśle związane z zasadniczą cechą takiego obowiązku, której stanowią one w pewnym sensie jasną i ciemną stronę, sprowadzającą się mianowicie do tego, iż obowiązek ten dotyczy wszystkich komunikatów przekazywanych przez ogół użytkowników, przy czym nie jest wymagane jakiekolwiek powiązanie z poważnym przestępstwem.

251. Po pierwsze, już wcześniej w pkt 178–183 niniejszej opinii wyjaśniłem korzyści, jakich w walce z poważnymi przestępstwami przysparza zatrzymywanie danych dotyczących wszystkich komunikatów przekazywanych na terytorium krajowym.

252. Z drugiej strony niedogodności płynące z ogólnego obowiązku zatrzymywania danych wynikają z faktu, że ogromna większość zatrzymywanych danych dotyczy osób, które nigdy nie będą miały żadnego powiązania z poważnym przestępstwem. W tym względzie ważne jest, aby wyjaśnić charakter niedogodności, którymi zostaną dotknięte te osoby. Otóż natura owych niedogodności jest zależna od stopnia ingerencji w prawa podstawowe tych osób do poszanowania życia prywatnego oraz do ochrony danych osobowych.

253. W przypadku ingerencji „indywidualnej", dotykającej określonej jednostki, niedogodności wynikające z ogólnego obowiązku zatrzymywania danych zostały opisane z dużą wyrazistością przez rzecznika generalnego P. Cruza Villalóna w pkt 72–74 opinii w sprawie DRI [82]. Zgodnie z użytym przez niego sformułowaniem wykorzystywanie tych danych umożliwia „opracowanie mapy, równie wiernej co wyczerpującej, sporej części działań określonej osoby należących ściśle do jej życia prywatnego, wręcz stworzenie kompletnego i dokładnego wizerunku jej prywatnej tożsamości".

254. Innymi słowy, w odniesieniu do indywidualnej osoby, ogólny obowiązek zatrzymywania danych pozwala na ingerencje równie poważne, jak środki ukierunkowanej obserwacji niejawnej, w tym na zapoznanie się z treścią przekazanych komunikatów.

79 — Zobacz J. Rivers, Proportionality and variable intensity of review, 65(1) *Cambridge Law Journal* (2006) 174, s. 198: „It is vital to realise that the test of balance has a totally different function from the test of necessity. The test of necessity rules out inefficient human rights limitations. It filters out cases in which the same level of realisation of a legitimate aim could be achieved at less cost to rights. By contrast, the test of balance is strongly evaluative. It asks whether the combination of certain levels of rights-enjoyment combined with the achievement of other interests is good or acceptable".

80 — Zobacz B. Pirker, *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen 2013, s. 30: „In its simple form, one could state that proportionality *stricto sensu* leads to a weighing between competing values to assess which value should prevail".

81 — Specyfikę wymogu proporcjonalności sensu stricto w porównaniu z wymogami charakteru odpowiedniego i koniecznego może zilustrować następujący przykład. Wyobraźmy sobie, że państwo członkowskie nakazuje instalację mikrochipa elektronicznego służącego geolokalizacji każdej osobie zamieszkującej na jego terytorium, przy czym ów mikrochip umożliwia organom władzy śledzenie przyjść i wyjść jego nosiciela w roku poprzednim. Taki środek mógłby zostać uznany za „konieczny", jeżeli żaden inny środek nie pozwala na osiągnięcie tego samego stopnia skuteczności w walce z poważnymi przestępstwami. Jednakże w mojej ocenie taki środek jest nieproporcjonalny w demokratycznym społeczeństwie, zważywszy, że niedogodności wynikające z naruszenia praw do nienaruszalności cielesnej, do poszanowania życia prywatnego oraz do ochrony danych osobowych są nadmierne w stosunku do wynikających z niego korzyści w walce z poważnymi przestępstwami.

82 — C-293/12 i C-594/12, EU:C:2013:845. Zobacz także wyrok DRI, pkt 27, 37.

255. Chociaż nie należy umniejszać wagi takich ingerencji indywidualnych, to wydaje mi się jednak, że konkretne zagrożenia wynikające z ogólnego obowiązku zatrzymywania danych uwidaczniają się dopiero w kontekście ingerencji „masowej".

256. W odróżnieniu od środków ukierunkowanej obserwacji niejawnej, obowiązek taki może bowiem w znacznym stopniu ułatwić ingerencje masowe, to znaczy ingerencje dotykające istotnej części, a nawet ogółu danej populacji, co można zilustrować za pomocą następujących przykładów.

257. Załóżmy w pierwszej kolejności, że osoba, która posiada dostęp do zatrzymanych danych, ma zamiar zidentyfikować w populacji państwa członkowskiego wszystkie jednostki cierpiące na zaburzenia psychiczne. Zanalizowanie w tym celu treści wszystkich komunikatów przekazanych na terytorium krajowym wymagałoby znacznych zasobów. Natomiast bazy danych dotyczących komunikatów pozwalałyby na natychmiastowe zidentyfikowanie wszystkich osób, które kontaktowały się z psychologiem w trakcie okresu przechowywania danych [83]. Dodam, że technika ta może mieć zastosowanie do każdej ze specjalizacji medycznych zarejestrowanych w państwie członkowskim [84].

258. Załóżmy w drugiej kolejności, że ta sama osoba pragnie zidentyfikować osoby sprzeciwiające się polityce obecnego rządu. Również w tym przypadku przeprowadzenie w tym celu analizy treści rozmów wymagałoby znacznych zasobów. Natomiast wykorzystanie danych dotyczących komunikatów pozwoliłoby na zidentyfikowanie wszystkich krytykujących politykę rządu osób wpisanych na listy dystrybucji korespondencji elektronicznej. Ponadto dane te pozwoliłby również na wskazanie osób uczestniczących we wszelkich publicznych manifestacjach organizacji opozycyjnych wobec rządu [85].

259. Pragnę podkreślić, że zagrożenia związane z dostępem do danych dotyczących komunikatów (lub „metadanych") mogą być równe zagrożeniom wynikającym z dostępu do treści komunikatów lub większe od tych zagrożeń, co zostało podkreślone przez Open Rights Group i Privacy International, Law Society of England and Wales, a także w niedawnym sprawozdaniu Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka [86]. W szczególności, jak wskazują podane wyżej przykłady, „metadane" pozwalają na niemalże natychmiastowe skatalogowanie populacji w całości, na co nie pozwala treść komunikatu.

83 — Zatrzymywane dane obejmują bowiem tożsamość źródła i odbiorcy komunikatu, które to dane wystarczyłoby zestawić z wykazem numerów telefonów psychologów działających na terytorium krajowym.

84 — Zobacz w tym względzie Rada Praw Człowieka ONZ, sprawozdanie specjalnego sprawozdawcy Narodów Zjednoczonych dotyczące wspierania i ochrony praw człowieka i podstawowych wolności w ramach walki z terroryzmem, 28 grudnia 2009 r., A/HRC/13/37, nr 42: „[W] Niemczech badania wykazały niepokojącą konsekwencję polityki zatrzymywania danych: 52% zapytanych osób wskazało, że z powodu przepisów dotyczących zatrzymywania danych jest mało prawdopodobne, aby posłużyły się telekomunikacją w celu nawiązania kontaktu z terapeutą uzależnień, psychoterapeutą lub poradnią małżeńską" [tłumaczenie nieoficjalne].

85 — Jako że zatrzymywane dane obejmują lokalizację źródła i odbiorcy komunikatu, każda osoba wysyłająca lub otrzymująca komunikat podczas manifestacji może zostać łatwo zidentyfikowana dzięki zatrzymanym danym. W tym względzie Marc Goodman, specjalista FBI i Interpolu w dziedzinie zagrożeń związanych z nowymi technologiami, relacjonuje, że niedawno rząd Ukrainy podczas manifestacji opozycji dokonał identyfikacji wszystkich telefonów komórkowych znajdujących się w pobliżu starć ulicznych między siłami porządkowymi i zwolennikami opozycji. Wszystkie te telefony otrzymały wówczas wiadomość, którą ów autor opisał jako pewnie najbardziej „orwellowską" wiadomość kiedykolwiek wysłaną przez rząd: „Szanowny abonencie, został Pan zarejestrowany jako uczestnik poważnych zakłóceń porządku publicznego" (M. Goodman, *Future Crimes*, Anchor Books, New York 2016, s. 153, wolny przekład). Zobacz także Rada Praw Człowieka ONZ, sprawozdanie specjalnego sprawozdawcy ds. wolności opinii i wypowiedzi, 17 kwietnia 2013 r., A/HRC/23/40, nr 75; Rada Praw Człowieka ONZ, sprawozdanie Wysokiego Komisarza Narodów Zjednoczonych do spraw Praw Człowieka na temat prawa do poszanowania życia prywatnego w dobie łączności cyfrowej, 30 czerwca 2014 r., A/HRC/27/37, nr 3.

86 — Zobacz w tym względzie Rada Praw Człowieka ONZ, sprawozdanie Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka na temat prawa do poszanowania życia prywatnego w dobie łączności cyfrowej, 30 czerwca 2014 r., A/HRC/27/37, nr 19: „Idąc podobnym tokiem rozumowania, niektórzy prezentują pogląd, że przechwytywanie – lub gromadzenie – danych na temat komunikatów, a nie ich treści, nie stanowi jako takie ingerencji w życie prywatne. Tymczasem z punktu widzenia prawa do poszanowania życia prywatnego rozróżnienie to nie jest przekonujące. Zbiory informacji określanych powszechnie mianem »metadanych« mogą zawierać wskazówki dotyczące zachowania danej osoby, jej stosunków społecznych, jej preferencji prywatnych i jej tożsamości, *które wykraczają znacznie poza to, czego można dowiedzieć się z treści* prywatnego komunikatu" (wyróżnienie moje). Zobacz także Zgromadzenie Ogólne ONZ, sprawozdanie specjalnego sprawozdawcy Narodów Zjednoczonych dotyczące wspierania i ochrony praw człowieka i podstawowych wolności w ramach walki z terroryzmem, 23 września 2014 r., A/69/397, nr 53 [tłumaczenia nieoficjalne].

260. Dodam, że ryzyko nadużycia dostępu lub niezgodnego z prawem dostępu do zatrzymanych danych wcale nie jest tylko teoretyczne. Po pierwsze, ryzyko nadużycia dostępu przez właściwe organy należy łączyć ze skrajnie dużą liczbą wniosków o dostęp, przywołaną w uwagach przedstawionych Trybunałowi. W odniesieniu do systemu szwedzkiego spółka Tele2 Sverige oświadczyła, że otrzymywała około 10 000 wniosków o dostęp miesięcznie, a jest to liczba, która nie obejmuje wniosków otrzymywanych przez innych dostawców prowadzących działalność na terytorium Szwecji. W odniesieniu do systemu Zjednoczonego Królestwa T. Watson przedstawił liczby pochodzące ze sprawozdania urzędowego, mówiące o 517 236 zezwoleniach i 55 346 pilnych zezwoleniach ustnych wyłącznie w odniesieniu do roku 2014. Po drugie, ryzyko niezgodnego z prawem dostępu przez dowolną osobę jest nierozłącznym skutkiem samego tylko istnienia baz danych przechowywanych na nośnikach elektronicznych [87].

261. Moim zdaniem do sądów odsyłających należy ocena – zgodnie z orzecznictwem przypomnianym w pkt 247 niniejszej opinii – czy niedogodności powodowane przez ogólne obowiązki zatrzymywania danych rozpatrywane w postępowaniach głównych nie są w demokratycznym społeczeństwie nadmierne w porównaniu do zamierzonych celów. W ramach tej oceny sądy te powinny wyważyć zagrożenia i korzyści związane z takim obowiązkiem, a mianowicie:

— z jednej strony korzyści związane z zapewnieniem organom zajmującym się walką z poważnymi przestępstwami ograniczonej zdolności do odtwarzania przeszłości [88], a

— z drugiej strony poważne zagrożenia wynikające w demokratycznym społeczeństwie z uprawnienia do rejestrowania życia prywatnego jednostki i z uprawnienia do katalogowania całej populacji.

262. Oceny tej należy dokonać w świetle wszystkich istotnych cech krajowych systemów rozpatrywanych w postępowaniach głównych. W tym względzie podkreślam, że wiążące gwarancje określone przez Trybunał w pkt 60–68 wyroku DRI to jedynie gwarancje minimalne, służące ograniczeniu naruszenia praw przyznanych w dyrektywie 2002/58 i w art. 7 i 8 karty do tego, co absolutnie konieczne. Nie jest zatem wykluczone, że system krajowy zawierający wszystkie te gwarancje musi jednak zostać uznany za nieproporcjonalny w demokratycznym społeczeństwie z powodu dysproporcji między poważnymi zagrożeniami spowodowanymi przez ów obowiązek w demokratycznym społeczeństwie a wynikającymi z tego obowiązku korzyściami w walce z poważnymi przestępstwami.

VI – **Wnioski**

263. Mając na uwadze powyższe rozważania, proponuję Trybunałowi, by na pytania prejudycjalne przedstawione przez Kammarrätten i Stockholm (administracyjny sąd apelacyjny w Sztokholmie, Szwecja) oraz Court of Appeal (England & Wales) (Civil Division) [sąd apelacyjny (Anglia i Walia) (wydział cywilny), Zjednoczone Królestwo] odpowiedział następująco:

Artykuł 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywy o prywatności i łączności elektronicznej), zmienionej dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r., oraz art. 7, 8 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że nie stoją one na przeszkodzie temu, aby państwo członkowskie nałożyło na dostawców usług łączności elektronicznej obowiązek

87 — Zobacz w szczególności Rada Praw Człowieka ONZ, sprawozdanie specjalnego sprawozdawcy ds. wolności opinii i wypowiedzi, 17 kwietnia 2013 r., A/HRC/23/40, nr 67: „Bazy danych dotyczących łączności stają się podatne na kradzież, oszustwa i przypadkowe ujawnienie" [tłumaczenie nieoficjalne].

88 — Zobacz pkt 178–183 niniejszej opinii.

zatrzymywania wszystkich danych dotyczących komunikatów przekazywanych przez użytkowników ich usług, jeżeli spełnione są wszystkie następujące warunki, czego ustalenie w świetle wszystkich istotnych cech systemów krajowych spornych w postępowaniach głównych należy do sądów odsyłających:

— obowiązek ten i towarzyszące mu gwarancje muszą zostać ustanowione przez przepisy ustawowe lub wykonawcze, które posiadają cechy przystępności, przewidywalności i ochrony przed arbitralnością;

— obowiązek ten i towarzyszące mu gwarancje muszą szanować istotę praw uznanych w art. 7 i 8 karty praw podstawowych;

— obowiązek ten musi być absolutnie konieczny do walki z poważnymi przestępstwami, co oznacza, że żaden inny środek ani kombinacja środków nie mogłyby być równie skuteczne w walce z poważnymi przestępstwami, będąc jednocześnie mniej szkodliwe dla praw ustanowionych w dyrektywie 2002/58 i w art. 7 i 8 karty praw podstawowych;

— obowiązek ten musi być obwarowany wszystkimi gwarancjami wymienionymi przez Trybunał w pkt 60–68 wyroku z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in. (C-293/12 i C-594/12, EU:C:2014:238), dotyczącymi dostępu do danych, okresu przechowywania oraz ochrony i bezpieczeństwa danych, w celu ograniczenia naruszenia praw ustanowionych w dyrektywie 2002/58 i w art. 7 i 8 karty praw podstawowych do tego, co absolutnie konieczne, oraz

— obowiązek ten musi być proporcjonalny w społeczeństwie demokratycznym do celu walki z poważnymi przestępstwami, co oznacza, że poważne zagrożenia spowodowane przez ten obowiązek w społeczeństwie demokratycznym nie mogą być nadmierne wobec wynikających z niego korzyści w walce z poważnymi przestępstwami.