Zbiór Orzeczeń

OPINIA RZECZNIKA GENERALNEGO
MANUELA CAMPOSA SÁNCHEZA-BORDONY
przedstawiona w dniu 30 marca 2023 r. [1]

Sprawa C-162/22

A.G.
przy udziale:
Lietuvos Respublikos generalinė prokuratūra

[wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Lietuvos vyriausiasis administracinis teismas (najwyższy sąd administracyjny, Litwa)]

Odesłanie prejudycjalne – Telekomunikacja – Przetwarzanie danych osobowych – Dyrektywa 2002/58/WE – Zakres stosowania – Artykuł 15 ust. 1 – Dostęp do danych zatrzymywanych przez dostawców usług łączności elektronicznej i zbieranych w ramach postępowań przygotowawczych – Późniejsze wykorzystanie danych w trakcie dochodzenia w sprawie przewinienia dyscyplinarnego

1. Niniejsze odesłanie prejudycjalne dotyczy zasadniczo ustalenia, czy dane osobowe uzyskane w toku postępowania przygotowawczego mogą następnie zostać wykorzystane w administracyjnym postępowaniu dyscyplinarnym przeciwko urzędnikowi publicznemu.

2. Odpowiedź na to pytanie stwarza Trybunałowi kolejną okazję do wypowiedzenia się na temat zakresów stosowania dyrektywy 2002/58/WE [2] z jednej strony oraz dyrektywy (UE) 2016/680 [3] i rozporządzenia (UE) 2016/679 [4] z drugiej strony.

3. W odniesieniu do dyrektywy 2002/58 istnieje utrwalone już orzecznictwo Trybunału dotyczące sytuacji i warunków, w jakich państwa członkowskie mogą ograniczyć zakres praw i obowiązków w niej ustanowionych [5].

[1] Język oryginału: hiszpański.

[2] 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).

[3] Dyrektywa Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. 2016, L 119, s. 89).

[4] Rozporządzenie Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. 2016, L 119, s. 1). Jest ono zwane dalej „RODO".

[5] W szczególności jako najistotniejsze wyroki składające się na to orzecznictwo można przytoczyć wyroki: z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in. (C-293/12 i C-594/12, EU:C:2014:238); z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970); z dnia 6 października 2020 r., La Quadrature du Net i in. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791; zwany dalej „wyrokiem La Quadrature du Net"); z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej) (C-746/18, EU:C:2021:152); a także z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in. (C-140/20, EU:C:2022:258; zwany dalej „wyrokiem Commissioner of An Garda Síochána").

I. Ramy prawne

A. Prawo Unii

1. Dyrektywa 2002/58

4. Artykuł 1 („Zakres i cel”) stanowi:

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

2. Przepisy niniejszej dyrektywy dookreślają i uzupełniają dyrektywę 95/46/WE[6] zgodnie z celami przedstawionymi w ust. 1. Ponadto zapewniają ochronę uzasadnionych interesów abonentów będących osobami prawnymi.

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

5. Artykuł 5 („Poufność komunikacji”) w ust. 1 stanowi:

„Państwa członkowskie zapewniają, poprzez ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. W szczególności zakazują słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy bez zgody zainteresowanych użytkowników, z wyjątkiem upoważnienia zgodnego z art. 15 ust. 1. Niniejszy ustęp nie zabrania technicznego przechowywania, które jest niezbędne do przekazania komunikatu, bez uszczerbku dla zasady poufności”.

6. Artykuł 15 („Stosowanie niektórych przepisów dyrektywy 95/46/WE”) stanowi:

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

[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).

określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 [TUE].

[…]

2. Przepisy rozdziału III, dotyczącego środków zaskarżenia, odpowiedzialności i sankcji dyrektywy 95/46/WE, stosuje się w odniesieniu do przepisów krajowych przyjętych zgodnie z niniejszą dyrektywą i w odniesieniu do indywidualnych uprawnień wynikających z niniejszej dyrektywy.

[…]".

2. R

7. Artykuł 2 („Materialny zakres stosowania") stanowi:

„1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

2. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:

a) w ramach działalności nieobjętej zakresem prawa Unii;

[…]

d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

[…]".

8. Artykuł 5 („Zasady dotyczące przetwarzania danych osobowych") ma następujące brzmienie:

„1. Dane osobowe muszą być:

[…]

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami (»ograniczenie celu«);

[…]".

9. Artykuł 6 („Zgodność przetwarzania z prawem”) stanowi:

„1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

[…]

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

[…]

3. Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona:

a) w prawie Unii; lub

b) w prawie państwa członkowskiego, któremu podlega administrator.

[…]

4. Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego, stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi:

a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;

b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem;

c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych zgodnie z art. 10;

d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;

[…]”.

3. Dyrektywa 2016/680

10. Artykuł 1 („Przedmiot i cele”) w ust. 1 stanowi:

„1. Niniejsza dyrektywa ustanawia przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów

zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom”.

11. Artykuł 2 („Zakres zastosowania”) w ust. 1 stanowi:

„Niniejsza dyrektywa ma zastosowanie do przetwarzania danych osobowych przez właściwe organy do celów określonych w art. 1 ust. 1”.

12. Artykuł 4 („Zasady dotyczące przetwarzania danych osobowych”) stanowi:

„1. Państwa członkowskie zapewniają, by dane osobowe były:

[…]

b) zbierane w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzane w sposób niezgodny z tymi celami;

[…]

2. Przetwarzanie przez tego samego lub innego administratora w jednym z celów określonych w art. 1 ust. 1 innym niż cel, w którym dane osobowe zostały zebrane, jest dozwolone, o ile:

a) administratorowi wolno przetwarzać takie dane osobowe w takim celu na mocy prawa Unii lub prawa państwa członkowskiego; oraz

b) przetwarzanie jest niezbędne i proporcjonalne w tym innym celu na mocy prawa Unii lub prawa państwa członkowskiego.

[…]”.

13. Artykuł 9 („Szczególne warunki przetwarzania”) stanowi w ust. 1:

„Danych osobowych zebranych przez właściwe organy do celów określonych w art. 1 ust. 1 nie przetwarza się do celów innych niż określone w art. 1 ust. 1, chyba że takie przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego. Jeżeli przetwarzanie danych osobowych odbywa się w takich innych celach, zastosowanie ma [RODO], chyba że przetwarzanie odbywa się w toku działalności nieobjętej prawem Unii”.

B. Prawo krajowe

1. Lietuvos Respublikos elektroninių ryšių įstatymas [7]

14. Artykuł 65 ust. 2 nakłada na dostawców usług łączności elektronicznej obowiązek zatrzymywania danych wymienionych w załączniku 1 do tej ustawy oraz, w stosownych przypadkach, udostępniania ich właściwym organom w celu wykorzystania ich w walce z poważną przestępczością [8].

15. Zgodnie z art. 77 ust. 1 dostawcy usług łączności elektronicznej muszą dostarczyć właściwym organom informacje będące w ich posiadaniu zgodnie z prawem, które są niezbędne w szczególności do zapobiegania przestępczości, wykrywania i ścigania czynów zabronionych.

16. Zgodnie z art. 77 ust. 4 jeżeli istnieje uzasadnione orzeczenie sądowe lub inna podstawa prawna przewidziana ustawą, dostawcy usług łączności elektronicznej muszą zapewnić techniczną możliwość kontroli treści połączeń odbywających się poprzez sieci łączności elektronicznej, w szczególności organom dochodzeniowym i organom prowadzącym postępowanie przygotowawcze zgodnie z zasadami przewidzianymi w prawie karnym procesowym.

2. Lietuvos Respublikos kriminalinės žvalgybos įstatymas [9]

17. Zgodnie z art. 6 ust. 3 pkt 1 jeżeli spełnione są przesłanki określone w samej ustawie o wywiadzie kryminalnym i po uzyskaniu uprzedniej zgody prokuratury lub organu sądowego, organy dochodzeniowe [10] mogą uzyskiwać informacje od dostawców usług łączności elektronicznej.

18. Zgodnie z art. 8 ust. 1 i 3 organy prowadzące dochodzenie w sprawach karnych podejmują działania niezwłocznie po uzyskaniu informacji dotyczących przygotowania lub popełnienia bardzo poważnego, poważnego lub stosunkowo poważnego przestępstwa, a jeżeli w wyniku dochodzenia okaże się, że popełnione zostało przestępstwo, niezwłocznie wszczyna się postępowanie karne.

19. Zgodnie z art. 19 ust. 1 pkt 5 informacje uzyskane w wyniku czynności dochodzeniowych mogą zostać wykorzystane w przypadkach określonych w ust. 3 i 4 tego przepisu oraz w innych przypadkach przewidzianych ustawą.

20. Zgodnie z art. 19 ust. 3 informacje dotyczące czynu noszącego znamiona przestępstwa związanego z korupcją mogą zostać odtajnione w porozumieniu z prokuraturą i wykorzystane w ramach dochodzenia w sprawie przewinień dyscyplinarnych lub służbowych.

[7] Ustawa Republiki Litewskiej o łączności elektronicznej w brzmieniu nadanym ustawą nr IX-2135 z dnia 15 kwietnia 2004 r., zmieniona ustawą nr XIII-2172 z dnia 6 czerwca 2019 r., zwana dalej „ustawą o łączności elektronicznej".

[8] Dane wymienione w tym załączniku („Kategorie danych podlegających ochronie") są danymi niezbędnymi do ustalenia pochodzenia i przeznaczenia połączenia, daty, godziny, czasu trwania, rodzaju połączenia oraz lokalizacji urządzenia komunikacyjnego (w tym łączności komórkowej) użytkowników.

[9] Ustawa Republiki Litewskiej o wywiadzie kryminalnym w brzmieniu nadanym ustawą nr XI-2234 z dnia 2 października 2012 r., zmieniona ustawą nr XIII-1837 z dnia 20 grudnia 2018 r., zwana dalej „ustawą o wywiadzie kryminalnym".

[10] W celu określenia służb prowadzących odpowiednie dochodzenia będę używał terminu „informacje", a nie „wywiad".

3. Lietuvos Respublikos baudžiamojo proceso kodeksas [11]

21. Zgodnie z art. 154 („Kontrola, rejestrowanie i zatrzymywanie informacji przekazywanych poprzez sieci łączności elektronicznej") (ust. 1) osoba prowadząca dochodzenie może, na podstawie orzeczenia sędziego śledczego wydanego na wniosek prokuratury, słuchać, nagrywać i zatrzymywać rozmowy przekazywane poprzez sieci łączności elektronicznej, jeżeli istnieje podstawa do przypuszczenia, że można uzyskać dane dotyczące bardzo poważnego lub poważnego przestępstwa, które jest w trakcie przygotowania, popełnienia lub które już zostało popełnione, lub stosunkowo poważnego przestępstwa lub przestępstwa, które nie ma poważnego charakteru.

22. Zgodnie z art. 177 („Zakaz ujawniania informacji uzyskanych w wyniku postępowania przygotowawczego") (ust. 1) informacje uzyskane w wyniku postępowania przygotowawczego są poufne i do czasu rozpoznania sprawy przez sąd mogą zostać ujawnione jedynie za zgodą prokuratury i tylko w uzasadnionym zakresie [12].

II. Okoliczności faktyczne, postępowanie główne i pytanie prejudycjalne

23. Lietuvos Respublikos generalinė prokuratūra (prokuratura generalna Republiki Litewskiej; zwana dalej „prokuraturą generalną") wszczęła dochodzenie wewnętrzne w sprawie działań A.G., który zajmował wówczas stanowisko prokuratora w Apygardos prokuratūra (prokuraturze okręgowej), z uwagi na to, że działania te nosiły znamiona przewinienia podczas sprawowania urzędu.

24. Komisja prokuratury generalnej stwierdziła, że A.G. dopuścił się przewinienia podczas sprawowania urzędu, i zaproponowała, aby nałożyć na niego karę dyscyplinarną polegającą na odwołaniu z urzędu prokuratora.

25. Przewinienie to zostało ustalone na podstawie informacji uzyskanych w toku postępowania administracyjnego, wynikających z działań służb informacji kryminalnych, wyjaśnień innych urzędników oraz wyjaśnień wnoszącego odwołanie, a także na podstawie ustaleń dokonanych w dwóch postępowaniach przygotowawczych.

26. W szczególności z ustaleń wynikało, że między A.G. a adwokatem podejrzanego w postępowaniu przygotowawczym prowadzonym przez A.G. nawiązywane były połączenia telefoniczne w przedmiocie spraw, w których ten adwokat występował w charakterze obrońcy [13].

27. Monitorowanie i rejestrowanie informacji przekazywanych poprzez sieci łączności elektronicznej odbywało się na podstawie orzeczeń sądowych.

[11] Kodeks postępowania karnego Republiki Litewskiej z dnia 14 marca 2002 r. w brzmieniu mającym zastosowanie do postępowania głównego, zwany dalej „kodeksem postępowania karnego".

[12] Zgodnie z Ikiteismino tyrimo duomenų teikimo ir panaudojimo ne baudžiamojo persekiojimo tikslais ir ikiteismino tyrimo duomenų apsaugos rekomendajos (zaleceniami w sprawie dostarczania i wykorzystywania danych z postępowania przygotowawczego do celów niezwiązanych ze ściganiem przestępstw oraz ochroną danych z postępowania przygotowawczego) zatwierdzonymi zarządzeniem prokuratora generalnego nr 1-279 z dnia 17 sierpnia 2017 r., w brzmieniu zmienionym zarządzeniem nr 1-211 z dnia 25 czerwca 2018 r., w szczególności pkt 23, po otrzymaniu wniosku o udostępnienie danych z postępowania przygotowawczego prokurator podejmuje decyzję o ich udostępnieniu. W przypadku podjęcia decyzji o udostępnieniu danych prokurator musi określić zakres, w jakim mogą one zostać udostępnione.

[13] Jak wskazano na rozprawie, nadal pozostają w toku postępowania karne przeciwko A.G. i temu adwokatowi w związku z tymi czynami.

28. Prokurator generalny zastosował karę polegającą na odwołaniu z urzędu A.G., który wniósł w związku z tym skargę do Vilniaus apygardos administracinis teismas (regionalnego sądu administracyjnego w Wilnie, Litwa), wnosząc o uchylenie kary.

29. Skarga ta została oddalona wyrokiem z dnia 16 lipca 2021 r., ponieważ sąd pierwszej instancji stwierdził, że działania służb informacji kryminalnych były zgodne z prawem, podobnie jak wykorzystanie w toku postępowania dyscyplinarnego informacji uzyskanych przez te służby.

30. A.G. wniósł odwołanie od wyroku wydanego przez sąd pierwszej instancji do Lietuvos vyriausiasis administracinis teismas (najwyższego sądu administracyjnego, Litwa), który kieruje do Trybunału następujące pytanie prejudycjalne:

„Czy art. 15 ust. 1 dyrektywy 2002/58 […] w związku z art. 7, 8, 11 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej [(zwanej dalej »kartą«)] należy interpretować w ten sposób, że zakazuje on właściwym organom publicznym wykorzystywania danych zatrzymywanych przez dostawców usług łączności elektronicznej, które mogą dostarczać informacji o danych użytkownika środków łączności elektronicznej i o połączeniach realizowanych przez takiego użytkownika, w dochodzeniach, które dotyczą związanych z korupcją przewinień podczas sprawowania urzędu publicznego, niezależnie od tego, czy dostępu do tych danych udzielono w konkretnej sprawie na potrzeby zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego?”.

III. Postępowanie przed Trybunałem

31. Wniosek o wydanie orzeczenia w trybie prejudycjalnym został złożony w Trybunale Sprawiedliwości w dniu 3 marca 2022 r.

32. Uwagi na piśmie zostały przedstawione przez A.G., rządy czeski, estoński, węgierski, irlandzki, włoski i litewski oraz przez Komisję Europejską.

33. Na rozprawie, która odbyła się w dniu 2 lutego 2023 r., stawili się A.G., rządy francuski, węgierski, irlandzki i litewski oraz Komisja.

IV. Analiza

A. Dopuszczalność. Określenie zakresu odpowiedzi na pytanie prejudycjalne

34. Sąd odsyłający jest sądem administracyjnym, właściwym do kontroli sądowej decyzji, również administracyjnych. Taki charakter ma decyzja wydana przez prokuratora generalnego, który nałożył na urzędnika prokuratury okręgowej karę w postaci odwołania z urzędu w związku z czynami stanowiącymi przewinienia służbowe.

35. Przedmiotem postępowania głównego nie są zatem orzeczenia organów sądowych w sprawach karnych. Nawet jeśli orzeczenia te współistnieją z (dyscyplinarnym) postępowaniem administracyjnym, które doprowadziło do odwołania z urzędu[14], należy podkreślić, że spór istnieje tylko w odniesieniu do decyzji o odwołaniu z urzędu.

[14] Zobacz przypis 13 do niniejszej opinii.

36. W związku z tym w postanowieniu odsyłającym pojawia się pewna nieścisłość w odniesieniu do okoliczności faktycznych sporu, które stanowią kontekst, w jaki wpisuje się pytanie prejudycjalne.

37. Jak podkreśliły rząd czeski i Komisja, nie jest możliwe ustalenie z całą pewnością na podstawie postanowienia odsyłającego, czy właściwe organy: a) zwróciły się do dostawców usług łączności elektronicznej w celu uzyskania spornych danych, czy też b) same uzyskały te dane w sposób bezpośredni.

38. Nie jest to bynajmniej kwestia mało istotna. Zależy od niej określenie, które przepisy prawa Unii są istotne dla udzielenia odpowiedzi na pytanie prejudycjalne. W zależności od tego, czy okoliczności faktyczne miały miejsce w taki czy inny sposób, należy zastosować:

– dyrektywę 2002/58, jeżeli uzyskane dane wynikają z obowiązku przetwarzania nałożonego na dostawców usług łączności elektronicznej; lub

– dyrektywę 2016/680, jeżeli dane zostały uzyskane bezpośrednio przez organ publiczny, bez nakładania obowiązków na tych dostawców.

39. W tym drugim przypadku ochrona danych osobowych podlegałaby prawu krajowemu, bez uszczerbku dla stosowania dyrektywy 2016/680[15]. W związku z tym w pytaniu prejudycjalnym przyjęto by niewłaściwe podejście, kładąc nacisk na dyrektywę 2002/58.

40. Rząd węgierski, w przekonaniu, że dane osobowe zostały uzyskane w drodze operacji podsłuchu przeprowadzonych przez służby informacji kryminalnych, kwestionuje dopuszczalność odesłania prejudycjalnego, ponieważ jego zdaniem dyrektywa 2002/58 nie ma w związku z tym zastosowania.

41. Jednakże zdaniem Komisji:

– dyrektywa 2016/680 ma zastosowanie w zakresie, w jakim chodzi o wykorzystanie do celów późniejszego dochodzenia danych osobowych zbieranych i zatrzymywanych bezpośrednio przez organy w ramach uprzedniego postępowania przygotowawczego;

– dyrektywa 2002/58 ma zastosowanie, jeżeli – jak stwierdził sąd odsyłający[16] – przynajmniej niektóre dane musiały być zbierane i zatrzymywane na podstawie przepisu krajowego przyjętego zgodnie z art. 15 ust. 1 tej dyrektywy. Dyrektywa 2002/58 ma zatem znaczenie dla rozstrzygnięcia sporu.

42. Zgadzam się z tym podejściem Komisji, które ponadto jest jedynym podejściem pozwalającym na przezwyciężenie (uzasadnionych) zastrzeżeń co do dopuszczalności postanowienia odsyłającego.

[15] Wyrok La Quadrature du Net, pkt 103: „kiedy państwa członkowskie wprowadzają bezpośrednio środki stanowiące odstępstwo od poufności łączności elektronicznej, bez nakładania obowiązków przetwarzania na dostawców usług łączności elektronicznej, ochrona danych osób, których dane dotyczą, jest objęta nie dyrektywą 2002/58, ale jedynie prawem krajowym, z zastrzeżeniem stosowania [dyrektywy 2016/680]”.

[16] Punkt 37 postanowienia odsyłającego.

43. Jeżeli rozumieć pytanie prejudycjalne w ten sposób, znaczenie dyrektywy 2002/58 dla udzielenia na nie odpowiedzi:

– wynika z domniemania związanego z każdym odesłaniem prejudycjalnym, dotyczącego konieczności wystąpienia z takim odesłaniem, za które odpowiedzialność spoczywa na sądzie odsyłającym [17];

– można zaakceptować z tego względu, że zwrócono się do Trybunału o dokonanie wykładni tylko w odniesieniu do tej dyrektywy 2002/58, którą sąd uznaje za kluczową dla rozstrzygnięcia sporu [18].

44. Zdaniem sądu odsyłającego dla zawisłego przed nim postępowania istotne są bowiem:

„(i) dostęp do *danych zatrzymywanych przez dostawców usług łączności elektronicznej* nie tylko w celu zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego; oraz

(ii) *korzystanie z zatrzymywanych danych* uzyskanych w celu zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego przy prowadzeniu dochodzenia w sprawie związanego z korupcją przewinienia podczas sprawowania urzędu” [19].

45. Wszystko wydaje się zatem wskazywać na to, że niezależnie od ewentualnej zbieżności danych osobowych, których przetwarzanie nie mogłoby być objęte zakresem stosowania dyrektywy 2002/58 (lecz zakresem stosowania dyrektywy 2016/680), w dochodzeniu, które doprowadziło do nałożenia kary, wykorzystano dane osobowe uzyskane od dostawców usług łączności elektronicznej.

46. Odpowiedź Trybunału powinna ograniczać się do wniosku sądu odsyłającego zgodnie z jego sformułowaniem przedstawionym przez ten sąd. Należy zatem ustalić, czy dane osobowe uzyskane i przetwarzane na podstawie art. 15 ust. 1 dyrektywy 2002/58 w ramach postępowania przygotowawczego mogą zostać następnie wykorzystane w (administracyjnym) postępowaniu dyscyplinarnym przeciwko urzędnikowi publicznemu.

47. Po określeniu w ten sposób granic odesłania prejudycjalnego odwrotnością do tego, co zostało przedstawione powyżej, jest okoliczność, że następujące kwestie pozostają poza zakresem odesłania prejudycjalnego:

– Po pierwsze, kwestie dotyczące zgodności z prawem *pierwotnego uzyskania* danych osobowych na podstawie art. 15 ust. 1 dyrektywy 2002/58. Pytanie sądu odsyłającego ogranicza się do

[17] Zobacz między innymi wyroki: z dnia 4 grudnia 2018 r., Minister for Justice and Equality i Commissioner of An Garda Síochána (C-378/17, EU:C:2018:979, pkt 26); a także z dnia 22 grudnia 2022 r., Airbnb Ireland i Airbnb Payments UK (C-83/21, EU:C:2022:1018, pkt 82).

[18] Jednoznaczne odniesienie do dyrektywy 2002/58 w sentencji postanowienia odsyłającego i milczenie na temat dyrektywy 2016/680 w jego uzasadnieniu prawnym prowadzą do tego samego rezultatu. Zupełnie inną kwestią jest, że Trybunał, nie wykraczając poza granice pytania, może udzielić sądowi odsyłającemu użytecznych wskazówek do wydania przez niego wyroku, powołując się ewentualnie na inne przepisy prawa Unii. Zobacz podobnie wyrok z dnia 18 września 2019 r., VIPA (C-222/18, EU:C:2019:751, pkt 50 i przytoczone tam orzecznictwo).

[19] Punkt 35 postanowienia odsyłającego. Podkreślenie moje.

późniejszego wykorzystania tych danych w postępowaniu dyscyplinarnym, bez podawania w wątpliwość zgodności z prawem ich pierwotnego uzyskania [20].

– Po drugie, kwestie dotyczące wykorzystania danych uzyskanych i przetwarzanych bezpośrednio przez organy publiczne w ramach wcześniejszych postępowań przygotowawczych. Sąd odsyłający nie podnosi również wątpliwości w tej kwestii, której uregulowanie jest objęte zakresem prawa krajowego i dyrektywy 2016/680.

48. Podsumowując – w poniższych rozważaniach co do istoty należy pominąć wykładnię dyrektywy 2016/680 [21]. W odniesieniu do dyrektywy 2002/58 rozważania zostaną ograniczone do wykorzystania danych osobowych uzyskanych na jej podstawie w drodze operacji przetwarzania, których pierwotną zgodność z prawem należy domniemywać w zakresie, w jakim nie jest ona kwestionowana w postępowaniu głównym.

B. Co do istoty

1. Przypomnienie orzecznictwa Trybunału dotyczącego stosowania dyrektywy 2002/58

49. Z art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 wynika, że państwa członkowskie mogą uchwalić środek stanowiący odstępstwo od zasady poufności ustanowionej w art. 5 ust. 1 tej dyrektywy, gdy taki środek jest „niezbędny, właściwy i proporcjonalny w ramach społeczeństwa demokratycznego" oraz „[ściśle]" proporcjonalny do zamierzonego celu [22].

50. W szczególności możliwość uzasadnienia przez państwa członkowskie ograniczenia praw i obowiązków przewidzianych w szczególności w art. 5, 6 i 9 dyrektywy 2002/58 należy oceniać w drodze badania wagi ingerencji, jaką stanowi takie ograniczenie, oraz sprawdzenia, czy znaczenie celu interesu ogólnego, do którego zmierza to ograniczenie, pozostaje w relacji do tej wagi [23].

51. „Aby spełniać wymóg proporcjonalności, uregulowanie krajowe musi zawierać jasne i precyzyjne przepisy regulujące zakres i sposób stosowania rozpatrywanego środka oraz ustanawiające minimalne wymogi służące temu, aby osoby, o których dane osobowe chodzi, miały wystarczające gwarancje pozwalające na skuteczną ochronę tych danych przed ryzykiem nadużyć. Uregulowanie to musi być prawnie wiążące w prawie wewnętrznym i w szczególności wskazywać, w jakich okolicznościach i pod jakimi warunkami można przyjąć środek przewidujący przetwarzanie takich danych […]" [24].

[20] Nie jest zatem konieczne, aby Trybunał wypowiedział się w przedmiocie zgodności z prawem tych wcześniejszych operacji. Gdyby to uczynił, należałoby powtórzyć, że *dostęp* do danych będących w posiadaniu dostawców usług łączności elektronicznej może być udzielony, tylko jeżeli ich *zatrzymywanie* jest zgodne z art. 15 ust. 1 dyrektywy 2002/58. Zobacz podobnie wyrok La Quadrature du Net, pkt 167. Przepis ten, interpretowany w związku z art. 7, 8, 11 i art. 52 ust. 1 karty, stoi na przeszkodzie środkom ustawodawczym przewidującym w tych celach prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji (wyrok La Quadrature du Net, pkt 168).

[21] Odniosę się do niej jednak pomocniczo w końcowej części niniejszej opinii.

[22] Wyrok La Quadrature du Net, pkt 129.

[23] Wyrok La Quadrature du Net, pkt 131 i przytoczone tam orzecznictwo.

[24] Wyrok Commissioner of An Garda Síochána, pkt 54.

52. Jeśli chodzi o względy interesu ogólnego mogące uzasadniać środek przyjęty na podstawie art. 15 ust. 1 dyrektywy 2002/58, zgodnie z zasadą proporcjonalności istnieje hierarchia celów w zależności od znaczenia każdego z nich: znaczenie celu przyświecającego takiemu środkowi musi pozostawać w związku z wagą ingerencji [25].

53. W tej hierarchii celów ochrona bezpieczeństwa narodowego, interpretowana w świetle art. 4 ust. 2 TUE, wykracza poza inne cele, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, a mianowicie obronność, bezpieczeństwo publiczne lub zapobieganie, dochodzenie, wykrywanie i karanie przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej. Cel polegający na zwalczaniu przestępstw w ogólności, choćby poważnych, i ochrony bezpieczeństwa publicznego należy do tej drugiej kategorii [26].

54. Z tej kategoryzacji celów wynika, że:

– Cel polegający na ochronie bezpieczeństwa narodowego, pierwszy w porządku hierarchicznym wskazanym przez Trybunał, pozwala na tak daleko idące ingerencje jak te, które stanowią środki ustawodawcze umożliwiające nałożenie na dostawców usług łączności elektronicznej obowiązku uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji [27].

– Kolejny z najistotniejszych celów, a mianowicie zwalczanie poważnej przestępczości, może uzasadniać ingerencje takie jak na przykład ukierunkowane zatrzymywanie danych o ruchu i danych o lokalizacji lub adresów IP przydzielonych źródłu połączenia na okres ograniczony do tego, co ściśle niezbędne [28].

2. Zastosowanie tego orzecznictwa w niniejszym odesłaniu prejudycjalnym

55. Zdaniem sądu odsyłającego rozpatrywane informacje zostały uzyskane w drodze poważnych ingerencji w prawa zagwarantowane na mocy art. 7, 8 i 11 karty [29].

56. Pragnę powtórzyć, że nie chodzi tu o zbadanie pierwotnej zgodności z prawem uzyskania tych danych, to znaczy o ocenę, czy ingerencja była wystarczająco uzasadniona ze względu na wagę przestępstwa, przeciwko któremu miały być podjęte działania.

57. Sąd odsyłający wypowiedział się w obu tych kwestiach (waga ingerencji i waga naruszenia) w sposób, który nie jest przedmiotem sporu w postępowaniu głównym, a zatem nie ma znaczenia dla odesłania prejudycjalnego.

[25] Wyrok Commissioner of An Garda Síochána, pkt 56.

[26] Wyrok La Quadrature du Net, pkt 135 i 136, w których wyjaśniono, że bezpieczeństwo narodowe stanowi wyłączną odpowiedzialność państwa, która obejmuje pierwszorzędny interes w ochronie podstawowych funkcji państwa i podstawowych interesów społeczeństwa przed działalnością mogącą poważnie zdestabilizować podstawowe struktury konstytucyjne, polityczne, gospodarcze lub społeczne kraju, w szczególności bezpośrednio zagrozić społeczeństwu, ludności lub państwu jako takiemu, taką jak działalność terrorystyczna. Zagrożenia te różnią się ze względu na swój charakter i szczególną wagę od ogólnych zagrożeń powstania napięć i problemów, choćby poważnych, dla bezpieczeństwa publicznego. Cel ochrony bezpieczeństwa narodowego może zatem uzasadniać środki związane z dalej idącą ingerencją w prawa podstawowe niż środki, które mogłyby być uzasadnione tymi innymi celami.

[27] Wyrok Commissioner of An Garda Síochána, pkt 58.

[28] Wyrok La Quadrature du Net, pkt 168.

[29] Wynika to z pkt 46 postanowienia odsyłającego: zawiera on odniesienie do danych, które mogą dostarczyć informacji o połączeniach dokonywanych przez użytkownika środka łączności elektronicznej lub o lokalizacji urządzeń końcowych, z których użytkownik korzysta i które umożliwiają wyciągnięcie dokładnych wniosków na temat życia prywatnego danych osób.

58. Zgodnie ze sformułowaniem sądu odsyłającego istotne jest obecnie ustalenie, czy dane te: a) mogą być również wykorzystane w późniejszych dochodzeniach mających na celu zwalczanie przestępczości w ogólności (zakładając, że pojęcie to obejmuje zachowanie będące przedmiotem spornej kary dyscyplinarnej); czy też b) mogą być wykorzystane jedynie w dochodzeniach mających na celu zwalczanie poważnej przestępczości.

59. Rządy czeski i irlandzki zbadały, czy zachowanie będące przedmiotem postępowania przed sądem odsyłającym powinno zostać uznane za „poważne naruszenie", i doszły do wniosku, że tak jest.

60. Uważam jednak, że jest to kwestia, co do której Trybunał nie musi orzekać, ponieważ kwalifikacja zachowania należy do sądu odsyłającego.

61. Sąd odsyłający stwierdza, że jeśli wykorzystanie danych uzyskanych w drodze poważnej ingerencji w prawa podstawowe mogłoby być uzasadnione jedynie walką z poważną przestępczością i zapobieganiem poważnym zagrożeniom dla bezpieczeństwa publicznego, to dane te nie mogły być wykorzystane w dochodzeniach w sprawie przewinień dyscyplinarnych związanych z korupcją [30] – to znaczy w dochodzeniach takich jak to będące przedmiotem sporu w niniejszej sprawie.

62. W oparciu o tę ocenę istotne jest ustalenie, czy przewinienia dyscyplinarne, w celu ścigania których zamierza się wykorzystać określone dane osobowe, muszą być jakościowo równoważne pod względem ich wagi przewinieniom, które uzasadniały uzyskanie tych danych [31].

63. Na rozprawie rząd litewski przyznał, że odwołanie z urzędu zostało zastosowane z powodu naruszenia zasad etyki przez ukaranego prokuratora. Ocena, czy takie naruszenie (przeciek informacji dotyczących postępowania przygotowawczego) może zostać zrównane z poważnym przestępstwem lub wiązać się z poważnym zagrożeniem dla ochrony bezpieczeństwa publicznego, zależy od szeregu czynników, które może zweryfikować jedynie sąd odsyłający [32].

64. Na rozprawie odnoszono się wielokrotnie do walki z korupcją jako zjawiska leżącego u podstaw zachowań takich jak rozpatrywane w niniejszej sprawie. Debata nad tą kwestią wymagałaby wielu niuansów w celu zachowania rygoru wymaganego we wszystkich przejawach uprawnienia państwa do nakładania kar. Należałoby na przykład ustalić, czy termin „korupcja" jest używany w znaczeniu ogólnym, czy też odnosi się do konkretnego rodzaju zachowania, do

[30] Postanowienie odsyłające, pkt 46 in fine.

[31] W wyroku Europejskiego Trybunału Praw Człowieka (ETPC) z dnia 18 stycznia 2022 r. w sprawie Adomaitis przeciwko Litwie (CE:ECHR:2022:0118JUD001483318; zwanym dalej „wyrokiem ETPC w sprawie Adomaitis"), dotyczącym przechwytywania łączności elektronicznej w przypadku ciągłego nadużywania władzy przez dyrektora zakładu karnego, dostarczono wskazówek umożliwiających ocenę tej równoważności.

[32] Co do zasady nie można zrównywać czynów karalnych, których ściganie następuje w drodze postępowania karnego, z jednej strony, z czystymi naruszeniami zasad etyki, które są karane w drodze postępowania dyscyplinarnego, z drugiej strony. Postępowanie karne i postępowanie dyscyplinarne różnią się, jeśli chodzi o ich przedmiot, charakter i wagę zachowania podlegającego ocenie. Rozbieżność postępowań wskazuje w tym celu na różnicę w wadze przedmiotów tych postępowań.

którego – w ujęciu abstrakcyjnym – włączenie samego naruszenia obowiązku zachowania tajemnicy, jeżeli nie towarzyszy mu związana z nim korzyść na rzecz urzędnika, byłoby być może nadmierne [33].

65. W każdym razie w sytuacji gdy sąd odsyłający uznaje, że waga naruszenia zasad etyki zawodowej, w związku z którym nałożono karę w niniejszej sprawie, jest mniejsza niż waga przestępstwa, którego dochodzenie uzasadniało środek przyjęty na podstawie art. 15 dyrektywy 2002/58, odpowiedź na jego pytanie prejudycjalne wynika z następujących stwierdzeń Trybunału:

– „[D]ostęp do danych o ruchu i do danych o lokalizacji zatrzymywanych przez dostawców w zastosowaniu środka przyjętego na podstawie art. 15 ust. 1 dyrektywy 2002/58, co musi mieć miejsce w pełnym poszanowaniu warunków wynikających z orzecznictwa, w którym dokonano wykładni dyrektywy 2002/58, może co do zasady być uzasadniony jedynie celem interesu ogólnego, dla którego dostawcy ci zostali zobowiązani do takiego zatrzymywania. Inaczej jest jedynie wtedy, gdy znaczenie celu przyświecającego dostępowi jest większe niż znaczenie celu, który uzasadniał zatrzymywanie danych” [34].

– „[W] szczególności […] nie można w żadnym wypadku udzielić dostępu do takich danych do celów ścigania i ukarania zwykłego przestępstwa, jeżeli ich zatrzymywanie było uzasadnione celem walki z poważną przestępczością lub, a fortiori, celem ochrony bezpieczeństwa narodowego” [35].

66. W tym względzie obowiązuje zatem swego rodzaju zasada równoważności między celami interesu publicznego, które uzasadniają *uzyskanie* danych osobowych, z jednej strony, a celami, które uzasadniają ich późniejsze *wykorzystanie*, z drugiej strony. Jak wskazano powyżej, jedynym wyjątkiem od tej zasady jest to, że znaczenie celu realizowanego przez dostęp jest większe niż znaczenie celu, który uzasadniał zatrzymywanie danych.

67. Rozumienie tego w inny sposób prowadziłoby do wypaczenia systemu gwarancji ustanowionego w dyrektywie 2002/58: prawa, które dyrektywa ta chroni, mogłyby być przedmiotem poważnych ingerencji poza przypadkami przewidzianymi w art. 15 owej dyrektywy i warunkami określonymi w orzecznictwie Trybunału.

68. W szczególności poświęcenie nienaruszalności prawa do poufności połączeń jest prawnie dopuszczalne jedynie w świetle konkretnego celu interesu ogólnego, któremu służy. Dlatego też zgodność z prawem dostępu do zatrzymywanych danych należy sprawdzać w każdym konkretnym przypadku, dokonując wyważenia z jednej strony wagi, z jaką wiąże się dostęp, a z drugiej strony znaczenia celu interesu ogólnego, któremu ma służyć ta ingerencja.

[33] W Konwencji sporządzonej na podstawie artykułu K.3 ustęp 2 litera c) Traktatu o Unii Europejskiej w sprawie zwalczania korupcji urzędników Wspólnot Europejskich i urzędników państw członkowskich Unii Europejskiej (Dz.U. 1997, C 195, s. 2) przewidziano przypadki korupcji biernej („umyślne działanie urzędnika, który bezpośrednio lub za pośrednictwem żąda lub otrzymuje korzyści dowolnego rodzaju dla siebie lub strony trzeciej lub przyjmuje obietnicę takiej korzyści w zamian za dokonanie lub powstrzymanie się, z naruszeniem swoich obowiązków urzędniczych, od dokonania czynności wynikającej z jego funkcji lub w ramach wykonywania jego funkcji”) i korupcji czynnej („umyślne działanie kogokolwiek, polegające na dawaniu obietnicy lub przekazywaniu, w sposób bezpośredni lub za pośrednictwem, korzyści dowolnego rodzaju, urzędnikowi lub stronie trzeciej, aby sprawić, by osoba ta dokonała lub powstrzymała się, z naruszeniem swoich obowiązków urzędniczych, od dokonania czynności wynikającej z jej funkcji lub w ramach wykonywania jej funkcji”), które należy zakwalifikować jako przestępstwa.

[34] Wyrok Commissioner of An Garda Síochána, pkt 98.

[35] Wyrok La Quadrature du Net, pkt 166.

69. Nie można zgodzić się z wykładnią dyrektywy 2002/58, zgodnie z którą po udzieleniu dostępu w pierwszym przypadku, który skutecznie go uzasadnia, otwarta jest droga do późniejszego dostępu (w rzeczywistości do ponownego wykorzystania uzyskanych danych), opartego na celu hierarchicznie niższym niż cel tego pierwotnego przypadku.

70. W tym celu wymogi dotyczące pierwotnego dostępu (w tym wymogi określone przez Trybunał w odniesieniu do wydania zgody na dostęp)[36] mają zastosowanie do późniejszego wykorzystania tych samych danych przez inne organy.

C. Pomocniczo: wpływ dyrektywy 2016/680

71. Jak dotąd przedstawiłem to, co uważam za najbardziej odpowiednie do celów udzielenia odpowiedzi na wniosek o wydanie orzeczenia w trybie prejudycjalnym zgodnie z jego sformułowaniem, to znaczy poprzez przedstawienie sądowi odsyłającemu wykładni dyrektywy 2002/58, o którą sąd ten wnosi.

72. W przypadku gdyby dane będące przedmiotem sporu w niniejszej sprawie nie zostały uzyskane na podstawie art. 15 ust. 1 dyrektywy 2002/58, lecz bezpośrednio przez służby informacji kryminalnych państwa członkowskiego w postępowaniu karnym, sytuacja byłaby inna.

73. W takim przypadku zastosowanie miałyby przepisy prawa krajowego, bez uszczerbku dla stosowania dyrektywy 2016/680 w odniesieniu do przetwarzania danych osobowych uzyskanych w postępowaniu przygotowawczym. Zakładam, że działania służb informacji kryminalnych w przypadkach takich jak niniejszy są objęte zakresem dyrektywy 2016/680. Zostało to potwierdzone na rozprawie.

74. Jak wskazałem w opinii w sprawie Inspektor v Inspektorata kam Visshia sadeben savet (Cele przetwarzania danych osobowych – Postępowanie karne)[37], „RODO i dyrektywa 2016/680 tworzą spójny system, w którym:

– W RODO ustanowione są *przepisy ogólne* dotyczące ochrony osób fizycznych w odniesieniu do przetwarzania ich danych osobowych.

– W dyrektywie 2016/680 ustanowione są *przepisy szczególne* dotyczące przetwarzania takich danych w ramach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej”[38].

75. Następnie przypomniałem[39], że:

– „Ochrona zapewniona przez system utworzony przez te dwa akty prawne opiera się na zasadach zgodności z prawem, rzetelności, przejrzystości oraz – w zakresie, w jakim to ma znaczenie w niniejszej sprawie – na zasadzie ścisłego ograniczenia zbierania danych i ich przetwarzania w celach określonych przez prawo”.

[36] Wyrok Commissioner of An Garda Síochána, pkt 106, w którym powołano się na wyrok Prokuratuur, pkt 51.

[37] C-180/21 (EU:C:2022:406), zwana dalej „opinią Inspektor v Inspektorata”.

[38] Opinia Inspektor v Inspektorata, pkt 35.

[39] Opinia Inspektor v Inspektorata, pkt 36–39.

– „W szczególności art. 5 ust. 1 lit. b) RODO stanowi, że dane muszą być »zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach *i nieprzetwarzane dalej w sposób niezgodny z tymi celami*«. Takie jest też brzmienie art. 4 ust. 1 lit. b) dyrektywy 2016/680 jako lex specialis".

– „Dane osobowe nie mogą być zatem zbierane i przetwarzane w sposób ogólny, lecz tylko w określonych celach i z zastrzeżeniem warunków zgodności z prawem ustanowionych przez prawodawcę Unii" [40].

– „Zasada ścisłego powiązania między zbieraniem i przetwarzaniem danych z jednej strony a celami, którym obie te operacje powinny służyć, z drugiej strony nie ma charakteru bezwzględnego, ponieważ zarówno RODO, jak i dyrektywa 2016/680 dopuszczają pewną elastyczność […]".

76. Jednakże, zgodnie z dokonaną przez Trybunał wykładnią art. 4 ust. 2 dyrektywy 2016/680 [41], trudno przyjąć, że dane osobowe zebrane w toku postępowania karnego zostaną wykorzystane *w tym samym celu* w ramach późniejszego postępowania dyscyplinarnego przeciwko urzędnikowi publicznemu.

77. Muszę jednak przypomnieć, że zgodnie z art. 4 ust. 2 dyrektywy 2016/680 „[p]rzetwarzanie przez tego samego lub innego administratora w jednym z celów określonych w art. 1 ust. 1 innym niż cel, w którym dane osobowe zostały zebrane, jest dozwolone, o ile:

— administratorowi wolno przetwarzać takie dane osobowe w takim celu na mocy prawa Unii lub prawa państwa członkowskiego; oraz

— przetwarzanie jest niezbędne i proporcjonalne w tym innym celu na mocy prawa Unii lub prawa państwa członkowskiego".

78. W oparciu o to założenie sąd odsyłający będzie musiał rozważyć, czy (*odmienny*) cel dalszego przetwarzania jest jednym z celów określonych w art. 1 ust. 1 dyrektywy 2016/680, czy też wykracza on poza te cele:

– W pierwszym przypadku (przeznaczenie ad intra) konieczne będzie ustalenie, czy spełnione są obie przesłanki przewidziane w art. 4 ust. 2 dyrektywy 2016/680.

– W drugim przypadku (przeznaczenie ad extra) w grę wchodzi art. 9 ust. 1 dyrektywy 2016/680.

[40] Przesłanka „zgodności z prawem" jest wymagana na mocy z art. 5 ust. 1 lit. a) RODO [art. 4 ust. 1 lit. a) dyrektywy 2016/680], a w art. 6 RODO zostały określone jej warunki. W zakresie, w jakim jest to istotne w niniejszej sprawie, i zgodnie z lit. e) tego przepisu przetwarzanie musi być niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (samego przetwarzania).

[41] Wyrok z dnia 8 grudnia 2022 r., Inspektor v Inspektorata kam Visshia sadeben savet (Cele przetwarzania danych osobowych – Postępowanie karne), C-180/21 (EU:C:2022:967), zwany dalej „wyrokiem Inspektor v Inspektorata".

1. Wykorzystanie danych zgodnie z art. 4 ust. 2 dyrektywy 2016/680

79. Jeśli chodzi o *pierwszą* z dwóch przesłanek wymaganych w tym przepisie, będzie ona spełniona tylko wtedy, gdy w prawie państwa członkowskiego zostanie przyjęta ustawa [42] regulująca, kiedy administrator jest upoważniony do przetwarzania danych osobowych. Ustawa ta musi ponadto zawierać wiążące, jasne i precyzyjne przepisy [43].

80. Jest to jednak kwestia, której ustalenie należy oczywiście do sądu odsyłającego, po przeprowadzeniu analizy art. 177 kodeksu postępowania karnego, art. 19 ust. 3 ustawy o wywiadzie kryminalnym i zaleceń prokuratury generalnej [44]. Na podstawie tych elementów należy ocenić, w jakim stopniu prawo krajowe zezwala na wykorzystanie pod pewnymi warunkami informacji uzyskanych w ramach postępowania karnego w kontekście dochodzenia w sprawie przewinień dyscyplinarnych. Uwagi zawarte w wyroku ETPC w sprawie Adomaitis mogą być przydatne dla sądu odsyłającego w dokonaniu wspomnianego ustalenia [45].

81. Jeśli chodzi o *drugą* przesłankę, sąd odsyłający będzie musiał ocenić, czy przy przetwarzaniu danych będących przedmiotem niniejszej sprawy ingerencja była konieczna oraz czy była ona proporcjonalna [46].

82. Stwierdzenia zawarte w wyroku ETPC w sprawie Adomaitis również mogą przyczynić się do tej oceny:

– Jeśli chodzi o konieczny charakter, należy wyważyć, w jakim stopniu niewystarczające dowody w postaci innych informacji dostępnych w toku postępowania dyscyplinarnego sprawiły, że dla powodzenia toczącego się dochodzenia rzeczywiście konieczne było wykorzystanie spornych informacji [47].

– Jeśli chodzi o proporcjonalność, należy ocenić wagę naruszenia, które doprowadziło do wszczęcia postępowania dyscyplinarnego, zważywszy, że – jak podniósł rząd litewski i jak wynika z wyroku ETPC w sprawie Adomaitis [48] – wykorzystanie danych osobowych jest zastrzeżone dla przypadków naruszeń, w odniesieniu do których przewidziana jest najsurowsza kara dyscyplinarna, a mianowicie odwołanie z urzędu.

[42] Zgadzam się z Komisją, że ponieważ późniejsze wykorzystanie danych osobowych uzyskanych w toku postępowania przygotowawczego stanowi ingerencję w prawa podstawowe zagwarantowane na mocy art. 7 i 8 karty, to zgodnie z art. 52 ust. 1 karty niezbędne jest, aby było ono przewidziane ustawą.

[43] Punkt 48 niniejszej opinii.

[44] Przypis 12 do niniejszej opinii.

[45] W punkcie 83 tego wyroku uznano, że gwarancja zgodności ingerencji z prawem zapewniona przez krajowe przepisy ustawodawcze i litewskie orzecznictwo konstytucyjne jest wystarczająca.

[46] Jak zauważa Komisja, sprawa ta nie różni się znacząco od sprawy rozpatrywanej w wyroku ETPC z dnia 16 czerwca 2016 r. w sprawie Versini-Campinchi i Crasnianski przeciwko Francji (CE:ECHR:2016:0616JUD004917611). Zgodnie z pkt 57 tego wyroku wykorzystanie w ramach postępowania dyscyplinarnego w sprawie naruszenia tajemnicy zawodowej połączeń, które miały miejsce w postępowaniu karnym, odpowiada zgodnemu z prawem celowi w rozumieniu art. 8 EKPC. Ścisłe materialne powiązanie między przedmiotami postępowania karnego i postępowania dyscyplinarnego przemawia za wspólnością zgodności z prawem celów obu tych postępowań.

[47] Wyrok ETPC w sprawie Adomaitis, pkt 85.

[48] Wyrok ETPC w sprawie Adomaitis, pkt 87.

2. Wykorzystanie danych zgodnie z art. 9 dyrektywy 2016/680

83. Zgodnie z art. 9 ust. 1 dyrektywy 2016/680 dane osobowe zebrane przez właściwe organy do celów określonych w art. 1 ust. 1 można przetwarzać do celów innych niż określone w art. 1 ust. 1, gdy takie przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego. W takim przypadku zastosowanie będzie miało RODO, chyba że przetwarzanie odbywa się w toku działalności nieobjętej prawem Unii [49].

84. W przypadku gdyby sąd odsyłający uznał, że art. 4 ust. 2 dyrektywy 2016/680 nie ma zastosowania, będzie on musiał zastosować RODO. Zgodnie z tym rozporządzeniem konieczne będzie ustalenie, czy oprócz przepisu prawa spełniona jest przynajmniej jedna z przesłanek zgodności z prawem przetwarzania danych osobowych wymienionych wyczerpująco w art. 6 ust. 1 owego rozporządzenia.

V. Wnioski

85. W świetle powyższego proponuję Trybunałowi, by odpowiedział Lietuvos vyriausiasis administracinis teismas (najwyższemu sądowi administracyjnemu Litwy) w następujący sposób:

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

   należy interpretować w ten sposób, że:

   nie zezwala on właściwym organom publicznym na zbieranie zatrzymywanych przez dostawców usług łączności elektronicznej danych mogących dostarczyć szczegółowych informacji o użytkowniku oraz na wykorzystanie ich w ramach dochodzeń w sprawie zachowań stanowiących naruszenia mniej poważne niż te, których dochodzenie mogło w danym momencie uzasadniać dostęp do tych danych.

2. Pomocniczo:

   Artykuł 9 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW w związku z art. 6 i 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE w świetle art. 7 i 8 Karty praw podstawowych Unii Europejskiej

   należy interpretować w ten sposób, że:

[49] Wyjątek ten był przedmiotem wykładni zawężającej dokonanej w wyroku z dnia 22 czerwca 2021 r., Latvijas Republikas Saeima (Punkty karne) (C-439/19, EU:C:2021:504, pkt 66).

nie stoi on na przeszkodzie wykorzystaniu w postępowaniu administracyjnym o charakterze dyscyplinarnym danych osobowych uzyskanych zgodnie z prawem i bezpośrednio przez organ publiczny w ramach postępowania przygotowawczego, pod warunkiem że zgodnie z jasnymi, precyzyjnymi i wiążącymi przepisami prawa krajowego to postępowanie administracyjne i to postępowanie przygotowawcze są ze sobą powiązane, a także w zakresie, w jakim wykorzystanie danych służy zgodnemu z prawem celowi oraz jest konieczne i proporcjonalne, czego ustalenie należy do organu sądowego.