Zbiór Orzeczeń

OPINIA RZECZNIKA GENERALNEGO
GIOVANNIEGO PITRUZZELLI
przedstawiona w dniu 21 stycznia 2020 r.[1]

Sprawa C-746/18

H.K.
przeciwko
Prokuratuur

[wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Riigikohus (sąd najwyższy, Estonia)]

Odesłanie prejudycjalne – Przetwarzanie danych osobowych w sektorze łączności elektronicznej – Poufność komunikacji – Dostawcy usług łączności elektronicznej – Uogólnione i niezróżnicowane zatrzymywanie danych dotyczących ruchu i danych o lokalizacji – Dochodzenia – Dostęp organu dochodzeniowego do zatrzymanych danych za okresy o długości od jednego dnia do jednego roku – Zgoda udzielona przez prokuratora – Wykorzystanie danych w ramach postępowania karnego w charakterze dowodów – Dyrektywa 2002/58/WE – Artykuł 1 ust. 3, art. 3 i art. 15 ust. 1 – Karta praw podstawowych Unii Europejskiej – Artykuły 7, 8 i 11 oraz art. 52 ust. 1

I. Wprowadzenie

1. Niniejszy wniosek o wydanie orzeczenia w trybie prejudycjalnym dotyczy wykładni art. 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[2], zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r.[3], w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej[4].

2. Wniosek ten został złożony w ramach postępowania karnego wszczętego przeciwko H.K. ze względu na popełnienie szeregu kradzieży, posłużenie się kartą bankową należącą do innej osoby i dopuszczenie się przemocy wobec osoby uczestniczącej w postępowaniu sądowym.

3. Protokoły, na których opiera się ustalenie popełnienia tych przestępstw, zostały sporządzone w szczególności na podstawie danych osobowych powstałych w związku ze świadczeniem usług łączności elektronicznej. Riigikohus (sąd najwyższy, Estonia) wyraża wątpliwości co do zgodności z prawem Unii warunków, w jakich organy dochodzeniowe uzyskały dostęp do tych danych.

1 Język oryginału: francuski.

2 Dz.U. 2002, L 201, s. 37.

3 Dz.U. 2009, L 337, s. 11. Zwanej dalej „dyrektywą 2002/58”.

4 Zwanej dalej „kartą”.

4. Wątpliwości te dotyczą w pierwszej kolejności kwestii tego, czy okres, w odniesieniu do którego organy dochodzeniowe miały dostęp do danych, stanowi kryterium pozwalające ocenić wagę ingerencji, jaką stanowi ów dostęp, w prawa podstawowe podmiotów danych.

5. W drugiej kolejności sąd odsyłający zmierza do ustalenia, czy Prokuratuur (prokuratura, Estonia), biorąc pod uwagę różne zadania powierzone jej przez przepisy estońskie, stanowi „niezależny" organ administracyjny w rozumieniu wyroku z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in.[5].

II. Ramy prawne

A. Dyrektywa 2002/58

6. Artykuł 1 ust. 3 dyrektywy 2002/58/WE stanowi, że nie ma ona „zastosowania do działalności, która wykracza poza zakres Traktatu ustanawiającego Wspólnotę Europejską, takiej jak działalność określona w tytułach V i VI Traktatu o Unii Europejskiej, ani, w żadnym wypadku, do działalności dotyczącej bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając dobrobyt gospodarczy państwa, gdy działalność odnosi się do spraw bezpieczeństwa państwa) i działalności państwa w dziedzinie prawa karnego".

7. Ponadto art. 15 ust. 1 omawianej dyrektywy stanowi, że „[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, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego ([np.] bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy 95/46/WE[6]. W tym celu państwa członkowskie mogą między innymi uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa [Unii], w tym zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej".

B. Prawo estońskie

1. Ustawa o łączności elektronicznej

8. Elektroonilise side seadus (ustawa o łączności elektronicznej)[7] z dnia 8 grudnia 2004 r., w brzmieniu mającym zastosowanie do sporu w postępowaniu głównym, stanowi w § 111[1], zatytułowanym „Obowiązek zatrzymywania danych":

„[…]

(2) Operatorzy usług telefonii stacjonarnej lub komórkowej i usług sieci telefonii stacjonarnej i telefonii komórkowej są zobowiązani przechowywać następujące dane:

1) numer osoby wywołującej oraz nazwę i adres abonenta;

5 C-203/15 i C-698/15, zwanego dalej „wyrokiem Tele2 Sverige i Watson i in.", EU:C:2016:970 [pkt 120 i pkt 2 sentencji].

6 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).

7 RT I 2004, 87, 593.

2) numer osoby wywoływanej i nazwę i adres abonenta;

3) w wypadku usług dodatkowych takich jak przekazywanie lub przekierowanie połączeń – wybrany numer oraz nazwę i adres abonenta;

4) datę i godzinę rozpoczęcia i zakończenia połączenia;

5) wykorzystaną usługę telefonii stacjonarnej lub komórkowej;

6) międzynarodowy identyfikator abonenta sieci komórkowej (International Mobile Subscriber Identity – IMSI) osoby wywołującej i wywoływanej;

7) międzynarodowy identyfikator urządzenia ruchomego (International Mobile Equipment Identity – IMEI) osoby wywołującej i wywoływanej;

8) identyfikator lokalizacji w chwili rozpoczęcia połączenia;

9) dane pozwalające ustalić położenie geograficzne komórek przez odniesienie się do ich identyfikatorów lokalizacji w czasie, przez który zatrzymywane są dane;

10) w przypadku anonimowych usług opłaconych z góry – datę i dokładny czas początkowej aktywacji usługi oraz identyfikator lokalizacji, w której dokonano aktywacji usługi.

[…]

(4) Dane, o których mowa w ust. 2 i 3 niniejszego paragrafu, są przechowywane przez okres jednego roku od dnia połączenia, jeżeli zostały wygenerowane lub przetworzone podczas świadczenia usługi łączności […].

[…]

(11) Dane, o których mowa w ust. 2 i 3 niniejszego paragrafu, są przekazywane:

1) zgodnie z kriminaalmenetluse seadustik [kodeksem postępowania karnego [8]] organowi dochodzeniowemu, organowi uprawnionemu do podejmowania środków nadzoru, prokuraturze, sądowi;

[…]”.

2. Kodeks postępowania karnego

9. Paragraf 17 kodeksu postępowania karnego, w brzmieniu mającym zastosowanie do sporu w postępowaniu głównym, zatytułowany „Strony postępowania sądowego”, stanowi w ust. 1:

„Stronami postępowania sądowego są: prokuratura […]”

10. Zgodnie z § 30 kodeksu postępowania karnego, zatytułowanym „Prokuratura w postępowaniu karnym”:

„(1) Prokuratura kieruje postępowaniem przygotowawczym, zapewniając jego legalność i skuteczność, i jest oskarżycielem publicznym przed sądem.

8 RT I 2003, 27, 166.

(2) Kompetencje prokuratury w ramach postępowania karego wykonuje w jej imieniu prokurator, który działa w sposób niezależny i związany jest jedynie ustawą".

11. Paragraf 90^1 kodeksu postępowania karnego, zatytułowany „Żądanie danych od przedsiębiorstw łączności", przewiduje w ust. 2 i 3:

„(2) Organ dochodzeniowy może za zgodą prokuratury w toku postępowania przygotowawczego lub za zgodą sądu w toku postępowania sądowego zażądać od dostawcy usług łączności elektronicznej danych wymienionych w § 111^1 ust. 2 i 3 ustawy o łączności elektronicznej, które nie są wymienione w ust. 1 niniejszego paragrafu. Ta zgoda powinna dokładnie wskazywać okres, którego może dotyczyć żądanie danych.

(3) Zgodnie z niniejszym paragrafem można żądać danych tylko, jeżeli jest to niezbędne do osiągnięcia celu postępowania karnego".

12. Paragraf 211 kodeksu postępowania karnego, zatytułowany „Cel postępowania przygotowawczego", ma następujące brzmienie:

„(1) Celem postępowania przygotowawczego jest zgromadzenie dowodów i stworzenie pozostałych warunków do przeprowadzenia procesu.

(2) W toku postępowania przygotowawczego organ dochodzeniowy i prokuratura ustalają okoliczności odciążające i obciążające podejrzanego lub oskarżonego".

3. Ustawa o prokuraturze

13. Prokuratuuriseadus (ustawa o prokuraturze)[9] z dnia 22 kwietnia 1998 r., w brzmieniu mającym zastosowanie do sporu w postępowaniu głównym, stanowi w § 1, zatytułowanym „Prokuratura":

„(1) Prokuratura jest organem rządowym, podległym Justiitsministeeriumi [ministerstwu sprawiedliwości, Estonia], który bierze udział w planowaniu działań monitorowania niezbędnych do wykrywania i zwalczania przestępstw, kieruje postępowaniem przygotowawczym, zapewniając jego legalność i skuteczność, pełni funkcję oskarżyciela publicznego przed sądem oraz wykonuje inne zadania spoczywające na niej na mocy ustawy.

(1^1) Prokuratura wypełnia w sposób niezależny swoje zadania ustawowe i działa na podstawie niniejszej ustawy, innych ustaw i aktów prawnych wydanych na podstawie tych ustaw.

[…]".

14. Paragraf 2 ustawy o prokuraturze, zatytułowany „Prokurator", stanowi w ust. 2:

„Prokurator jest niezależny przy wypełnianiu swoich zadań i działa wyłącznie zgodnie z ustawą i własnymi przekonaniami".

9 RT I 1998, 41, 625.

III. Okoliczności faktyczne, postępowanie główne i pytania prejudycjalne

15. Wyrokiem z dnia 6 kwietnia 2017 r. H.K. została skazana przez Viru Maakohus (sąd pierwszej instancji Viru, Estonia) na karę dwóch lat pozbawienia wolności za popełnienie w okresie od 4 sierpnia 2015 r. do 1 lutego 2016 r. ośmiu kradzieży artykułów spożywczych i innych dóbr materialnych o wartości od 3 do 40 EUR, a także kwot pieniężnych od 5,20 do 2100 EUR, za wykorzystanie karty bankowej innej osoby w celu pobrania pieniędzy z bankomatu i wyrządzenie przez to tej osobie szkody w wysokości 3941,82 EUR i za popełnienie aktów przemocy wobec osoby biorącej udział w postępowaniu sądowym [10].

16. Skazując H.K. za te przestępstwa, Viru Maakohus (sąd pierwszej instancji Viru) oparł się między innymi na szeregu protokołów sporządzonych na podstawie danych dotyczących łączności elektronicznej, o których mowa w § 111^1 ust. 2 ustawy o łączności elektronicznej, otrzymanych przez organ dochodzeniowy od dostawcy usług telekomunikacyjnych w toku postępowania przygotowawczego, po uzyskaniu na podstawie § 90^1 ust. 2 kodeksu postępowania karnego zgód udzielonych przez prokuratora Viru Ringkonnaprokuratuur (prokuratury okręgowej Viru, Estonia).

17. I tak w dniu 2 listopada 2015 r. prokurator z prokuratury okręgowej Viru udzielił zgody organowi dochodzeniowemu na żądanie od przedsiębiorstwa telekomunikacyjnego dostarczenia danych, o których mowa w § 111^1 ust. 2 ustawy o łączności elektronicznej, celem ustalenia za pomocą dwóch numerów telefonu komórkowego należącego do H.K. transmisji połączeń i wiadomości, ich czasu trwania, rodzaju transmisji, a także danych osobowych oraz lokalizacji osoby wywołującej i wywoływanej w dniu 21 września 2015 r.

18. W odniesieniu do danych uzyskanych od przedsiębiorstwa telekomunikacyjnego na podstawie tej zgody organ dochodzeniowy sporządził w dniu 4 listopada 2015 r. protokół wskazujący maszty emisyjne, w których zasięgu używany był w dniu 21 września 2015 r. po godz. 19.00 numer abonencki, z którego korzystała H.K. Prokuratura zmierzała do wykazania przed sądem poprzez ten protokół wraz z innymi dowodami, że H.K. dopuściła się kradzieży, która miała miejsce w dniu 21 września 2015 r.

19. W dniu 25 lutego 2016 r. zastępca prokuratora prokuratury okręgowej Viru dla celów śledztwa dotyczącego przestępstwa z § 303 ust. 1 Karistusseadustik (kodeksu karnego) [11] udzielił organowi dochodzeniowemu zgody na zażądanie od przedsiębiorstwa telekomunikacyjnego dostarczenia danych, o których mowa w § 111^1 ust. 2 ustawy o łączności elektronicznej, dotyczących siedmiu numerów abonenckich, którymi dysponowała H.K. w okresie od 1 marca 2015 r. do 19 lutego 2016 r.

20. Na podstawie danych uzyskanych od przedsiębiorstwa telekomunikacyjnego dzięki tej zgodzie organ dochodzeniowy sporządził w dniu 15 marca 2016 r. protokół wskazujący daty, w których H.K. dzwoniła do współoskarżonych i odbierała od nich telefony, a także daty, w których wysyłała do współoskarżonych i otrzymywała od nich wiadomości. Prokuratura zmierza do wykazania przed sądem poprzez ten protokół wraz z innymi dowodami, że H.K. od wiosny 2015 r. wielokrotnie groziła współoskarżonym przez telefon.

10 Sąd odsyłający uściśla, że doszło do połączenia tej kary z karą pozbawienia wolności w wymiarze czterech lat i siedmiu miesięcy, na którą H.K. została skazana przez Viru Maakohus (sąd pierwszej instancji Viru) wyrokiem z dnia 22 marca 2016 r., w związku z czym ostatecznie H.K. została skazana na odbycie kary łącznej pięciu lat i jednego miesiąca pozbawienia wolności.

11 Chodzi o przestępstwo polegające na wywieraniu wpływu na wymiar sprawiedliwości. Pragnę zauważyć, że kwalifikacja czynów zarzucanych H.K. została w tym względzie zmieniona przez Viru Maakohus (sąd pierwszej instancji Viru) zgodnie z § 323 ust. 1 kodeksu karnego na przemoc w odniesieniu do uczestnika postępowania sądowego.

21. Dzięki tej samej zgodzie w dniach 20 kwietnia i 6 maja 2016 r. organ dochodzeniowy sporządził jeszcze protokoły dotyczące danych uzyskanych od przedsiębiorstwa telekomunikacyjnego. Protokoły te wskazują stacje bazowe, w obszarze których z sześciu numerów abonenckich wykorzystywanych przez H. K wykonywano i odbierano połączenia telefoniczne w dniach 4, 27 i 31 sierpnia 2015 r., a także w dniach od 1 do 3 września 2015 r. Dzięki wspomnianym protokołom oraz całości pozostałych dowodów prokuratura zamierzała wykazać przed sądem, że sześć kradzieży we wskazanych dniach zostało popełnionych przez H.K.

22. W dniu 20 kwietnia 2016 r. organ dochodzeniowy sporządził protokół zawierający dane dotyczące dwóch numerów abonenckich używanych przez H.K. Mówiąc dokładniej, w protokole tym określono stacje bazowe, w obszarze których za pośrednictwem tych numerów abonenckich w dniach od 16 do 19 stycznia 2015 r. nawiązywano i przyjmowano połączenia. Prokurator zmierzał do wykazania poprzez ten protokół wraz z innymi dowodami, że H.K. jest osobą, która w dniach od 17 do 19 stycznia 2015 r. wypłacała pieniądze z bankomatu, używając karty bankowej poszkodowanego.

23. Dane użyte w rzeczonym protokole zostały uzyskane od przedsiębiorstwa telekomunikacyjnego dzięki zgodom udzielonym w dniach 28 stycznia i 2 lutego 2015 r. przez prokuratora naczelnego prokuratury okręgowej Viru w innej sprawie karnej. Przedmiotem tej sprawy karnej było przestępstwo z § 200 ust. 2 pkt 7, 8 i 9 kodeksu karnego, a mianowicie dwie kradzieże z rozbojem popełnione w dniach 23 i 27 stycznia 2015 r. przez grupę z użyciem broni i z włamaniem. Na podstawie tych zgód organ dochodzeniowy mógł zażądać od przedsiębiorstwa telekomunikacyjnego dostarczenia w odniesieniu do okresu od 1 stycznia do 2 lutego 2015 r. danych, o których mowa w § 111^1 ust. 2 ustawy o łączności elektronicznej, dotyczących obu numerów abonenckich oraz różnych międzynarodowych identyfikatorów urządzenia ruchomego H.K.

24. Z tego opisu okoliczności faktycznych postępowania głównego wynika, że prokuratura zgodnie z § 90^1 ust. 2 kodeksu postępowania karnego zezwoliła organowi dochodzeniowemu na skierowanie do przedsiębiorstwa telekomunikacyjnego w ramach postępowania przygotowawczego żądań udostępnienia danych. Zgody zostały udzielone dla celów dochodzenia dotyczącego różnych przestępstw w odniesieniu do danych obejmujących numery abonenckie oskarżonej na okres, odpowiednio, jednego dnia, około jednego miesiąca oraz około jednego roku.

25. H.K. wniosła apelację od orzeczenia Viru Maakohus (sądu pierwszej instancji Viru) do Tartu Ringkonnakohus (sądu apelacyjnego w Tartu, Estonia), który oddalił tę apelację orzeczeniem z dnia 17 listopada 2017 r. W związku z tym H.K. wniosła skargę kasacyjną do Riigikohus (sądu najwyższego), żądając uchylenia orzeczeń pierwszej i drugiej instancji, zakończenia postępowania karnego przeciwko niej oraz jej uniewinnienia.

26. H.K. podnosi, że protokoły zawierające dane uzyskane od przedsiębiorstwa telekomunikacyjnego nie są dopuszczalnymi dowodami i że jej skazanie na podstawie tych protokołów jest bezzasadne. Zgodnie z wyrokiem Tele2 Sverige i Watson i in. przepisy § 111^1 ustawy o łączności elektronicznej przewidujące zobowiązanie tych dostawców usług do zatrzymywania danych dotyczących łączności oraz wykorzystanie tych danych do celów jej skazania są sprzeczne z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty.

27. Zdaniem sądu odsyłającego powstaje zatem pytanie, czy rozpatrywane protokoły sporządzone przez organ dochodzeniowy na podstawie danych, o których mowa w § 111^1 ust. 2 ustawy o łączności elektronicznej, zażądanych od przedsiębiorstwa telekomunikacyjnego za zgodą prokuratury, można uznać za dopuszczalne.

28. Dane, które dostawcy usług łączności elektronicznej mają obowiązek zatrzymywać przez okres jednego roku, obejmują między innymi numer osoby wywołującej i wywoływanej, nazwę i adres abonenta, datę i godzinę rozpoczęcia i zakończenia połączenia, wykorzystaną usługę telefonii stacjonarnej lub komórkowej, międzynarodowy identyfikator abonenta sieci komórkowej

i międzynarodowy identyfikator urządzenia ruchomego osoby wywołującej i wywoływanej, jak też identyfikator komórki w chwili rozpoczęcia połączenia i dane pozwalające ustalić położenie geograficzne komórki. Sąd odsyłający wskazuje przy tym, że chodzi o dane, które są związane z transmisją połączeń i wiadomości za pomocą telefonu stacjonarnego lub komórkowego, jak też z lokalizacją urządzenia łączności ruchomej, ale nie dostarczają żadnych informacji o treści połączeń.

29. Jak wynika z wyroków Tele2 Sverige i Watson i in. oraz z dnia 2 października 2018 r., Ministerio Fiscal [12], przepisy krajowe regulujące zatrzymywanie danych o ruchu i danych o lokalizacji, a także dostęp do tych danych w ramach postępowania karnego, takie jak § 111^1 ust. 2 i 4 ustawy o łączności elektronicznej i § 90^1 ust. 2 kodeksu postępowania karnego, wchodzą w zakres stosowania dyrektywy 2002/58.

30. Dopuszczalność dowodów zależy od poszanowania reguł proceduralnych regulujących ich zbieranie. Zatem przy ocenie dopuszczalności spornych w postępowaniu głównym protokołów jako dowodów należy zbadać również kwestię tego, w jakim zakresie zbieranie od przedsiębiorstwa telekomunikacyjnego danych, na których opierają się te protokoły, było zgodne z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty.

31. Mając na uwadze wyroki Tele2 Sverige i Watson i in. [13] oraz Ministerio Fiscal [14], sąd odsyłający zastanawia się, czy art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty należy interpretować w ten sposób, że dostęp organów państwowych do danych, które pozwalają na ustalenie miejsca nawiązania i zakończenia połączenia telefonicznego z telefonu stacjonarnego lub komórkowego osoby podejrzanej, jego datę, godzinę i czas trwania oraz rodzaj, użyte urządzenie łączności i lokalizację użytego urządzenia łączności ruchomej, stanowi na tyle poważną ingerencję w prawa podstawowe gwarantowane wspomnianymi artykułami karty, że dostęp ten musi być ograniczony do zwalczania poważnych przestępstw kryminalnych, niezależnie od okresu, w odniesieniu do którego organy państwowe zwróciły się o dostęp do przechowywanych danych.

32. W tym względzie sąd odsyłający uważa, że długość okresu objętego żądaniem przekazania danych stanowi istotny element oceny wagi ingerencji w prawa podstawowe, jaką jest dostęp do rozpatrywanych danych. Jest zatem możliwe, że nie należy uznawać tej ingerencji za poważną, ponieważ wymagane dane dotyczą jedynie bardzo krótkiego okresu, takiego jak jeden dzień. W takiej sytuacji, ogólnie rzecz biorąc, z danych tych nie można wyciągnąć szczegółowych wniosków dotyczących życia prywatnego podmiotu danych, a zatem dostęp organów państwowych do rzeczonych danych może być uzasadniony celem ogólnym w postaci dochodzenia i ścigania przestępstw.

33. Ponadto sąd odsyłający zastanawia się nad kwestią tego, czy w świetle wniosków wynikających z wyroku Ministerio Fiscal [15] dostęp do danych takich, jak będące przedmiotem sporu w postępowaniu głównym, można uzasadnić tym samym celem, w przypadku gdy ilość danych, do których organy mają dostęp, jest ograniczona i w rezultacie ingerencja w rozpatrywane prawa podstawowe nie jest poważna. Co się tyczy ilości danych, ważne jest uwzględnienie rodzaju danych (takich jak dane dotyczące adresata połączenia lub lokalizacji urządzenia) i czasu trwania (na przykład jeden dzień, jeden miesiąc lub jeden rok). Zdaniem tego sądu im poważniejsze jest przestępstwo, tym poważniejsza może być dozwolona ingerencja w prawa podstawowe w ramach postępowania, co oznacza, że tym większa jest ilość danych, do których organy państwowe mogą mieć dostęp.

12 C-207/16, zwany dalej „wyrokiem Ministerio Fiscal”, EU:C:2018:788.

13 Punkt 2 sentencji tego wyroku.

14 Punkty 53, 57 tego wyroku.

15 Punkty 55–57 tego wyroku.

34. Wreszcie sąd odsyłający zastanawia się, czy prokuraturę można uznać za „niezależny" organ administracyjny w rozumieniu wyroku Tele2 Sverige i Watson i in.[16]. Podnosi, że w Estonii to właśnie prokuratura kieruje postępowaniem przygotowawczym, którego celem jest między innymi zgromadzenie dowodów. Podkreśla również, że organ dochodzeniowy i prokuratura weryfikują dowody obciążające i dowody odciążające dotyczące podejrzanego. Wreszcie sąd zauważa, że kompetencje prokuratury wykonuje w jej imieniu prokurator, który realizuje swoje zadania w sposób niezależny, co wynika z § 30 ust. 1 i 2 kodeksu postępowania karnego oraz § 1 ust. 1 i 1^1, a także z § 2 ust. 2 ustawy o prokuraturze.

35. W tym kontekście sąd odsyłający podkreśla, że jego wątpliwości co do niezależności wymaganej przez prawo Unii są przede wszystkim konsekwencją faktu, że prokuratura po przeprowadzeniu postępowania przygotowawczego wnosi akt oskarżenia wobec danej osoby, jeżeli jest przekonana, że w sprawie karnej zostały zebrane wszystkie niezbędne dowody i są podstawy do tego. Sąd ten wskazuje, że w takim przypadku to właśnie prokuratora podczas procesu jest oskarżycielem publicznym i jest tym samym stroną postępowania. Sąd odsyłający podnosi również, że Europejski Trybunał Praw Człowieka przyznał już, że w określonych warunkach środki nadzoru są dopuszczone także bez uprzedniej kontroli sądowej, jeżeli kontrola sądowa odbywa się a posteriori[17].

36. W tych okolicznościach Riigikohus (sąd najwyższy) postanowił zawiesić postępowanie i skierować do Trybunału następujące pytania prejudycjalne:

„1) Czy art. 15 ust. 1 dyrektywy [2002/58] w związku z art. 7, 8, 11 i art. 52 ust. 1 [karty] należy interpretować w ten sposób, że w postępowaniu karnym dostęp organów państwowych do danych, które pozwalają na ustalenie miejsca nawiązania i zakończenia połączenia telefonicznego z telefonu stacjonarnego lub komórkowego osoby podejrzanej, jego datę, godzinę i czas trwania oraz rodzaj, użyte urządzenie i lokalizację użytego urządzenia łączności ruchomej, stanowi na tyle poważną ingerencję w prawa podstawowe gwarantowane wspomnianymi artykułami karty, że dostęp ten musi być ograniczony do zapobiegania, dochodzenia, wykrywania i karania poważnych przestępstw kryminalnych, niezależnie od okresu, w odniesieniu do którego organy państwowe mają dostęp do przechowywanych danych?

2) Czy art. 15 ust. 1 dyrektywy [2002/58] należy interpretować w oparciu o zasadę proporcjonalności przywołaną w pkt 55–57 wyroku [Ministerio Fiscal] w ten sposób, że jeżeli ilość wspomnianych w pytaniu pierwszym danych, do których organy państwowe mają dostęp, nie jest bardzo duża (zarówno pod względem ich rodzaju, jak i rozmiaru czasowego), wynikająca z tego ingerencja w prawa podstawowe może być uzasadniona w sposób ogólny zapobieganiem, dochodzeniem, wykrywaniem i karaniem przestępstw kryminalnych, i że im większa jest ilość danych, do których mają dostęp organy państwowe, tym poważniejsze muszą być przestępstwa kryminalne, których zwalczaniu ma służyć ingerencja?

3) Czy określony w pkt 2 sentencji wyroku [Tele2 Sverige i Watson i in.] wymóg, by dostęp właściwych organów krajowych do danych był poddany uprzedniej kontroli przez sąd lub niezależny organ administracyjny, oznacza, że art. 15 ust. 1 dyrektywy [2002/58] należy interpretować w ten sposób, iż za niezależny organ administracyjny można uznać prokuraturę, która kieruje postępowaniem przygotowawczym i jest przy tym na mocy ustawy zobowiązana do działania niezależnego i podlega tylko ustawie, a w ramach postępowania przygotowawczego bada zarówno okoliczności łagodzące, jak i obciążające oskarżonego, ale w późniejszym postępowaniu sądowym pełni funkcję oskarżyciela publicznego?".

16 Punkt 120 wyroku i pkt 2 sentencji wyroku.

17 Sąd odsyłający przytacza w tym względzie wyroki ETPC: z dnia 2 września 2010 r. w sprawie Uzun przeciwko Niemcom (CE:ECHR:2010:0902JUD003562305, §§ 71–74); z dnia 12 stycznia 2016 r. w sprawie Szabó i Vissy przeciwko Węgrom (CE:ECHR:2016:0112JUD003713814, § 77).

IV. Analiza

37. Poprzez pytania pierwsze i drugie sąd odsyłający zmierza w istocie do ustalenia, czy art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty należy interpretować w ten sposób, że do kryteriów pozwalających ocenić wagę ingerencji w prawa podstawowe, jaką jest udostępnienie właściwym organom państwowym danych osobowych, które dostawcy usług łączności elektronicznej mają obowiązek zatrzymywać na mocy przepisów krajowych, należą kategorie udostępnianych danych oraz długość okresu, dla którego wystąpiono o dostęp.

38. Przed udzieleniem odpowiedzi na to pytanie sformułuję dwie serie uwag wstępnych, które pozwolą mi na udzielenie odpowiedzi, po pierwsze, na argumenty podniesione przez niektóre państwa członkowskie w odniesieniu do zakresu stosowania dyrektywy 2002/58, a po drugie, na propozycję ze strony Komisji Europejskiej, by w ramach niniejszego odesłania prejudycjalnego zbadać zgodność z prawem Unii przepisów estońskich w zakresie, w jakim nakładają one na dostawców usług łączności elektronicznej obowiązek zatrzymywania szeregu kategorii danych osobowych generowanych w ramach tych usług.

A. Uwagi wstępne

1. W przedmiocie zakresu stosowania dyrektywy 2002/58

39. Rządy irlandzki, węgierski i polski podnoszą wątpliwości co do zakresu stosowania dyrektywy 2002/58.

40. Rząd irlandzki uważa, jak się wydaje, że uregulowanie krajowe dotyczące dostępu organów właściwych w sprawach karnych do zatrzymanych danych jest na mocy art. 1 ust. 3 dyrektywy 2002/58 wyłączone z jej zakresu stosowania.

41. Argument ten należy oddalić na podstawie orzecznictwa Trybunału wynikającego z wyroków Tele2 Sverige i Watson i in. oraz Ministerio Fiscal.

42. Należy w tym względzie wskazać, że Trybunał orzekł już, iż środki ustawodawcze, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, „są objęte zakresem stosowania tej dyrektywy, nawet jeśli odnoszą się do działalności właściwej państwom lub organom państwowym i niezwiązanej z dziedzinami, w których prowadzą działalność jednostki, nawet jeżeli cele, którym środki te mają służyć, są zasadniczo zbieżne z celami działalności, o których mowa w art. 1 ust. 3 dyrektywy 2002/58”[18]. Zdaniem Trybunału, „[a]rtykuł 15 ust. 1 owej dyrektywy stosuje się bowiem przy założeniu, że środki krajowe, które są w nim wymienione, wchodzą w zakres stosowania tej dyrektywy, ponieważ ta ostatnia upoważnia wyraźnie państwa członkowskie do ich przyjmowania wyłącznie z poszanowaniem ustanowionych w niej warunków. Ponadto środki ustawodawcze, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, normują działalność dostawców usług łączności elektronicznej do celów, o których mowa w tym przepisie”[19].

43. Trybunał stwierdził na tej podstawie, iż „wspomniany art. 15 ust. 1 w związku z art. 3 dyrektywy 2002/58 należy interpretować w ten sposób, że do zakresu stosowania tej dyrektywy należy nie tylko środek ustawodawczy, który nakłada na dostawców usług łączności elektronicznej obowiązek zatrzymywania danych o ruchu i danych o lokalizacji, lecz również środek ustawodawczy dotyczący dostępu organów krajowych do danych zatrzymywanych przez owych dostawców”[20].

18 Wyrok Ministerio Fiscal (pkt 34 i przytoczone tam orzecznictwo).

19 Ibidem.

20 Wyrok Ministerio Fiscal (pkt 35 i przytoczone tam orzecznictwo).

44. Otóż, zdaniem Trybunału, „[z]agwarantowana w art. 5 ust. 1 dyrektywy 2002/58 ochrona poufności łączności elektronicznej i związanych z nimi danych dotyczących ruchu znajduje bowiem zastosowanie do środków stosowanych przez podmioty inne niż użytkownicy, niezależnie od tego, czy są to podmioty prywatne, czy też państwowe. Jak potwierdza motyw 21 tej dyrektywy, ma ona na celu uniemożliwienie każdego niedozwolonego »dostępu« do komunikatów, włączając w to »dane związane z tego rodzaju komunikatem«, w celu ochrony poufności łączności elektronicznej” [21].

45. W odniesieniu do tych argumentów Trybunał dodał, że „środki ustawodawcze nakładające na dostawców usług łączności elektronicznej obowiązek zatrzymywania danych osobowych lub udzielenia właściwym organom krajowym dostępu do tych danych, wymagają przetwarzania wspomnianych danych przez tych dostawców […]. Środki takie, w zakresie, w jakim regulują działalność wspomnianych dostawców, nie mogą zatem być traktowane jako działalność właściwa państwom, o której mowa w art. 1 ust. 3 dyrektywy 2002/58” [22].

46. Zgodnie z tym, co Trybunał orzekł w wyroku Ministerio Fiscal [23], z ogółu tych argumentów wynika, że wniosek o udzielenie dostępu do danych osobowych zatrzymywanych przez dostawców usług łączności elektronicznej, złożony w ramach karnego postępowania przygotowawczego, wchodzi w zakres stosowania dyrektywy 2002/58.

47. Ponadto rządy węgierski i polski podnoszą argument, zgodnie z którym prawo Unii nie reguluje kwestii dopuszczalności dowodów w postępowaniu karnym.

48. O ile prawdą jest, że prawo to na obecnym etapie swojego rozwoju nie reguluje zasad dotyczących dopuszczalności dowodów w postępowaniu karnym, o tyle sąd odsyłający wyraźnie wskazał, dlaczego wykładnia prawa Unii, o której dokonanie wnosi, jest niezbędna do tego, aby mógł wypowiedzieć się w przedmiocie dopuszczalności dowodów. Ich dopuszczalność zależy bowiem od przestrzegania warunków i przepisów proceduralnych regulujących gromadzenie tych dowodów. Zatem przy ocenie dopuszczalności spornych w postępowaniu głównym protokołów jako dowodów sąd odsyłający powinien zbadać kwestię wstępną, w jakim zakresie zbieranie od przedsiębiorstwa telekomunikacyjnego danych, na których opierają się te protokoły, było zgodne z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty. Ta kwestia wstępna dotyczy zaś aspektu, który jak podkreśliłem wcześniej, jest regulowany przez prawo Unii. W tym względzie przepisy krajowe mające zastosowanie do postępowania dowodowego muszą dochowywać wymogów wynikających z praw podstawowych gwarantowanych prawem Unii [24]. W tych okolicznościach argument podniesiony przez rządy węgierski i polski jest moim zdaniem pozbawiony znaczenia.

2. W przedmiocie zatrzymywania danych o ruchu i danych o lokalizacji

49. Nawet jeśli pytania przedstawione przez sąd odsyłający dotyczą warunków dostępu do danych, Komisja zwraca się do Trybunału o wypowiedzenie się w ramach niniejszego odesłania prejudycjalnego również w przedmiocie problematyki dotyczącej zatrzymywania danych. W tym względzie zauważa ona w istocie, że zgodny z prawem dostęp do zatrzymanych danych wymaga, aby uregulowanie krajowe nakładające na dostawców usług łączności elektronicznej obowiązek przechowywanie danych generowanych w ramach ich usług spełniało wymogi określone w art. 15 ust. 1 dyrektywy 2002/58 w związku z postanowieniami karty lub aby dane te były zatrzymywane przez tych dostawców z ich własnej inicjatywy, w szczególności w celach handlowych, zgodnie z tą samą dyrektywą.

21 Wyrok Ministerio Fiscal (pkt 36 i przytoczone tam orzecznictwo).

22 Wyrok Ministerio Fiscal (pkt 37 i przytoczone tam orzecznictwo).

23 Wyrok Ministerio Fiscal (pkt 38, 39).

24 Zobacz w szczególności analogicznie wyrok z dnia 10 kwietnia 2003 r., Steffensen (C-276/01, EU:C:2003:228, pkt 71). W wyroku tym Trybunał odniósł się również do tej problematyki z punktu widzenia zasady skuteczności jako ograniczenia autonomii proceduralnej państw członkowskich (pkt 66–68 wspomnianego wyroku).

50. Jeśli chodzi o sprawę w postępowaniu głównym, Komisja zauważa, że dane, do których organ dochodzeniowy miał dostęp, były zatrzymywane przez dostawców usług łączności elektronicznej nie z własnej inicjatywy w celach handlowych, lecz z tytułu obowiązku zatrzymywania nałożonego na nie w § 111[1] ustawy o łączności elektronicznej. Podnosi ona również, że H.K. kwestionuje zgodność z prawem przepisów krajowych dotyczących zarówno dostępu do danych, jak i ich zatrzymywania [25].

51. Mając to na względzie, pragnę zauważyć, że podobnie jak to miało miejsce w przypadku wniosku o wydanie orzeczenia w trybie prejudycjalnym leżącego u źródła wyroku Ministerio Fiscal [26], pytania przedstawione przez sąd odsyłający w ramach niniejszej sprawy nie mają na celu ustalenia, czy dane osobowe będące przedmiotem postępowania głównego były zatrzymywane przez dostawców usług łączności elektronicznej z poszanowaniem warunków określonych w art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty. Pytania te dotyczą wyłącznie zgodności z tymi przepisami warunków, w jakich dostęp krajowych organów dochodzeniowych do takich danych jest dozwolony na mocy przepisów estońskich. Dlatego debata, która zawiązała się przed Trybunałem, dotyczyła niemal wyłącznie tychże warunków dostępu.

52. W każdym razie sąd odsyłający, jeżeli uzna za konieczne w celu rozstrzygnięcia zawisłego przed nim sporu orzeczenie w przedmiocie zgodności z prawem Unii § 111[1] ustawy o łączności elektronicznej, może oprzeć się na orzecznictwie wynikającym z wyroku Tele2 Sverige i Watson i in.

53. W tym względzie pozwolę sobie po prostu przypomnieć, że zdaniem Trybunału „art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8, 11 i art. 52 ust. 1 karty należy interpretować w ten sposób, iż stoi on na przeszkodzie uregulowaniu krajowemu przewidującemu do celów zwalczania przestępczości uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej” [27].

54. Do sądu odsyłającego należy sprawdzenie w razie potrzeby, czy przepisy estońskie nakładają na dostawców usług łączności elektronicznej obowiązek zatrzymywania danych, który ma charakter uogólniony i niezróżnicowany, oraz do wyciągnięcia z tego konsekwencji dla celów rozstrzygnięcia sporu w postępowaniu głównym. Gdyby system zatrzymywania danych wprowadzony przez Republikę Estońską należało uznać za niezgodny z prawem Unii z uwagi na to, że jest nieproporcjonalny w świetle realizowanego celu, dostęp do danych zatrzymanych w jego ramach również nie mógłby być uzasadniony tym samym celem.

55. Jedynie wówczas, gdy ów obowiązek zatrzymywania zostanie poddany odpowiednim ograniczeniom, w szczególności w odniesieniu do kategorii odnośnych danych i okresu ich zatrzymywania, w ramach systemu zapewniającego ich zróżnicowanie w zależności od realizowanego celu, w zakresie absolutnie koniecznym dla osiągnięcia tego celu, obowiązek ten będzie mógł spełnić kryterium proporcjonalności.

56. W ramach niniejszej opinii nie omówię dokładniej pojęcia „ograniczonego zatrzymywania danych”, które szczegółowo przeanalizował rzecznik generalny M. Campos Sánchez-Bordona w opinii, która przedstawił w dniu 15 stycznia 2020 r. w sprawie Ordre des barreaux francophones et germanophone i in. [28].

25 Komisja podkreśla w tym kontekście, że niniejsza sprawa różni się od sprawy, w której zapadł wyrok Ministerio Fiscal.

26 Wyrok Ministerio Fiscal (pkt 49, 50).

27 Zobacz wyrok Tele2 Sverige i Watson i in. (pkt 112).

28 C-520/18, EU:C:2020:7. Zobacz w szczególności punkty 72–107 tej opinii.

B. W przedmiocie dostępu właściwych organów państwowych do zatrzymanych danych

1. Wnioski płynące z wyroku Tele2 Sverige i Watson i in.

57. Trybunał rozważa problematykę dostępu właściwych organów państwowych do zatrzymanych danych „niezależnie od zakresu obowiązku zatrzymywania danych nałożonego na dostawców usług łączności elektronicznej", a w szczególności niezależnie od uogólnionego lub indywidualnego charakteru zatrzymywania danych [29]. Jest to związane z faktem, że Trybunał uznaje zatrzymywanie danych i dostęp do nich za dwie odrębne ingerencje w prawa podstawowe chronione kartą.

58. Dostęp do zatrzymanych danych powinien „odpowiadać rzeczywiście i ściśle jednemu z […] celów", o których mowa w art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58. Musi również istnieć zgodność pomiędzy wagą ingerencji a realizowanym celem. Jeśli ingerencja zostanie uznana za „poważną", może być uzasadniona jedynie względami związanymi z poważną przestępczością [30].

59. Tak jak ma to miejsce w przypadku zatrzymywania danych, dostęp do nich uzyskiwany przez właściwe organy państwowe jest dopuszczalny wyłącznie w granicach tego, co absolutnie konieczne [31]. Co więcej, odnośne środki ustawodawcze powinny „ustanawiać jasne i dokładne reguły określające, w jakich okolicznościach i pod jakimi warunkami dostawcy usług łączności elektronicznej powinni udzielać właściwym organom władz krajowych dostępu do tych danych. Ponadto tego rodzaju środek musi być prawnie wiążący w prawie krajowym" [32]. Mówiąc ściślej, uregulowania krajowe powinny „ustanawiać również materialne i proceduralne warunki regulujące dostęp odpowiednich organów władz krajowych do przechowywanych danych" [33].

60. Z powyższego można wywnioskować, że „dostęp do zatrzymanych danych, niezależnie od jakiegokolwiek związku, nawet pośredniego, z realizowanym celem, nie może być uważany za ograniczony do tego, co absolutnie konieczne" [34].

61. Zdaniem Trybunału „rozpatrywane przepisy krajowe winny opierać się na obiektywnych kryteriach umożliwiających określenie okoliczności i warunków przyznania dostępu właściwym organom władz krajowych do danych abonentów lub zarejestrowanych użytkowników. W tym względzie, biorąc pod uwagę cel polegający na zwalczaniu poważnej przestępczości, dostęp ten może co do zasady zostać przyznany jedynie w odniesieniu do danych dotyczących osób podejrzewanych o planowanie, popełnianie czy też popełnienie już poważnego przestępstwa bądź też zaangażowanych w taki czy inny sposób w takie przestępstwo" [35].

62. Innymi słowy, uregulowanie krajowe przyznające właściwym organom państwowym dostęp do zatrzymanych danych powinno mieć zakres wystarczająco ograniczony, aby zapobiec sytuacji, w której taki dostęp może dotyczyć znacznej liczby osób, a nawet wszystkich osób i środków łączności elektronicznej, jak również ogółu zatrzymanych danych. Trybunał podkreślił w związku z tym kryterium związku pomiędzy podmiotami danych a zamierzonym celem.

63. Ponadto Trybunał ustanowił warunki, którym powinien odpowiadać każdy przypadek dostępu właściwych organów państwowych do zatrzymanych danych.

29 Zobacz wyrok Tele2 Sverige i Watson i in. (pkt 113).
30 Zobacz wyrok Tele2 Sverige i Watson i in. (pkt 115).
31 Zobacz wyrok Tele2 Sverige i Watson i in. (pkt 116).
32 Zobacz wyrok Tele2 Sverige i Watson i in. (pkt 117).
33 Zobacz wyrok Tele2 Sverige i Watson i in. (pkt 118).
34 Zobacz wyrok Tele2 Sverige i Watson i in. (pkt 119).
35 Ibidem.

64. Przede wszystkim dostęp ten powinien „co do zasady, z wyjątkiem należycie uzasadnionych pilnych przypadków, [być] uzależniony od uprzedniej kontroli sądu lub niezależnego organu administracyjnego” [36]. Decyzja tego sądu lub tego podmiotu powinna zostać wydana „na uzasadniony wniosek owych organów, złożony w szczególności w ramach postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw” [37].

65. Następnie zdaniem Trybunału ważne jest, aby „właściwe organy władz krajowych, którym przyznano dostęp do przechowywanych danych, informowały o tym zainteresowane osoby w trybie właściwego postępowania krajowego, od chwili, w której informacja taka nie będzie mogła narazić na szwank prowadzonych przez te organy postępowań dochodzeniowo-śledczych” [38].

66. Wreszcie państwa członkowskie powinny przyjąć przepisy dotyczące bezpieczeństwa i ochrony danych zatrzymywanych przez dostawców usług łączności elektronicznej przed ryzykiem nadużyć oraz przed jakimkolwiek niedozwolonym dostępem do tych danych [39].

2. Wnioski płynące z wyroku Ministerio Fiscal

67. W sprawie tej zwrócono się do Trybunału z pytaniem dotyczącym zgodności z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7 i 8 karty uregulowania krajowego przewidującego dostęp właściwych organów państwowych, takich jak policja, do danych dotyczących tożsamości posiadaczy określonych kart SIM.

68. W swoim wyroku Trybunał wskazał, że jeśli chodzi o cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu przestępstw kryminalnych, brzmienie art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 nie ogranicza tego celu jedynie do zwalczania poważnych przestępstw, lecz odnosi się ogólnie do „przestępstw kryminalnych” [40].

69. Rozumowanie przedstawione przez Trybunał wyjaśnia, że jeśli chodzi o dostęp do danych uzyskiwany przez właściwe organy państwowe, musi istnieć związek pomiędzy wagą ingerencji a wagą rozpatrywanych przestępstw.

70. Trybunał przypomniał zatem, odwołując się do pkt 99 wyroku Tele2 Sverige i Watson i in., że niewątpliwie orzekł, iż „w zakresie zapobiegania, dochodzenia, wykrywania i ścigania przestępstw kryminalnych jedynie walka z poważną przestępczością może usprawiedliwiać dostęp organów publicznych do danych osobowych zatrzymywanych przez dostawców usług łączności elektronicznej, których całokształt może dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, o których dane chodzi” [41].

71. Jednocześnie Trybunał uściślił, że „uzasadnił jednak tę wykładnię, powoławszy się na okoliczność, że cel realizowany przez uregulowanie normujące ten dostęp powinien być powiązany z wagą ingerencji w odnośne prawa podstawowe, jaką dostęp taki pociąga za sobą” [42].

72. W istocie „zgodnie z zasadą proporcjonalności poważna ingerencja może bowiem być uzasadniona w zakresie zapobiegania, dochodzenia, wykrywania i ścigania przestępstw karnych jedynie przez cel polegający na zwalczaniu przestępczości, którą można uznać za »poważną«” [43].

36 Zobacz wyrok Tele2 Sverige i Watson i in. (pkt 120).
37 Ibidem.
38 Zobacz wyrok Tele2 Sverige i Watson i in. (pkt 121).
39 Zobacz wyrok Tele2 Sverige i Watson i in. (pkt 122).
40 Wyrok Ministerio Fiscal (pkt 53).
41 Wyrok Ministerio Fiscal (pkt 54).
42 Wyrok Ministerio Fiscal (pkt 55).
43 Wyrok Ministerio Fiscal (pkt 56).

73. Jeżeli natomiast „ingerencja wynikająca z takiego dostępu nie jest poważna, to może być uzasadniona przez cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu ogółu »przestępstw kryminalnych«” [44].

74. Rozważania te wskazywały zatem na potrzebę oceny, czy w świetle okoliczności sprawy ingerencję w prawa podstawowe ustanowione w art. 7 i 8 karty, z jaką wiąże się dostęp policji do danych, należy uznać za „poważną”, czy też nie.

75. Tymczasem w odróżnieniu od tego, co miało miejsce w wyroku Tele2 Sverige i Watson i in., ingerencji w prawa chronione w art. 7 i 8 karty, jaką stanowił dostęp do odnośnych danych, Trybunał nie zakwalifikował jako „poważnej” [45]. Wniosek o udzielenie dostępu miał bowiem „na celu jedynie identyfikację posiadaczy kart SIM działających, w okresie dwunastu dni, z [międzynarodowym identyfikatorem urządzenia ruchomego] skradzionego telefonu komórkowego” [46]. Chodziło więc o dostęp „do numerów telefonu odpowiadających tym kartom SIM, a także do danych dotyczących tożsamości cywilnej posiadaczy owych kart, takich jak nazwisko, imię oraz, w stosownych przypadkach, adres. Natomiast dane te nie dotycz[yły] […] komunikatów przekazanych przy użyciu skradzionego telefonu komórkowego ani jego lokalizacji” [47].

76. Trybunał wysnuł stąd wniosek, że „dane objęte wnioskiem o udzielenie dostępu rozpatrywanym w postępowaniu głównym pozwalają jedynie powiązać, w danym okresie, kartę lub karty SIM działające w skradzionym telefonie komórkowym z tożsamością cywilną posiadaczy owych kart SIM. Bez badania krzyżowego z danymi dotyczącymi komunikatów przekazanych przy użyciu wspomnianych kart SIM i z danymi dotyczącymi lokalizacji, dane te nie umożliwiają poznania ani daty, godziny, czasu trwania i odbiorców komunikatów przekazanych przy użyciu przedmiotowej karty lub przedmiotowych kart SIM, ani miejsc, w których łączność miała miejsce, lub częstotliwości komunikowania się z określonymi osobami w danym okresie. Rzeczone dane te nie pozwalają zatem na wyciągnięcie konkretnych wniosków dotyczących prywatnego życia osób, o których dane chodzi” [48].

77. Odrzuciwszy kwalifikację jako „poważnej ingerencji”, Trybunał mógł uznać, że jako uzasadnienie rozpatrywanej ingerencji można było przywołać cel polegający na ogólnym zapobieganiu, dochodzeniu, wykrywaniu i ściganiu przestępstw kryminalnych, nawet o mniejszej wadze [49].

78. Sąd odsyłający zadaje pytania prejudycjalne pierwsze i drugie – służące ocenie wagi ingerencji, jaką stanowi dostęp do danych w ramach procedury karnej będącej przedmiotem postępowania głównego – właśnie w świetle tego orzecznictwa. Mówiąc konkretniej, dąży on do ustalenia, czy kategorie danych oraz długość okresu, dla którego żądany jest dostęp do tych danych, stanowią w tym kontekście właściwe kryteria.

3. Kryteria umożliwiające ocenę wagi ingerencji

79. Jak wynika z orzecznictwa Trybunału, im większa liczba kategorii danych, do których zażądano dostępu, tym większe prawdopodobieństwo uznania ingerencji za „poważną”.

80. W związku z powyższym postawione przez sąd odsyłający pytania pierwsze i drugie skłaniają Trybunał do wyjaśnienia, czy, poza kategoriami danych, przy określaniu wagi ingerencji odgrywa również rolę długość okresu, którego dostęp dotyczy.

44 Wyrok Ministerio Fiscal (pkt 57).
45 Wyrok Ministerio Fiscal (pkt 61).
46 Wyrok Ministerio Fiscal (pkt 59).
47 Ibidem.
48 Wyrok Ministerio Fiscal (pkt 60).
49 Wyrok Ministerio Fiscal (pkt 62).

81. Moim zdaniem, należy udzielić odpowiedzi twierdzącej. Pragnę zresztą zauważyć, że Trybunał w wyroku Ministerio Fiscal Trybunał w ramach dokonywanej przez siebie oceny również uwzględnił długość okresu objętego dostępem, czyli dwanaście dni [50].

82. Wagę ingerencji można ocenić, rozważając łącznie charakter odnośnych danych i długość okresu, którego dotyczy dostęp. Te dwa aspekty umożliwiają bowiem sprawdzenie poszanowania kryterium decydującego o wadze ingerencji, to znaczy, czy dostęp do odnośnych danych może pozwolić właściwym organom państwowym na wyciągnięcie precyzyjnych wniosków dotyczących życia prywatnego osób, których dane są udostępniane. Dla sporządzenia dokładnego portretu danej osoby konieczne jest zaś nie tylko udostępnienie wielu kategorii danych, takich jak dane identyfikacyjne, o ruchu i lokalizacji, lecz również to, by dostęp ten dotyczył okresu wystarczająco długiego, aby móc zidentyfikować w dostatecznie precyzyjny sposób główne elementy życia danej osoby.

83. Zatem okres, którego dotyczy żądanie danych stosownie do zgody na dostęp, podobnie jak liczba udostępnianych kategorii, stanowi istotny element oceny wagi ingerencji w prawa podstawowe podmiotów danych. Jak wskazuje Komisja, należy także wziąć pod uwagę skumulowanie szeregu wniosków o udzielenie dostępu, dotyczących jednej i tej samej osoby, nawet jeśli dotyczą one krótkich okresów.

84. Jak wynika z wniosku o wydanie orzeczenia w trybie prejudycjalnym, dane, do których organ dochodzeniowy miał dostęp, to dane wymienione w § 111^1 ust. 2 ustawy o łączności elektronicznej. Dane te pozwalają na ustalenie miejsca nawiązania i zakończenia połączenia telefonicznego z telefonu stacjonarnego lub komórkowego danej osoby, jego datę, godzinę i czas trwania oraz rodzaj, użyte urządzenie łączności i lokalizację użytego urządzenia łączności ruchomej. Dane te zostały przekazane organowi dochodzeniowemu w odniesieniu do okresów jednego dnia, jednego miesiąca i niemalże jednego roku.

85. Ocena stopnia ingerencji w prawa podstawowe wynikającej z dostępu właściwych organów państwowych do zatrzymanych danych osobowych jest rezultatem konkretnej analizy okoliczności każdej sprawy. W każdym przypadku do sądu odsyłającego należy dokonanie oceny, czy dane, do których dostęp został zatwierdzony, mogą pozwolić, w zależności od ich rodzaju i długości okresu objętego udostępnieniem, na wyciągnięcie precyzyjnych wniosków w przedmiocie życia prywatnego podmiotów danych.

86. W takim przypadku ingerencja powinna zostać uznana za „poważną” w rozumieniu orzecznictwa Trybunału, a zatem może być uzasadniona w dziedzinie zapobiegania, dochodzenia, wykrywania i ścigania przestępstw kryminalnych wyłącznie celem zwalczania przestępczości, którą również należy zakwalifikować jako „poważną” [51].

4. W przedmiocie zgodności pomiędzy wagą ingerencji a zamierzonym celem

87. Z orzecznictwa Trybunału wynika, że ingerencja w prawa podstawowe, która została uznana za „poważną”, wiąże się z wymogiem przedstawienia wzmocnionego uzasadnienia.

88. Co się tyczy wagi domniemanych przestępstw kryminalnych, w związku z którymi udzielono dostępu do danych, Komisja zauważa, że rozpatrywane uregulowanie krajowe zezwala w szczególności na walkę z przestępstwami w ogólności [52].

50 Wyrok Ministerio Fiscal (pkt 59). Zobacz podobnie opinia rzecznika generalnego Saugmandsgaarda Øe w sprawie Ministerio Fiscal (C-207/16, EU:C:2018:300), który zauważa, że wniosek organów policji odnosił się do „jasno określonego i krótkiego okresu, to znaczy dwunastu dni” (pkt 33, a także pkt 84).

51 Wyrok Ministerio Fiscal (pkt 56).

52 Paragraf 111^1 ust. 11 ustawy o łączności elektronicznej i § 90^1 kodeksu postępowania karnego.

89. Do sądu odsyłającego należy zbadanie, czy w okolicznościach sprawy dostęp do danych, takich jak dane będące przedmiotem postępowania głównego, rzeczywiście i ściśle odpowiada jednemu z celów, o których mowa w art. 15 ust. 1 dyrektywy 2002/58. W tym względzie należy przypomnieć, że przepis ten nie ogranicza celu polegającego na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu przestępstw wyłącznie do przestępstw poważnych, ale dotyczy ogólnie „przestępstw kryminalnych” [53].

90. Jeśli sąd odsyłający dojdzie do wniosku, że ingerencję należy uznać za „poważną”, do niego należy ocena, czy dane przestępstwo może być również uznane zgodnie z krajowym prawem karnym za „poważne”.

91. W tym względzie uważam, że określenie tego, co można zakwalifikować jako „poważne przestępstwo”, trzeba pozostawić uznaniu państw członkowskich.

92. W różnych krajowych systemach prawnych to samo przestępstwo może bowiem podlegać karze mniej lub bardziej surowej. Również określenie okoliczności obciążających może różnić się w poszczególnych państwach członkowskich.

93. Jak słusznie podnosi rząd estoński, zagrożenie karą nie jest jedynym kryterium decydującym o wadze przestępstw. Należy również wziąć pod uwagę charakter przestępstw, szkodę wyrządzoną społeczeństwu, naruszenie wartości prawnych oraz ogólne skutki, jakie niosą krajowemu porządkowi prawnemu, a także wartościom demokratycznego społeczeństwa. Specyficzny kontekst historyczny, gospodarczy i społeczny każdego państwa członkowskiego również odgrywa rolę w tym względzie. Ponadto w ramach okoliczności obciążających należy zadać sobie pytanie, czy przestępstwa kryminalne popełniono, przykładowo, w warunkach recydywy lub w odniesieniu do grupy osób podatnych na zagrożenia.

94. W celu dokonania oceny proporcjonalności dostępu należy również wziąć pod uwagę, że zgodnie z § 90^1 ust. 3 kodeksu postępowania karnego „można żądać danych tylko, jeżeli jest to niezbędne do osiągnięcia celu postępowania karnego”. Jak wskazuje rząd estoński, kryterium niezbędności [54] zobowiązuje zarówno osoby prowadzące dochodzenie, jak i osoby odpowiedzialne za wydanie zgody do rozważenia i oceny, jakie dane są niezbędne do przeprowadzenia postępowania karnego, bez których w ramach rozpatrywanej sprawy nie byłoby możliwe działanie na rzecz odkrycia prawdy i ujęcia domniemanego sprawcy lub przestępcy.

95. Dodam, że jak słusznie podkreślił rząd francuski, wagę przestępstwa, a nawet jego dokładną kwalifikację prawną nie zawsze można określić w sposób precyzyjny, w sytuacji gdy zgoda na dostęp do zatrzymanych danych następuje na wczesnym etapie dochodzenia, w związku z czym na tym etapie przedwczesne byłoby zaliczenie danego przestępstwa do kategorii przestępstw poważnych lub ogólnie przestępstw. Ta niepewność, nierozerwalnie związana z dochodzeniami karnymi, których celem jest odkrycie prawdy, powinna być uwzględniona przez sąd odsyłający przy ocenie kwestii proporcjonalności dostępu.

96. Niemniej jednak niepewność w tym względzie, która może istnieć na początku dochodzenia karnego, nie może wyeliminować wymogu, zgodnie z którym każdy wniosek o udzielenie dostępu musi być uzasadniony koniecznością poszukiwania dowodów dotyczących konkretnego czynu niedozwolonego lub przestępnego, na podstawie podejrzenia popartego okolicznościami o charakterze obiektywnym. Zatem wniosek o udzielenie dostępu nie może mieć na celu zbadania w danym okresie wszystkich czynów i zachowań danej osoby w celu wykrycia ewentualnych przestępstw. Ponadto, jeśli w toku dochodzenia ujawniono nowe czyny, dostęp do danych w celu ich udowodnienia powinien być przedmiotem nowej zgody na dostęp.

53 Wyrok Ministerio Fiscal (pkt 53).

54 Nazywane też „zasadą ultima ratio”.

97. W świetle powyższych rozważań proponuję, aby Trybunał orzekł, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty należy interpretować w ten sposób, że do kryteriów pozwalających ocenić wagę ingerencji w prawa podstawowe, jaką jest udostępnienie właściwym organom państwowym danych osobowych, które dostawcy usług łączności elektronicznej mają obowiązek zatrzymywać na mocy przepisów krajowych, należą kategorie udostępnianych danych oraz długość okresu, dla którego wystąpiono o ten dostęp. Do sądu odsyłającego należy dokonanie oceny w zależności od wagi ingerencji, czy wspomniany dostęp jest absolutnie niezbędny dla osiągnięcia celu polegającego na zapewnieniu zapobiegania przestępstwom, ich dochodzenia, wykrywania i ścigania.

C. Kontrola uprzednia sprawowana przez sąd lub niezależny organ administracyjny

98. W celu zapewnienia, że dostęp właściwych organów państwowych do zatrzymanych danych jest ograniczony do tego, co jest ściśle niezbędne do osiągnięcia zamierzonego celu, Trybunał uznał za ważne, aby dostęp ten „był co do zasady, z wyjątkiem należycie uzasadnionych pilnych przypadków, uzależniony od uprzedniej kontroli *sądu lub niezależnego organu administracyjnego*, a decyzja tego sądu lub organu była wydawana na uzasadniony wniosek owych organów, złożony w szczególności w ramach postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw” [55].

99. W trzecim pytaniu prejudycjalnym sąd odsyłający zwraca się do Trybunału o wyjaśnienie kryteriów, jakie powinien spełniać organ administracyjny, aby można było uznać go za „niezależny” w rozumieniu wyroku Tele2 Sverige i Watson i in. Mówiąc ściślej, sąd odsyłający zastanawia się, czy prokuratura może być uznana za niezależny organ administracyjny, biorąc pod uwagę okoliczność, że kieruje postępowaniem przygotowawczym, a podczas procesu pełni funkcję oskarżyciela publicznego.

100. W celu udzielenia odpowiedzi na to pytanie przydatne będzie uwzględnienie dwóch obszarów orzecznictwa Trybunału, mianowicie, po pierwsze, orzecznictwa dotyczącego niezależności krajowych organów nadzorujących ochronę danych osobowych, a po drugie, orzecznictwa dotyczącego niezależności wydającego nakaz organu sądowego w ramach europejskiego nakazu aresztowania.

101. Zdaniem Trybunału niezależność stanowi istotną cechę – potwierdzoną w szczególności w art. 8 ust. 3 karty – organów odpowiedzialnych za kontrolę przestrzegania przepisów Unii w zakresie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, w celu zapewnienia skuteczności i pewności tej kontroli oraz wzmocnienia ochrony osób, których dotyczą decyzje tych organów [56].

102. Trybunał orzekł już w odniesieniu do art. 28 ust. 1 akapit drugi dyrektywy 95/46, że „organy nadzorcze właściwe w zakresie przetwarzania danych osobowych powinny cechować się niezależnością pozwalającą im na wykonywanie ich zadań bez wpływu z zewnątrz. Ta niezależność wyklucza w szczególności jakiekolwiek nakazy i jakikolwiek inny wpływ z zewnątrz – bez względu na jego formę oraz na to, czy jest bezpośredni, czy pośredni – który mógłby zaważyć na decyzjach tych organów i podważyć w ten sposób wykonywanie przez nie ich zadań polegających na ustaleniu słusznej równowagi pomiędzy ochroną prawa do poszanowania życia prywatnego a swobodą przepływu danych osobowych” [57].

55 Wyrok Tele2 Sverige i Watson i in. (pkt 120 i przytoczone tam orzecznictwo), wyróżnienie moje. Zobacz podobnie opinia 1/15 (umowa PNR UE-Kanada) z dnia 26 lipca 2017 r. (EU:C:2017:592, pkt 202, 208).

56 Zobacz w szczególności wyrok z dnia 6 października 2015 r., Schrems (C-362/14, EU:C:2015:650, pkt 40, 41 i przytoczone tam orzecznictwo). Zobacz także opinia 1/15 (Umowa PNR UE-Kanada) z dnia 26 lipca 2017 r. (EU:C:2017:592, pkt 229).

57 Wyrok z dnia 8 kwietnia 2014 r., Komisja/Węgry (C-288/12, EU:C:2014:237, pkt 51 i przytoczone tam orzecznictwo).

103. Trybunał położył również nacisk na wymóg, zgodnie z którym biorąc pod uwagę odgrywaną przez nie rolę strażnika prawa do prywatności, organy nadzorcze powinny być „poza jakimkolwiek podejrzeniem stronniczości”[58].

104. W zakresie, w jakim pytanie trzecie przedstawione przez sąd odsyłający dotyczy prokuratury, należy również uwzględnić kryteria sformułowane przez Trybunał w jego orzecznictwie dotyczącym niezależności organu sądowego w ramach europejskiego nakazu aresztowania. I tak zdaniem Trybunału kontrola przy wydawaniu nakazu aresztowania „powinna być sprawowana w sposób obiektywny, z uwzględnieniem wszystkich dowodów obciążających i odciążających, a także w sposób niezależny, co zakłada istnienie przepisów ustawowych i organizacyjnych wykluczających wszelkie ryzyko, że podjęcie decyzji o wydaniu takiego nakazu aresztowania może podlegać zewnętrznym instrukcjom, w szczególności ze strony władzy wykonawczej”[59]. Należy jednak mieć na uwadze, że przeprowadzana przez Trybunał w każdym przypadku konkretna ocena, czy prokuratura spełnia te kryteria[60], jest dokonywana w szczególnych ramach wydawania europejskiego nakazu aresztowania i nie można zatem jej automatycznie przenosić na inne dziedziny, takie jak ochrona danych osobowych.

105. Uściślijszy powyższe, należy stwierdzić, iż wspomniane dwa obszary orzecznictwa Trybunału są zbieżne w tym, że podkreślają w każdej z rzeczonych dziedzin, że organ państwowy właściwy do badania przestrzegania przepisów prawa Unii musi mieć charakter niezależny, co obejmuje dwa wymogi[61]. Po pierwsze, organ ten nie może być związany poleceniami ani podlegać naciskom zewnętrznym mogącym wpłynąć na jego decyzje. Po drugie, organ ten powinien na mocy swojego statusu i powierzonych mu zadań spełniać wymóg obiektywizmu w wykonywanej przez niego kontroli, to znaczy musi dawać gwarancje bezstronności. Konkretniej rzecz ujmując, dokonana przez organ administracyjny ocena proporcjonalnego charakteru dostępu do zatrzymanych danych wymaga, by organ ów mógł zapewnić właściwą równowagę między interesami związanymi ze skutecznością dochodzenia w ramach walki z przestępczością i interesami dotyczącymi ochrony danych osobowych podmiotów, których dotyczy dostęp. W tym ostatnim aspekcie wymóg bezstronności jest zatem nierozerwalnie związany z pojęciem „niezależnego organu administracyjnego”, uwypuklonym przez Trybunał w wyroku Tele2 Sverige i Watson i in.

106. Należy sprawdzić, czy prokurator – biorąc pod uwagę różne zadania powierzone mu przez przepisy estońskie – spełnia to kryterium niezależności w obu wymiarach, gdy kontroluje absolutną konieczność dostępu do danych. Zatem pojęcie „niezależności”, którą powinien charakteryzować się organ administracyjny odpowiedzialny za taką kontrolę, ma wymiar funkcjonalny, w tym znaczeniu, że to w odniesieniu do szczególnego przedmiotu tej kontroli należy ocenić, czy organ ten jest w stanie podejmować działania bez interwencji ani nacisków z zewnątrz, które mogłyby wpłynąć na jego decyzje, a także z poszanowaniem obiektywizmu i ścisłego stosowania przepisów prawa. Podsumowując, pojęcie „niezależnego organu administracyjnego” w rozumieniu wyroku Tele2 Sverige i Watson i in. ma zapewnić obiektywizm, pewność i skuteczność tej kontroli.

58 Wyrok z dnia 8 kwietnia 2014 r., Komisja/Węgry (C-288/12, EU:C:2014:237, pkt 53 i przytoczone tam orzecznictwo).

59 Zobacz wyrok z dnia 9 października 2019 r., NJ (Prokuratura w Wiedniu) (C-489/19 PPU, EU:C:2019:849, pkt 38 i przytoczone tam orzecznictwo).

60 Zobacz ostatnio wyrok z dnia 12 grudnia 2019 r. JR i YC (Prokuratorzy Lyonu i Tours) (C-566/19 PPU et C-626/19 PPU, EU:C:2019:1077), w którym Trybunał uznał, że przedstawione mu okoliczności wystarczają do wykazania, że „prokuratorom we Francji przysługuje uprawnienie do dokonania oceny w sposób niezależny, w szczególności względem władzy wykonawczej, konieczności wydania europejskiego nakazu aresztowania i jego proporcjonalnego charakteru i że wykonują to uprawnienie w sposób obiektywny, przy uwzględnieniu wszystkich dowodów obciążających i odciążających” (pkt 55 tego wyroku).

61 W przedmiocie obu aspektów wymogu niezależności zob. analogicznie w odniesieniu do sądów krajowych orzekających w kwestiach związanych z wykładnią i stosowaniem prawa Unii wyrok z dnia 5 listopada 2019 r., Komisja/Polska (Niezależność sądów powszechnych) (C-192/18, EU:C:2019:924, pkt 108–110 i przytoczone tam orzecznictwo).

107. Oznacza to konieczność zbadania, czy przepisy estońskie, które określają status i zadania prokuratury, mogą wzbudzić w odczuciu podmiotów danych uzasadnione wątpliwości co do niezależności prokuratorów wobec czynników zewnętrznych i ich neutralności w odniesieniu do ścierających się interesów przy wykonywaniu przez nich kontroli proporcjonalności dostępu do danych.

108. Prokuratura odgrywa istotną rolę w prowadzeniu postępowania karnego, ponieważ kieruje postępowaniem przygotowawczym, a w szczególności dysponuje uprawnieniami w zakresie ścigania w odniesieniu do osoby podejrzanej o popełnienie przestępstwa, w celu postawienia jej przed sądem. Należy ją w tym względzie uznać za organ uczestniczący w sprawowaniu wymiaru sprawiedliwości w sprawach karnych [62].

109. Jak Trybunał stwierdził w odniesieniu do Procura della Repubblica (prokuratora Republiki, Włochy), korzystając ze sformułowania, które moim zdaniem można zastosować w niniejszej sprawie, prokurator „ma za zadanie nie rozstrzyganie sporu przy zachowaniu całkowitej niezależności, ale, ewentualnie, jako strona postępowania, która wnosi akt oskarżenia, skierowanie sporu do właściwego sądu” [63].

110. O ile mając na względzie jej status, organizację i zadania prokuratura posiada cechy szczególne, które odróżniają ją od sądu i uzasadniają uznanie jej za „organ uczestniczący w sprawowaniu wymiaru sprawiedliwości państw członkowskich w sprawach karnych”, o tyle pod kątem funkcjonalnym, jeżeli prawo krajowe przewiduje, że organem przeprowadzającym uprzednią kontrolę proporcjonalności dostępu wymaganą na mocy wyroku Tele2 Sverige i Watson i in. jest prokuratura, ta ostatnia powinna w tym aspekcie posiadać stopień niezależności analogiczny do sądu. Wykonywanie tej funkcji przez organ administracyjny, a nie przez sąd, nie może bowiem wpływać na obiektywizm, pewność i skuteczność tej kontroli.

111. W tym względzie należy przypomnieć, że zgodnie z § 90^1 ust. 2 kodeksu postępowania karnego organ dochodzeniowy może, na podstawie zgody prokuratury wydanej w postępowaniu przygotowawczym lub na podstawie zgody wydanej przez sąd w toku postępowania sądowego, zwrócić się do przedsiębiorstwa łączności elektronicznej o udostępnienie danych wymienionych w § 111^1 ust. 2 i 3 ustawy o łączności elektronicznej.

112. Ponadto z przepisów estońskich wynika, że w ramach postępowania karnego prokuratura kieruje postępowaniem przygotowawczym, którego celem jest zgromadzenie dowodów i stworzenie pozostałych warunków do przeprowadzenia procesu. Poza tym w toku postępowania przygotowawczego organ dochodzeniowy i prokuratura ustalają okoliczności odciążające i obciążające osobę podejrzaną lub oskarżoną. Po przeprowadzeniu postępowania przygotowawczego prokuratura wnosi akt oskarżenia wobec danej osoby, jeżeli jest przekonana, że w sprawie karnej zostały zebrane wszystkie niezbędne dowody i są podstawy do tego, a w tym przypadku to właśnie ona pełni funkcję oskarżyciela publicznego przed sądem.

113. Sąd odsyłający zwraca również uwagę, że chociaż w ramach postępowania karnego prokuratura w odniesieniu do środków, które stanowią najcięższe ingerencje w prawa podstawowe, ma obowiązek wystąpić o zgodę do sędziego śledczego (na przykład, w przypadku większości środków nadzoru i w odniesieniu do zatrzymania), prokuratura ma również uprawnienia do decydowania o wykonaniu czynności procesowych stanowiących daleko idącą ingerencję w szereg praw podstawowych [64].

62 Zobacz, w szczególności, wyrok z dnia 27 maja 2019 r., PF (Prokurator generalny Litwy) (C-509/18, EU:C:2019:457, pkt 39, 40).

63 Wyrok z dnia 12 grudnia 1996 r., X (C-74/95 i C-129/95, EU:C:1996:491, pkt 19).

64 Przykładowo, prokuratura udziela zgody na niejawną obserwację osoby, rzeczy lub miejsca oraz w wielu przypadkach na przeszukanie.

114. Wątpliwości wyrażone przez sąd odsyłający w odniesieniu do uznania prokuratury za „niezależny organ administracyjny" w rozumieniu wyroku Tele2 Sverige i Watson i in. wynikają przede wszystkim z tego, że po przeprowadzeniu postępowania przygotowawczego prokuratura jest zobowiązana do wniesienia aktu oskarżenia wobec danej osoby, jeżeli jest przekonana, że w sprawie karnej zostały zebrane wszystkie niezbędne dowody i są podstawy do tego. W takim przypadku to właśnie prokuratura pełni funkcję oskarżyciela publicznego przed sądem, a zatem jest również stroną postępowania. W związku z tym sąd odsyłający kwestionuje kwalifikację prokuratora jako „niezależnego organu administracyjnego" w rozumieniu wyroku Tele2 Sverige i Watson i in. głównie ze względu na jego przymiot oskarżyciela.

115. Wyrażone w ten sposób przez sąd odsyłający wątpliwości dotyczą zatem w szczególności bezstronności prokuratury przy kontroli proporcjonalności dostępu organów dochodzeniowych do danych, przeprowadzanej przez nią przed udzieleniem zgody na ów dostęp.

116. Przed przystąpieniem do analizy tego aspektu dotyczącego bezstronności pragnę zauważyć, że § 1 ust. 11 ustawy o prokuraturze stanowi, iż prokuratura „wypełnia w sposób niezależny swoje zadania ustawowe". Co więcej, zgodnie z § 2 ust. 2 tej ustawy „[p]rokurator jest niezależny przy wypełnianiu swoich zadań i działa wyłącznie zgodnie z ustawą i własnymi przekonaniami" [65].

117. W tym względzie rząd estoński wskazuje, że o ile prokuratura jest organem podlegającym ministerstwu sprawiedliwości, o tyle przepisy estońskie odmawiają temu ministerstwu jakichkolwiek możliwości oceniania poszczególnych postępowań lub interweniowania w zawisłej sprawie karnej. Rząd ten wyjaśnia, że naruszenie niezależności prokuratora stanowi przestępstwo zagrożone karą.

118. Jeśli nie ma zatem podstaw, by wątpić w niezależność prokuratury w ramach zadań, które na nią ciążą na mocy przepisów estońskich, to jednak wydaje mi się, że niezależność ta może budzić uzasadnione wątpliwości co do zdolności prokuratury do przeprowadzenia neutralnej i obiektywnej uprzedniej kontroli proporcjonalności dostępu do danych, jeżeli w ramach danej sprawy może wykonywać w tym samym czasie zadania polegające na prowadzeniu dochodzenia karnego, decydowaniu o ściganiu karnym i pełnieniu funkcji oskarżyciela publicznego przed sądem.

119. Prawdą jest, że szereg elementów zawartych w przepisach estońskich stanowi gwarancje, iż prokuratura w ramach wykonywanych zadań działa z poszanowaniem wymogu bezstronności.

120. I tak na mocy § 211 ust. 2 kodeksu postępowania karnego prokuratura zobowiązana jest ustalić okoliczności odciążające i obciążające osobę podejrzaną lub oskarżoną.

121. Co więcej, jak wynika z § 1 ust. 1 ustawy o prokuraturze, jest ona zobowiązana do zapewnienia legalności postępowania przygotowawczego, którym kieruje. Ponadto zgodnie z § 1 ust. 1^1 i § 2 ust. 2 tej ustawy prokuratura powinna wykonywać swoje zadania zgodnie z ustawą. Oznacza to, że w przypadku gdy prokuratura kieruje postępowaniem przygotowawczym, jej celem jest nie tylko zapewnienie skuteczności tego postępowania, lecz także zagwarantowanie, że postępowanie to nie będzie prowadzone z nieproporcjonalnym naruszeniem prawa do prywatności podmiotów danych. Można bowiem uznać, że zezwolenie na dostęp do zatrzymanych danych stanowi integralną część szerszego zadania prokuratury, polegającego na kontroli zgodności z prawem środków zastosowanych przez organy dochodzeniowe, w szczególności proporcjonalności czynności dochodzeniowych w świetle charakteru i wagi czynów.

65 Zobacz także podobnie § 30 ust. 2 kodeksu postępowania karnego.

122. Można by zatem podnieść argument, że właśnie z uwagi na to, iż prokuratura kieruje postępowaniem przygotowawczym, jest ona w stanie ocenić, czy ze względu na specyfikę poszczególnych spraw dostęp do danych zatrzymywanych przez operatorów telekomunikacyjnych jest absolutnie konieczny w braku dowodów alternatywnych dla celów kontynuowania dochodzenia w przedmiocie podejrzewanego przestępstwa.

123. Nie zmienia to faktu, że z punktu widzenia podmiotów danych, których dotyczy wniosek o udzielenie dostępu, okoliczność, że organ administracyjny, który ma sprawdzić, czy dostęp ten jest absolutnie niezbędny w ramach dochodzenia, jest tym samym organem, który może je ścigać karnie, a następnie pełnić funkcję oskarżyciela publicznego w ewentualnym późniejszym procesie, może moim zdaniem osłabiać gwarancje bezstronności przewidziane w przepisach estońskich. Z tego punktu widzenia może istnieć potencjalny konflikt między z jednej strony tymi zadaniami prokuratury a z drugiej strony wymogiem neutralności i obiektywizmu uprzedniej kontroli proporcjonalności dostępu do danych.

124. W ramach jej zadań prokuratura jest bowiem zobowiązana do zgromadzenia dowodów, oceny ich znaczenia i wyciągnięcia wniosków co do winy danej osoby. Do tegoż organu państwa należy wniesienie i popieranie aktu oskarżenia w ramach funkcji oskarżyciela publicznego, którą pełni w trakcie procesu, będąc zatem stroną postępowania. Z uwagi na te zadania prokuratura podlega wymogowi dowodowemu, który w oczach osób podejrzanych o popełnienie przestępstwa może wydawać się nie do pogodzenia ze zdolnością tego organu do dokonania w sposób neutralny i obiektywny uprzedniej kontroli proporcjonalnego charakteru dostępu do danych.

125. Jak podnosi Komisja, może istnieć ryzyko, że ze względu na kumulację zadań, jakie na niej spoczywają, podmioty danych mogą postrzegać prokuraturę w ten sposób, że ma ona interes w szerokim udostępnianiu ich danych, niezależnie od tego, czy są one obciążające czy odciążające. Co więcej, osoby podejrzane o popełnienie przestępstwa mogą żywić uzasadnione wątpliwości co do bezstronności prokuratury, gdy udziela ona zgody na dostęp do ich danych, jeżeli w późniejszym postępowaniu może wystąpić przeciwko nim jako oskarżyciel. Uważam zaś, że wymóg bezstronności organu administracji, któremu powierzono przeprowadzenie uprzedniej kontroli wymaganej przez wyrok Tele2 Sverige i Watson i in., zakłada pewien dystans i neutralność w odniesieniu do interesów, które mogą się ścierać w ramach postępowania przygotowawczego, mianowicie z jednej strony jego skuteczności, a z drugiej strony ochrony danych osobowych podmiotów tych danych. Zdaniem Komisji sytuacja mogłaby być inna, gdyby wewnętrzna organizacja administracyjna prokuratury była taka, że prokurator, który decyduje w przedmiocie wniosku o udzielenie dostępu, nie odgrywa żadnej roli w postępowaniu przygotowawczym ani na późniejszych etapach postępowania, w tym jako oskarżyciel publiczny.

126. Ponieważ, jak zostało to potwierdzone w trakcie rozprawy, prokuratura jest zorganizowana w Republice Estońskiej w sposób hierarchiczny, nie jestem przekonany, by ta sugestia Komisji mogła zaradzić problemom wynikającym ze zbiegu zadań, które przepisy estońskie powierzają prokuraturze. W każdym jednak razie nie pozbawia to znaczenia koncepcji, która leży u podstaw tej sugestii, a mianowicie, że uprzednią kontrolę proporcjonalnego charakteru dostępu do danych powinien przeprowadzać organ administracyjny, który, po pierwsze, nie jest bezpośrednio zaangażowany w prowadzenie omawianego dochodzenia karnego, a po drugie, zajmuje neutralną pozycję wobec stron postępowania karnego. Takiemu organowi, niezależnemu od interesów związanych z dochodzeniem i oskarżeniem publicznym w ramach rozpatrywanego postępowania, nie można by zarzucać, że uprzywilejowuje interes dochodzenia ze szkodą dla interesów związanych z ochroną danych osobowych. Organ ten byłby zatem w stanie wydać przy zachowaniu pełnej bezstronności decyzję ograniczającą dostęp do zatrzymanych danych do tego, co absolutnie konieczne do osiągnięcia zamierzonego celu, zgodnie z wymogami art. 15 ust. 1 dyrektywy 2002/58 stosownie do jego wykładni

dokonanej przez Trybunał w wyrokach z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in.[66] oraz Tele2 Sverige i Watson i in. Jednocześnie mam świadomość, że zapewnienie punktu widzenia oddalonego od interesów związanych z danym postępowaniem nie powinno nastąpić za cenę zmniejszenia skuteczności wykrywania, ścigania i karania przestępstw karnych.

127. W celu poszanowania autonomii proceduralnej państw członkowskich Trybunał nie powinien głębiej ingerować w ogólną organizację wymiaru sprawiedliwości w państwach członkowskich, ani też w organizację wewnętrzną prokuratur. Do państw członkowskich należy ustanowienie narzędzi właściwych do zapewnienia, by uprzednia kontrola dostępu do zatrzymanych danych zapewniała właściwą równowagę między interesami związanymi z skutecznością dochodzenia karnego a prawem do ochrony danych podmiotów, których ów dostęp dotyczy.

128. Na koniec wyjaśnię, że moim zdaniem braku uprzedniej kontroli przez „niezależny" – w rozumieniu wyroku Tele2 Sverige i Watson i in. – organ administracyjny nie można zrekompensować istnieniem kontroli sądowej, która może zostać przeprowadzona po uzyskaniu zgody[67]. W przeciwnym razie wymóg uprzedniej kontroli straciłby swoją rację bytu polegającą na uniemożliwieniu udzielenia dostępu do zatrzymanych danych w zakresie nieproporcjonalnym w stosunku do celu polegającego na dochodzeniu, ściganiu i karaniu przestępstw.

129. W świetle powyższych rozważań proponuję Trybunałowi, aby na trzecie pytanie prejudycjalne odpowiedział, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty należy interpretować w ten sposób, że wymóg, zgodnie z którym dostęp właściwych organów państwowych do zatrzymanych danych powinien podlegać uprzedniej kontroli sprawowanej przez sąd lub przez niezależny organ administracyjny, nie jest spełniony, jeżeli przepisy krajowe przewidują, iż taka kontrola jest przeprowadzana przez prokuraturę, której zadaniem jest kierowanie postępowaniem przygotowawczym i która jednocześnie może pełnić funkcję oskarżyciela publicznego w trakcie procesu.

V. Wnioski

130. W świetle powyższego proponuję, aby Trybunał udzielił następujących odpowiedzi na pytania przedstawione przez Riigikohus (sąd najwyższy, Estonia):

1) Artykuł 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa dotycząca prywatności i łączności elektronicznej), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r., w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej, należy interpretować w ten sposób, że do kryteriów pozwalających ocenić wagę ingerencji w prawa podstawowe, jaką jest udostępnienie właściwym organom państwowym danych osobowych, które dostawcy usług łączności elektronicznej mają obowiązek zatrzymywać na mocy przepisów krajowych, należą kategorie udostępnianych danych oraz długość okresu, dla którego wystąpiono o ten dostęp. Do sądu odsyłającego należy dokonanie oceny w zależności od wagi ingerencji, czy wspomniany dostęp jest absolutnie niezbędny dla osiągnięcia celu polegającego na zapewnieniu zapobiegania przestępstwom, ich dochodzenia, wykrywania i ścigania.

66 C-293/12 i C-594/12, EU:C:2014:238.

67 Zgodnie z informacjami dostarczonymi Trybunałowi w toku rozprawy owa kontrola sądowa na gruncie prawa estońskiego może nastąpić po zakończeniu postępowania przygotowawczego, jeżeli podejrzany po zapoznaniu się z aktami sprawy postanawia zaskarżyć czynność w ramach tego postępowania, lub też w trakcie procesu.

2) Artykuł 15 ust. 1 dyrektywy 2002/58, zmienionej dyrektywą 2009/136, w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej, należy interpretować w ten sposób, że wymóg, zgodnie z którym dostęp właściwych organów państwowych do zatrzymanych danych powinien podlegać uprzedniej kontroli sprawowanej przez sąd lub przez niezależny organ administracyjny, nie jest spełniony, jeżeli przepisy krajowe przewidują, iż taka kontrola jest przeprowadzana przez prokuraturę, której zadaniem jest kierowanie postępowaniem przygotowawczym i która jednocześnie może pełnić funkcję oskarżyciela publicznego w trakcie procesu.