Zbiór Orzeczeń

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

Sprawa C-623/17

Privacy International
przeciwko
Secretary of State for Foreign and Commonwealth Affairs,
Secretary of State for the Home Department,
Government Communications Headquarters,
Security Service,
Secret Intelligence Service

[wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Investigatory Powers Tribunal (sąd ds. uprawnień dochodzeniowych, Zjednoczone Królestwo)]

Odesłanie prejudycjalne – Przetwarzanie danych osobowych i ochrona prywatności w sektorze łączności elektronicznej – Dyrektywa 2002/58/WE – Zakres zastosowania – Artykuł 1 ust. 3 – Artykuł 15 ust. 3 – Karta praw podstawowych Unii Europejskiej – Artykuły 7, 8, 51 i art. 52 ust. 1 – Artykuł 4 ust. 2 TUE – Uogólnione i niezróżnicowane przekazywanie służbom bezpieczeństwa danych o połączeniach użytkowników usługi łączności elektronicznej

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

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

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

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

1 Język oryginału: hiszpański.

2 Sprawy połączone C-293/12 i C-594/12, EU:C:2014:238.

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

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

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

6 Sprawa C-207/16, EU:C:2018:788.

2. Wyroki te (w szczególności drugi z nich) budzą niepokój władz niektórych państw członkowskich, bowiem ich zdaniem prowadzą one do pozbawienia ich instrumentu, który państwa te uważają za niezbędny dla zapewnienia bezpieczeństwa narodowego i walki z terroryzmem. Dlatego też niektóre z państw członkowskich opowiadają się za uchyleniem lub doprecyzowaniem tego orzecznictwa.

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

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

I. Ramy prawne

A. Prawo Unii

5. Odsyłam do odpowiedniego punktu mojej opinii przedstawionej w sprawach połączonych C-511/18 i C-512/18.

B. Prawo krajowe (znajdujące zastosowanie w niniejszym sporze)

1. Telecommunications Act 1984 [11]

6. Zgodnie z art. 94 tej ustawy sekretarz stanu może wydawać operatorowi publicznej sieci łączności elektronicznej takie ogólne lub szczegółowe polecenia, jakie uzna za konieczne w interesie bezpieczeństwa narodowego lub stosunków z rządem kraju lub terytorium znajdującego się poza Zjednoczonym Królestwem.

2. Data Retention and Investigatory Powers Act 2014 [12]

7. Artykuł 1 tej ustawy stanowi:

„(1) Sekretarz stanu może w drodze nakazu zatrzymania zażądać od publicznego operatora telekomunikacyjnego zatrzymania określonych danych dotyczących łączności, jeżeli uzna, że jest to niezbędne i proporcjonalne w odniesieniu do jednego lub więcej celów, o których mowa w art. 22 ust. 2 lit. a)–h) Regulation of Investigatory Powers Act 2000 [(ustawy regulującej uprawnienia dochodzeniowe z 2000 r.; zwanej dalej »RIPA«)].

7 Poza niniejszą sprawą chodzi o sprawy połączone C-511/18 i C-512/18 La Quadrature du Net i in. oraz sprawę C-520/18, Ordre des barreaux francophones et germanophone i in., w których opinie również przedstawiono w dniu dzisiejszym.

8 Sprawa Privacy International, C-623/17.

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

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

11 Ustawa o telekomunikacji z 1984 r., zwana dalej „ustawą z 1984 r.”.

12 Ustawa z 2014 r. o zatrzymywaniu danych i uprawnieniach dochodzeniowych, zwana dalej „DRIPA”.

(2) Nakaz zatrzymania może:

(a) dotyczyć konkretnego operatora lub wszystkich operatorów;

(b) zobowiązywać do zatrzymywania wszystkich danych albo wszystkich danych określonego rodzaju;

(c) określać okres lub okresy, podczas których dane mają być zatrzymywane;

(d) zawierać inne wymogi lub ograniczenia dotyczące zatrzymywania danych;

(e) zawierać odmienne postanowienia ze względu na odmienne cele;

(f) odwoływać się do danych istniejących lub nieistniejących w dacie wydania lub wejścia w życie nakazu zatrzymania.

(3) Sekretarz stanu może w drodze rozporządzenia ustanowić kolejne przepisy dotyczące zatrzymywania określonych danych dotyczących łączności.

(4) Przepisy te mogą dotyczyć w szczególności:

(a) wymogów poprzedzających wydanie nakazu zatrzymania;

(b) maksymalnego okresu zatrzymania danych na podstawie nakazu zatrzymania;

(c) treści, wydania, wejścia w życie, przeglądu, zmiany lub uchylenia nakazu zatrzymania;

(d) integralności, bezpieczeństwa lub ochrony danych zatrzymanych na podstawie niniejszego artykułu, dostępu do danych oraz ich ujawnienia lub zniszczenia;

(e) spełnienia właściwych wymogów lub przestrzegania ograniczeń oraz weryfikacji zgodności z nimi;

(f) kodeksu dobrych praktyk w zakresie właściwych wymogów, ograniczeń lub uprawnień;

(g) zwrotu przez sekretarza stanu (ewentualnie pod pewnymi warunkami) kosztów poniesionych przez publicznych operatorów telekomunikacyjnych w celu spełnienia właściwych wymogów lub przestrzegania ograniczeń,

[…]

(5) Maksymalny okres przewidziany w zastosowaniu ust. 4 lit. b) nie może przekraczać 12 miesięcy od daty wskazanej w odniesieniu do danych objętych uregulowaniami, o których mowa w ust. 3.

(6) Publiczny operator telekomunikacyjny, który zatrzymuje określone dane dotyczące łączności na podstawie niniejszego artykułu, nie może ujawnić tych danych, chyba że:

(a) ujawnia je na podstawie:

(i) rozdziału 2 części 1 [RIPA]; lub

(ii) orzeczenia sądu lub innego zezwolenia sądowego; lub

(b) jest to przewidziane w uregulowaniu, o którym mowa w ust. 3.

(7) Sekretarz stanu może w drodze rozporządzenia wydać przepisy odnoszące się do wszelkich przepisów wydanych (lub które mają zostać wydane) na podstawie ust. 4 lit. d)–g) lub ust. 6, związane z danymi dotyczącymi łączności zatrzymanymi przez dostawców usług telekomunikacyjnych na podstawie kodeksu dobrych praktyk zgodnie z art. 102 ustawy z 2001 r. o zwalczaniu terroryzmu i przestępczości oraz o bezpieczeństwie [Anti-terrorism, Crime and Security Act 2001]".

3. RIPA

8. Artykuł 21 tej ustawy stanowi:

„[…]

(4) Do celów niniejszego rozdziału »dane dotyczące łączności« oznaczają:

(a) dane o ruchu zawarte w komunikacie lub powiązane z nim (przez nadawcę lub w inny sposób) dla celów dowolnej usługi pocztowej lub systemu telekomunikacyjnego, za pomocą którego komunikat ten jest lub może być transmitowany;

(b) wszelkie informacje, które nie obejmują treści komunikatu [z wyłączeniem informacji, o których mowa w lit. a)], dotyczące korzystania przez dowolną osobę:

(i) z dowolnej usługi pocztowej lub telekomunikacyjnej; lub

(ii) w zakresie związanym ze świadczeniem na rzecz dowolnej osoby lub korzystaniem przez nią z dowolnej usługi telekomunikacyjnej w ramach części systemu telekomunikacyjnego;

(c) wszelkie informacje nienależące do zakresu uregulowanego w lit. a) i b), które znajdują się w posiadaniu lub zostały uzyskane przez osobę świadczącą usługi pocztowe lub usługi telekomunikacyjne, w zakresie dotyczącym osób, na rzecz których owe usługi są świadczone.

[…]

(6) W niniejszym artykule pojęcie »danych dotyczących ruchu« użyte w odniesieniu do dowolnego komunikatu oznacza:

(a) wszelkie dane identyfikujące lub mogące identyfikować dowolną osobę, urządzenie lub miejsce, do którego lub z którego jest lub może być przekazywany komunikat;

(b) wszelkie dane identyfikujące lub selekcjonujące bądź mogące identyfikować lub selekcjonować urządzenie z wykorzystaniem którego jest lub może być przekazywany komunikat;

(c) wszelkie dane zawierające sygnały służące działaniu urządzenia wykorzystywanego w systemach łączności dla celów przekazywania dowolnego komunikatu; oraz

(d) wszelkie dane identyfikujące dane zawarte lub dołączone do danego komunikatu lub inne dane zawarte lub dołączone do danego komunikatu.

[…]".

9. Artykuł 22 przewiduje:

„(1) Artykuł ten ma zastosowanie w przypadku, kiedy osoba odpowiedzialna w rozumieniu niniejszego rozdziału uważa za konieczne, z przyczyn wymienionych w ust. 2 poniżej, uzyskanie dowolnych danych dotyczących łączności.

(2) Z przyczyn wskazanych w niniejszym ustępie uzyskanie danych dotyczących łączności jest konieczne, jeżeli jest to niezbędne

(a) w interesie bezpieczeństwa narodowego;

(b) w celu zapobiegania lub wykrywania przestępczości albo zapobiegania zakłóceniom porządku publicznego;

(c) w interesie dobrobytu gospodarczego Zjednoczonego Królestwa, jeżeli interesy te są równie istotne dla interesów bezpieczeństwa narodowego;

(d) w interesie bezpieczeństwa publicznego;

(e) w celu ochrony zdrowia publicznego;

(f) w celu kontroli nałożenia lub poboru jakiegokolwiek podatku, cła, opłaty lub innego obciążenia, wkładu lub opłaty należnej na rzecz organów administracji publicznej;

(g) w celu zapobiegania w nagłych przypadkach śmierci, uszkodzeniu ciała lub jakiemukolwiek uszczerbkowi dla zdrowia fizycznego lub psychicznego osoby fizycznej albo w celu złagodzenia jakiegokolwiek uszkodzenia ciała lub uszczerbku dla zdrowia fizycznego lub psychicznego osoby fizycznej;

(h) w każdym innym celu [niewskazanym w lit. a)–g)] określonym w nakazie wydanym przez sekretarza stanu na podstawie art. 22 ust. 2 lit. h) [DRIPA].

(4) Z zastrzeżeniem ust. 5, kiedy osoba odpowiedzialna uzna, że operator telekomunikacyjny lub pocztowy jest lub może być w posiadaniu danych lub może być w stanie je posiadać, może ona zażądać od operatora telekomunikacyjnego lub operatora pocztowego, aby ten:

(a) uzyskał dane, jeżeli jeszcze ich nie posiada; oraz

(b) w każdym przypadku ujawnił wszelkie posiadane dane oraz dane uzyskane w późniejszym czasie.

(5) Osoba odpowiedzialna może udzielić zgody na podstawie ust. 3 lub wystąpić z żądaniem na podstawie ust. 4 jedynie wtedy, gdy uzna, że uzyskanie określonych danych wynikające z działań prowadzonych na podstawie zezwolenia lub wymaganych na podstawie zezwolenia lub żądania jest proporcjonalne do zamierzonego celu uzyskania danych”.

10. Jeżeli istnieje powód, aby sądzić, że dane zostały uzyskane w sposób nieprawidłowy, wówczas zgodnie z brzmieniem art. 65 można wnieść skargę do Investigatory Powers Tribunal (sądu ds. uprawnień dochodzeniowych, Zjednoczone Królestwo).

II. Okoliczności faktyczne leżące u podstaw sporu i pytania prejudycjalne

11. Zdaniem sądu odsyłającego postępowanie główne dotyczy uzyskiwania i wykorzystywania masowych danych telekomunikacyjnych przez United Kingdom Security and Intelligence Agencies (służby bezpieczeństwa i wywiadu Zjednoczonego Królestwa; zwane dalej „SIA").

12. Dane te dotyczą tego, „kto" wykorzystuje telefon i Internet oraz „kiedy, gdzie, jak i z kim" je wykorzystuje. Obejmują one lokalizację telefonów komórkowych i stacjonarnych, z których wykonywane lub odbierane są połączenia, a także komputerów, z których uzyskuje się dostęp do Internetu. Nie obejmują one treści komunikatów, które mogą zostać uzyskane wyłącznie w drodze nakazu sądowego.

13. Strona skarżąca w postępowaniu głównym (Privacy International, organizacja pozarządowa działająca na rzecz ochrony praw człowieka) wniosła skargę do sądu odsyłającego, ponieważ uznała, iż uzyskiwanie i wykorzystywanie wspomnianych danych przez SIA narusza prawo do poszanowania życia prywatnego ustanowione w art. 8 Europejskiej konwencji praw człowieka (zwanej dalej „EKPC") oraz jest sprzeczne z prawem Unii.

14. Strony, przeciwko którym wniesiono skargę [13], utrzymują, że korzystają ze swoich uprawnień w sposób zgodny z prawem i konieczny, w szczególności, w celu ochrony bezpieczeństwa narodowego.

15. Zgodnie z informacjami zawartymi w postanowieniu odsyłającym na podstawie poleceń wydawanych przez sekretarza stanu w oparciu o art. 94 ustawy z 1984 r. SIA otrzymują masowe dane telekomunikacyjne od operatorów publicznych sieci łączności elektronicznej.

16. Wspomniane dane obejmują informacje o ruchu i lokalizacji oraz informacje o działalności społecznej, handlowej i finansowej, połączeniach i podróżach użytkowników. SIA przechowują uzyskane dane w bezpieczny sposób, stosując techniki nieukierunkowane (na przykład ich filtrowanie, zestawianie i agregację), to znaczy nienakierowane na konkretne i znane cele.

17. Sąd odsyłający uważa za udowodnione, iż techniki te są niezbędne w pracy SIA w celu zwalczania poważnych zagrożeń dla bezpieczeństwa publicznego, w szczególności terroryzmu, szpiegostwa i rozprzestrzeniania broni jądrowej. Możliwość uzyskiwania i wykorzystywania tych danych przez SIA ma kluczowe znaczenie dla ochrony bezpieczeństwa narodowego Zjednoczonego Królestwa.

18. Zdaniem sądu odsyłającego rozpatrywane środki są zgodne z prawem krajowym oraz art. 8 EKPC. Jednak w świetle wyroku Tele2 Sverige i Watson powziął on wątpliwości w zakresie ich zgodności z prawem Unii.

19. W tej sytuacji sąd odsyłający przedstawił Trybunałowi Sprawiedliwości następujące pytania prejudycjalne:

„1) Uwzględniając art. 4 TUE i art. 1 ust. 3 dyrektywy 2002/58 […] – czy zawarty w poleceniu sekretarza stanu dla dostawcy sieci łączności elektronicznej wymóg, zgodnie z którym dostawca ten musi przekazać masowe dane telekomunikacyjne służbom wywiadu i bezpieczeństwa państwa członkowskiego, wchodzi w zakres prawa Unii oraz dyrektywy o prywatności i łączności elektronicznej?

13 Secretary of State for Foreign and Commonwealth Affairs (sekretarz stanu spraw zagranicznych i Commonwealth, Zjednoczone Królestwo), Secretary of State for the Home Department (sekretarz stanu spraw wewnętrznych, Zjednoczone Królestwo) oraz trzy SIA Zjednoczonego Królestwa, to jest Government Communications Headquarters (sztab łączności rządowej Zjednoczonego Królestwa, GCHQ), Security Service (służba kontrwywiadu, Zjednoczone Królestwo) (MI5) oraz Secret Intelligence Service (służba wywiadu, Zjednoczone Królestwo) (MI6).

2) Jeżeli odpowiedź na pytanie pierwsze jest twierdząca, to czy do takiego polecenia sekretarza stanu zastosowanie mają którekolwiek z wymogów zawartych w wyroku Watson[14] lub inne wymogi, poza wymogami sformułowanymi przez Konwencję o ochronie praw człowieka i podstawowych wolności? Jeśli tak, w jaki sposób i w jakim zakresie zastosowanie mają takie wymogi, biorąc pod uwagę konieczność zastosowania przez służby wywiadu i bezpieczeństwa technik masowego uzyskiwania i automatycznego przetwarzania w celu ochrony bezpieczeństwa narodowego oraz zakres, w jakim możliwości takie, o ile są zgodne z Konwencją o ochronie praw człowieka i podstawowych wolności, mogą być w istotny sposób osłabione przez sformułowanie takich wymagań?".

20. Sąd odsyłający wyjaśnia kontekst zadanych przez siebie pytań w następujący sposób:

„a) możliwości wykorzystywania przez SIA [masowych danych telekomunikacyjnych], które zostały im przekazane, są konieczne do ochrony bezpieczeństwa narodowego Zjednoczonego Królestwa, w tym w obszarach zwalczania terroryzmu oraz przeciwdziałania szpiegostwu i rozprzestrzenianiu broni jądrowej;

b) SIA wykorzystują [masowe dane telekomunikacyjne] głównie w celu wykrywania wcześniej nieznanych zagrożeń dla bezpieczeństwa narodowego przez zastosowanie masowych technik nieukierunkowanych na konkretne osoby, opartych na gromadzeniu [tych danych] w jednym miejscu. Służy to przede wszystkim szybkiej identyfikacji i rozpracowaniu celu, a także zapewnieniu podstaw do podjęcia działań w obliczu bezpośredniego zagrożenia;

c) dostawca sieci łączności elektronicznej nie ma potem obowiązku zatrzymania [masowych danych telekomunikacyjnych] (przez okres dłuższy niż przewidują to jego zwykłe wymogi biznesowe), a dane te zatrzymuje wyłącznie państwo (SIA);

d) sąd krajowy ustalił (z wyjątkiem pewnych zastrzeżonych kwestii), że zabezpieczenia towarzyszące wykorzystywaniu [masowych danych telekomunikacyjnych] przez SIA są zgodne z wymogami EKPC; oraz

e) sąd krajowy stwierdził, że narzucenie wymogów określonych w [wyroku Tele2 Sverige i Watson], o ile mają zastosowanie, zniweczyłoby środki podjęte w celu ochrony bezpieczeństwa narodowego przez służby wywiadu i bezpieczeństwa i tym samym zagroziłoby bezpieczeństwu narodowemu Zjednoczonego Królestwa".

III. Postępowanie przed Trybunałem Sprawiedliwości

21. Wniosek o wydanie orzeczenia w trybie prejudycjalnym wpłynął do Trybunału Sprawiedliwości w dniu 31 października 2017 r.

22. Uwagi na piśmie przedstawiły rządy belgijski, cypryjski, czeski estoński, francuski, niemiecki, węgierski, irlandzki, łotewski, niderlandzki, norweski, polski, portugalski, hiszpański, szwedzki i rząd Zjednoczonego Królestwa oraz Komisja.

23. Rozprawa odbyła się w dniu 9 września 2019 r. i dotyczyła również spraw połączonych C-511/18 i C-512/18 oraz sprawy C-520/18. W rozprawie wzięły udział strony czterech postępowań prejudycjalnych, wskazane powyżej rządy oraz Komisja i Europejski Inspektor Ochrony Danych Osobowych.

14 To jest wymogów zawartych w wyroku Tele2 Sverige i Watson.

IV. Ocena

A. W przedmiocie zakresu zastosowania dyrektywy 2002/58 i wyłączenia kwestii bezpieczeństwa narodowego (pierwsze pytanie prejudycjalne)

24. W przedstawionej dziś opinii w sprawach połączonych C-511/18 i C-512/18 wyjaśniam powody, dla których moim zdaniem dyrektywa 2002/58 „ma zastosowanie co do zasady w przypadku, gdy dostawcy usług elektronicznych są ustawowo zobowiązani do przechowywania danych ich abonentów i do umożliwienia dostępu do nich organom władzy publicznej. Bez znaczenia jest przy tym okoliczność, że obowiązki te są nakładane na dostawców ze względów związanych z bezpieczeństwem narodowym” [15].

25. Rozwijając moją argumentację, przeanalizuję wpływ wyroków Trybunału Sprawiedliwości z dnia 30 maja 2006 r. w sprawach: Parlament Europejski/Rada i Komisja [16] oraz Tele2 Sverige i Watson, proponując przyjęcie ich całościowej wykładni [17].

26. W niniejszej opinii, po stwierdzeniu, że dyrektywa 2002/58 znajduje zastosowanie, przeanalizuję zawarte w niej wyłączenie odnoszące się do bezpieczeństwa narodowego oraz wpływ art. 4 ust. 2 TUE [18].

27. Z zastrzeżeniem poniższych wyjaśnień odsyłam do analiz przeprowadzonych w opinii przywołanej powyżej oraz opinii przedstawionej w sprawie C-520/18.

1. Zastosowanie dyrektywy 2002/58 w niniejszej sprawie

28. Zgodnie z rozpatrywanym w niniejszej sprawie uregulowaniami obowiązek obejmujący, poza zatrzymywaniem danych, przetwarzanie danych posiadanych przez nich w wyniku świadczenia usług na rzecz użytkowników publicznych sieci łączności w Unii jest nałożony na dostawców usług łączności elektronicznej [19].

29. Wspomniani operatorzy są zobowiązani przekazywać te dane SIA. Powstaje zatem pytanie, czy art. 15 ust. 1 dyrektywy 2002/58 zezwala na to, aby takie przekazywanie, z uwagi na jego cel, zostało wyłączone z zakresu stosowania prawa Unii.

30. Uważam, że nie. Zatrzymywanie, a następnie przekazywanie tych danych można uznać za przetwarzanie danych osobowych dokonywane przez dostawców usług łączności elektronicznej, co w naturalny sposób wpisuje się w zakres zastosowania dyrektywy 2002/58.

31. Względy związane z bezpieczeństwem narodowym nie mogą przeważyć nad tym ustaleniem, jak to sugeruje sąd odsyłający, w rezultacie bowiem rozpatrywany obowiązek zostałby wyłączony z zakresu zastosowania prawa Unii. Moim zdaniem, powtarzam, dostawcy przetwarzają dane w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii, co zgodnie z art. 3 ust. 1 dyrektywy 2002/58 mieści się dokładnie w zakresie jej zastosowania.

15 Opinia w sprawach połączonych C-511/18 i C-512/18, La Quadrature du Net i in., pkt 42.

16 Sprawy połączone C-317/04 i C-318/04, EU:C:2006:346.

17 Opinia w sprawach połączonych C-511/18 i C-512/18, La Quadrature du Net i in., pkt 44–76.

18 Ibidem, pkt 77–90.

19 Zgodnie z art. 2 dyrektywy 2002/58 na potrzeby tej dyrektywy stosuje się definicje zawarte w dyrektywie 95/46. Zgodnie z art. 2 lit. b) dyrektywy 95/46 przez „przetwarzanie danych osobowych” rozumie się „każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, *ujawnianie poprzez transmisję*, rozpowszechnianie lub *udostępnianie w inny sposób*, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie” (podkreślenie moje).

32. Jeśli przyjąć to założenie, to spór nie dotyczy już działalności SIA (które, jak wskazałem powyżej, mogłyby zostać wyłączone z zakresu zastosowania prawa Unii, jeżeli nie wywierałyby wpływu na operatorów łączności elektronicznej), lecz zatrzymywania i późniejszego przekazywania danych posiadanych przez wspomnianych operatorów. Z tego punktu widzenia w grę wchodzą prawa podstawowe gwarantowane przez Unię.

33. Elementem kluczowym dla rozstrzygnięcia tej kwestii jest, ponownie, obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych, do których dostęp jest następnie przekazywany organom władzy publicznej.

2. Odwołanie do bezpieczeństwa narodowego

34. Biorąc pod uwagę, iż w niniejszej sprawie sąd odsyłający kładzie szczególny nacisk na działania SIA mające wpływ na bezpieczeństwo narodowe, pozwalam sobie przytoczyć dotyczące tej kwestii punkty mojej przedstawionej dziś opinii w sprawach połączonych C-511/18 i C-512/18:

„77. Bezpieczeństwo narodowe […] zostało wskazane w dyrektywie 2002/58 w dwojakim znaczeniu. Po pierwsze, stanowi ono podstawę *wyłączenia* (stosowania tej dyrektywy) w odniesieniu do wszystkich rodzajów działalności państw członkowskich, które »go dotyczą«. Po drugie, stanowi ono podstawę *ograniczenia*, które musi nastąpić w drodze ustawy, praw i obowiązków ustanowionych w dyrektywie 2002/58, to znaczy w odniesieniu do działalności o charakterze prywatnym lub handlowym i niezwiązanej z *zastrzeżonymi* tylko dla państwa dziedzinami *działalności*.

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

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

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

[…]

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

[…]

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

85. »Równowaga«, o której mowa w […] motywie [jedenastym dyrektywy 2002/58], wynika z konieczności poszanowania kompetencji przysługujących państwom członkowskim w dziedzinie bezpieczeństwa narodowego, gdy państwa te wykonują owe kompetencje w *sposób bezpośredni i przy użyciu własnych środków*. Natomiast w przypadku gdy, nawet z tych samych względów związanych z bezpieczeństwem narodowym, wymagany jest udział jednostek, na które nakładane są określone obowiązki, przesądza to o objęciu uregulowaną prawem Unii dziedziną (ochrony życia prywatnego przysługującej tych podmiotom prywatnym).

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

[…]

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

3. Skutki zastosowania w niniejszej sprawie wyroku Tele2 Sverige i Watson

35. Sąd odsyłający skupił się na wykładni dokonanej przez Trybunał Sprawiedliwości w wyroku Tele2 Sverige i Watson, podkreślając trudności, które jego zdaniem wiązałyby się z jej zastosowaniem w niniejszej sprawie.

36. W wyroku Tele2 Sverige i Watson wskazano bowiem wymogi, jakie musi spełnić uregulowanie krajowe wprowadzające obowiązek zatrzymywania danych o ruchu i lokalizacji w celu ich późniejszego udostępnienia organom władzy publicznej.

37. Podobnie jak w sprawach połączonych C-511/18 i C-512/18 i z analogicznych względów uważam, iż rozpatrywane w niniejszej sprawie przepisy prawa krajowego nie spełniają wymogów ustanowionych w wyroku Tele2 Sverige i Watson, gdyż prowadzą one do uogólnionego i niezróżnicowanego zatrzymywania danych osobowych, co umożliwia dostęp przez długi czas do szczegółowych informacji o życiu osób, których te dane dotyczą.

38. W opinii przedstawionej w dwóch wspomnianych sprawach rozważam, czy byłoby możliwe zmodyfikowanie lub uzupełnienie stanowiska wyrażonego w tym wyroku, aby uwzględnić skutki, jakie pociąga ono dla walki z terroryzmem lub dla ochrony państwa przed innymi podobnymi zagrożeniami bezpieczeństwa narodowego.

39. Pozwolę sobie również przytoczyć poniżej te punkty przywołanej opinii, w których utrzymuję w istocie, iż, choć istnieje możliwość zmodyfikowania przywołanego orzecznictwa, to należy je w jego istocie utrzymać w mocy:

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

136. Zadanie to ma typowo ustawodawczy charakter, w wyznaczonych w orzecznictwie Trybunału granicach […].

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

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

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

B. W przedmiocie drugiego pytania prejudycjalnego

40. Sąd odsyłający zadaje swoje drugie pytanie na wypadek udzielenia przez Trybunał odpowiedzi twierdzącej na pytanie pierwsze. W takim przypadku sąd ten zmierza do ustalenia, jakie „inne wymogi, poza wymogami nałożonymi przez EKPC” czy też wymogami wynikającymi z wyroku Tele2 Sverige i Watson powinny mieć zastosowanie.

41. Stwierdza on w tym względzie, iż narzucenie wymogów określonych w wyroku Tele2 Sverige i Watson „zniweczyłoby środki podjęte w celu ochrony bezpieczeństwa narodowego przez służby wywiadu i bezpieczeństwa”.

42. Z uwagi na to, że odpowiedź, jakiej proponuję udzielić na pytanie pierwsze, jest przecząca, nie ma konieczności ustosunkowywania się do drugiego pytania. Jak wskazuje sam sąd odsyłający, jest ono bowiem uzależnione od stwierdzenia zgodności z prawem Unii „technik masowego uzyskiwania i automatycznego przetwarzania” danych osobowych wszystkich użytkowników ze Zjednoczonego Królestwa, które dostawcy usług łączności elektronicznej powinni przekazywać SIA.

43. Gdyby Trybunał Sprawiedliwości uznał za konieczne udzielenie odpowiedzi na pytanie drugie, uważam, iż należałoby potwierdzić określone w wyroku Tele2 Sverige i Watson wskazane powyżej wymogi odnoszące się do:

– zakazu uogólnionego dostępu do danych;

– potrzeby uprzedniego uzyskania sądu lub niezależnego organu zezwolenia na taki dostęp;

– obowiązku poinformowania osób, których dane są przetwarzane, z wyjątkiem sytuacji, kiedy zagraża to skuteczności tego środka;

– przechowywania danych na obszarze Unii.

44. Wystarczyłoby zatem, powtórzę, potwierdzić konieczność spełnienia tych wymogów ze względów, które wyjaśniłem w opiniach przedstawionych w sprawach połączonych C-511/18 i C-512/18 oraz w sprawie C-520/18, bez potrzeby wprowadzania „innych", dodatkowych wymogów, w znaczeniu, do którego odnosi się sąd odsyłający.

V. Wnioski

45. Mając na względzie powyższe rozważania, proponuję, aby Trybunał Sprawiedliwości udzielił Investigatory Powers Tribunal (sądowi ds. uprawnień dochodzeniowych, Zjednoczone Królestwo) następującej odpowiedzi:

Artykuł 4 TUE oraz art. 1 ust. 3 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) należy interpretować w ten sposób, że stoją one na przeszkodzie uregulowaniu krajowemu, które zobowiązuje dostawcę sieci łączności elektronicznej do przekazywania służbom wywiadu i bezpieczeństwa państwa członkowskiego „masowych danych telekomunikacyjnych", co wiąże się z uprzednim uogólnionym i niezróżnicowanym zbieraniem tych danych.

Tytułem ewentualnym:

Dostęp służb wywiadu i bezpieczeństwa państwa członkowskiego do danych przekazywanych przez dostawców sieci łączności elektronicznej powinien być zgodny z wymogami wynikającymi z wyroku z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970.