Zbiór Orzeczeń

OPINIA RZECZNIKA GENERALNEGO
MANUELA CAMPOSA SÁNCHEZA-BORDONY
przedstawiona w dniu 20 kwietnia 2023 r. [1]

**Sprawa C-548/21**

**C.G.**
**przeciwko**
**Bezirkshauptmannschaft Landeck**

[wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Landesverwaltungsgericht Tirol (regionalny sąd administracyjny w Tyrolu, Austria)]

Odesłanie prejudycjalne – Telekomunikacja – Ochrona danych osobowych – Dyrektywa (UE) 2016/680 – Postępowanie karne – Próba dostępu organów publicznych, bez zezwolenia sądu lub niezależnego organu administracji, do danych zapisanych w telefonie komórkowym

1. Niniejszy wniosek o wydanie orzeczenia w trybie prejudycjalnym dotyczy w istocie warunków, które powinny spełnić organy policji w celu uzyskania dostępu do danych przechowywanych w telefonie komórkowym osoby, przeciwko której prowadzone jest postępowanie przygotowawcze.

2. Jak postaram się wyjaśnić, odesłanie prejudycjalne zawiera istotne braki w odniesieniu do jego dopuszczalności. Gdyby, pomimo wszystko, Trybunał Sprawiedliwości zdecydował się zbadać istotę sprawy, będzie on musiał wypowiedzieć się w przedmiocie zakresu zastosowania, odpowiednio, dyrektywy 2002/58/WE [2] oraz dyrektywy (UE) 2016/680 [3].

[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).

# I. Ramy prawne

## *A. Prawo Unii*

### *1. Rozporządzenie (UE) 2016/679*[4]

3. Artykuł 2 („Materialny zakres stosowania”) ust. 2 stanowi:

„Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:

[…]

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”.

### *2. Dyrektywa 2016/680*

4. W motywie 2 wskazano:

„Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych powinny […] przestrzegać ich podstawowych praw i wolności, zwłaszcza prawa do ochrony danych osobowych. Niniejsza dyrektywa ma przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości”.

5. Zgodnie z motywem 46:

„Każde ograniczenie praw osoby, której dane dotyczą, musi być zgodne z Kartą [praw podstawowych Unii Europejskiej; zwaną dalej »kartą«] i [europejską Konwencją o ochronie praw człowieka i podstawowych wolności, zwaną dalej »EKPC«], w myśl wykładni zawartej, odpowiednio, w orzecznictwie Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka[5], a zwłaszcza musi odbywać się z poszanowaniem istoty tych praw i wolności”.

6. Motyw 49 brzmi następująco:

„Jeżeli dane osobowe przetwarza się w toku postępowania przygotowawczego i sądowego w sprawie karnej, państwa członkowskie powinny mieć możliwość zapewnienia wykonywania prawa do informacji, dostępu lub poprawienia, usunięcia i ograniczenia przetwarzania zgodnie z krajowymi przepisami o postępowaniu sądowym”.

[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, zwane dalej „RODO”).

[5] Zwanego dalej „ETPC”.

7. Artykuł 1 („Przedmiot i cele”) 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.

2. Zgodnie z niniejszą dyrektywą państwa członkowskie:

a) chronią prawa podstawowe i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych; oraz

[…]

3. Niniejsza dyrektywa nie wyklucza ustanowienia przez państwa członkowskie zabezpieczeń wyższych niż zabezpieczenia przewidziane w niniejszej dyrektywie dla ochrony praw i wolności osoby, której dane dotyczą, w związku z przetwarzaniem danych osobowych przez właściwe organy”.

8. Artykuł 2 („Zakres zastosowania”) ust. 1 stwierdza:

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

9. Artykuł 3 („Definicje”) wskazuje:

„Na użytek niniejszej dyrektywy:

[…]

2) »przetwarzanie« oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

[…]

7) »właściwy organ« oznacza:

   a) organ publiczny właściwy do 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; lub

[…]”.

10. Artykuł 4 („Zasady dotyczące przetwarzania danych osobowych”) ust. 1 stanowi:

„Państwa członkowskie zapewniają, by dane osobowe były:

a) przetwarzane zgodnie z prawem i rzetelnie;

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

c) adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane;

[…]

e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania;

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych”.

11. Artykuł 8 („Zgodność przetwarzania z prawem”) wskazuje:

„1. Państwa członkowskie zapewniają, by przetwarzanie było zgodne z prawem wyłącznie wówczas i w zakresie, w jakim jest ono niezbędne do wykonania zadania realizowanego przez właściwy organ w celach określonych w art. 1 ust. 1 oraz ma podstawę w prawie Unii lub prawie państwa członkowskiego.

2. Prawo państwa członkowskiego regulujące przetwarzanie w zakresie stosowania niniejszej dyrektywy określa co najmniej powody przetwarzania, dane osobowe mające podlegać przetwarzaniu oraz cele przetwarzania”.

12. Artykuł 13 („Informacje udostępniane lub przekazywane osobie, której dane dotyczą”) przewiduje:

„1. Państwa członkowskie zapewniają, by administrator udostępniał osobie, której dane dotyczą, przynajmniej następujące informacje:

[…]

d) informacje o prawie do wniesienia skargi do organu nadzorczego oraz dane kontaktowe organu nadzorczego;

[…]

3. Państwa członkowskie mogą przyjąć akty prawne pozwalające opóźnić, ograniczyć lub pominąć informowanie osoby, której dane dotyczą, przewidziane w ust. 2 w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby:

a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;

b) uniemożliwić zakłócanie zapobiegani[a] przestępczości, prowadzeni[a] postępowań przygotowawczych, wykrywani[a] i ścigani[a] czynów zabronionych i wykonywaniu kar;

c) chronić bezpieczeństwo publiczne;

d) chronić bezpieczeństwo narodowe;

e) chronić prawa i wolności innych osób.

[…]".

13. Zgodnie z art. 15 („Ograniczenia prawa dostępu") ust. 1:

„Państwa członkowskie mogą przyjąć akty prawne pozwalające ograniczyć w całości lub w części prawo dostępu osoby, której dane dotyczą, w takim stopniu i przez taki okres, w jakim takie częściowe lub całkowite ograniczenie jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby:

a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;

b) uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar;

c) chronić bezpieczeństwo publiczne;

d) chronić bezpieczeństwo narodowe;

e) chronić prawa i wolności innych osób".

14. Na podstawie art. 27 („Ocena skutków dla ochrony danych"):

„1. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych, państwa członkowskie zapewniają, by administrator przed przetworzeniem dokonał oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

2. Ocena, o której mowa w ust. 1, zawiera co najmniej ogólny opis planowanych operacji przetwarzania, ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą, środki

planowane w celu rozwiązania takiego ryzyka, zabezpieczenia, środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazanie zgodności z niniejszą dyrektywą, z uwzględnieniem praw i uzasadnionych interesów osób, których dane dotyczą, i innych zainteresowanych osób".

15. Artykuł 28 („Uprzednie konsultacje z organem nadzorczym") stanowi:

„1. Państwa członkowskie zapewniają, by administrator lub podmiot przetwarzający przed przetwarzaniem danych osobowych, które będzie częścią mającego powstać nowego zbioru danych, skonsultowali się z organem nadzorczym, jeżeli:

a) ocena skutków dla ochrony danych, o której mowa w art. 27, wykaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia w razie niepodjęcia przez administratora środków w celu zminimalizowania tego ryzyka; lub

b) odnośny rodzaj przetwarzania – zwłaszcza z użyciem nowych technologii, mechanizmów lub procedur – stwarza poważne ryzyko naruszenia praw i wolności osób, których dane dotyczą.

[…]".

16. Artykuł 54 („Prawo do skutecznego środka prawnego przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu") stanowi:

„Z zastrzeżeniem dostępnych środków administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego na mocy art. 52, państwa członkowskie zapewniają osobie, której dane dotyczą, prawo do skutecznego środka prawnego przed sądem, jeżeli osoba ta uważa, iż jej prawa ustanowione w przepisach przyjętych na podstawie niniejszej dyrektywy zostały naruszone wskutek przetwarzania jej danych osobowych w sposób niezgodny z tymi przepisami".

### *B. Prawo krajowe*

17. Paragraf 18 Strafprozessordnung[6] przyznaje policji kryminalnej zadania w służbie wymiaru sprawiedliwości w sprawach karnych (ust. 1). Postępowania przygotowawcze prowadzone przez policję kryminalną należą do obowiązków organów bezpieczeństwa (ust. 2). Organy służb bezpieczeństwa publicznego dokonują czynności wykonawczych policji kryminalnej obejmujących prowadzenie postępowania przygotowawczego i ściganie przestępstw (ust. 3).

18. Zgodnie z § 99 StPO policja kryminalna prowadzi postępowanie przygotowawcze z urzędu lub na podstawie zawiadomienia, stosując się do nakazów prokuratora i sądu (ust. 1). Jeżeli czynność dokonywana w postępowaniu przygotowawczym wymaga nakazu prokuratora, policja kryminalna może, również bez nakazu, skorzystać z odpowiednich uprawnień w przypadku bezpośredniego zagrożenia. W takim przypadku powinna ona niezwłocznie wystąpić o zatwierdzenie czynności (ust. 2).

[6] Kodeks postępowania karnego, zwany dalej „StPO", BGBl nr 631/1975 w brzmieniu obowiązującym w momencie wystąpienia okoliczności faktycznych sprawy (BGBl I nr 24/2020).

19. Zgodnie z § 111 ust. 2 StPO, w przypadku gdy informacje przechowywane na nośnikach danych mają być przedmiotem zbierania danych, każdy jest zobowiązany umożliwić dostęp do wspomnianych informacji oraz, na wniosek, dostarczyć elektroniczny nośnik danych w powszechnie stosowanym formacie pliku lub umożliwić jego dostarczenie. Ponadto musi on umożliwić wykonanie kopii zapasowej informacji przechowywanych na nośnikach danych.

## II. Okoliczności faktyczne, postępowanie główne i pytania prejudycjalne

20. C.G. jest obywatelem niemieckim, który pracuje i mieszka w Austrii.

21. W dniu 23 lutego 2021 r., podczas kontroli na obecność narkotyków, urzędnicy urzędu celnego w Innsbrucku (Austria) przejęli adresowaną do C.G. paczkę, która zawierała 85 gramów marihuany.

22. W dniu 6 marca 2021 r. dwaj funkcjonariusze policji przesłuchali C.G. na okoliczność nadawcy przesyłki i dokonali przeszukania jego mieszkania. W trakcie przeszukania zatrzymano jego telefon komórkowy (wraz z kartą SIM i kartą SD) oraz doręczono mu protokół zatrzymania rzeczy.

23. Poproszony o umożliwienie wglądu do danych dotyczących połączeń zapisanych w jego telefonie komórkowym, C.G. nie wyraził na to zgody, jak również odmówił podania kodu dostępu do telefonu.

24. W Bezirkspolizeikommando w Landeck (Austria) nie udało się usunąć blokady telefonu komórkowego. Telefon został przesłany do Bundeskriminalamt (głównego urzędu policji kryminalnej) w Wiedniu (Austria), gdzie ponownie podjęto bezskuteczną próbę odblokowania telefonu i odczytania przechowywanych w nim danych.

25. W chwili zastosowania tych środków przez policję nie wydano w odniesieniu do nich nakazu prokuratury ani orzeczenia sądu.

26. W dniu 31 marca 2021 r. C.G. wniósł do Landesverwaltungsgericht Tirol (regionalnego sądu administracyjnego w Tyrolu, Austria) skargę na zastosowany wobec niego środek przymusu, kwestionując zatrzymanie telefonu komórkowego. Telefon komórkowy zwrócono mu w dniu 20 kwietnia 2021 r.

27. C.G. nie powiadomiono o próbie analizy zawartości telefonu komórkowego; dowiedział się o tym, ponieważ funkcjonariusz policji, który dokonał zatrzymania, a następnie rozpoczął analizę cyfrową, został przesłuchany w charakterze świadka pod przysięgą. Próba ta nie została również udokumentowana w aktach policji kryminalnej.

28. W związku z powyższym Landesverwaltungsgericht Tirol (regionalny sąd administracyjny w Tyrolu) przedstawił Trybunałowi Sprawiedliwości następujące pytania prejudycjalne:

„1) Czy art. 15 ust. 1 (ewentualnie w związku z art. 5) dyrektywy 2002/58 w brzmieniu zmienionym dyrektywą 2009/136/WE w świetle art. 7 i 8 [k]arty […]należy interpretować w ten sposób, że dostęp organów władzy publicznej do danych zapisanych na telefonach komórkowych stanowi ingerencję w prawa podstawowe opisane w przywołanych

postanowieniach karty, która to ingerencja jest na tyle poważna, by pociągnąć za sobą ograniczenie dostępu w kontekście zapobiegania, dochodzenia, wykrywania i ścigania przestępstw do zwalczania poważnej przestępczości?

2) Czy art. 15 ust. 1 dyrektywy 2002/58 w brzmieniu zmienionym dyrektywą 2009/136, w świetle art. 7, 8 i 11 oraz art. 52 ust. 1 [k]arty […] należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu, takiemu jak § 18 w związku z § 99 ust. 1 [StPO], które skutkuje tym, że organy bezpieczeństwa same, w trakcie postępowania karnego, bez zezwolenia sądu lub niezależnego organu administracyjnego zapewniają sobie obszerny i niekontrolowany dostęp do wszystkich danych cyfrowych zapisanych na telefonie komórkowym?

3) Czy art. 47 [k]arty […] w związku z jej art. 41 i 52 należy interpretować, mając na uwadze równość broni oraz skuteczność środka prawnego, jako stojący na przeszkodzie uregulowaniu państwa członkowskiego, które, tak jak § 18 w związku z § 99 ust. 1 [StPO], zezwala na analizę danych cyfrowych z telefonu komórkowego bez uprzedniego poinformowania o tym zainteresowanego, względnie bez poinformowania go przynajmniej po zastosowaniu środka?”.

## III. Postępowanie przed Trybunałem Sprawiedliwości

29. Wniosek o wydanie orzeczenia w trybie prejudycjalnym wpłynął do Trybunału Sprawiedliwości w dniu 6 września 2021 r.

30. W dniu 20 października 2021 r. Trybunał Sprawiedliwości zwrócił się do sądu odsyłającego o wskazanie, czy dyrektywa 2016/680 może mieć znaczenie w sprawie.

31. W dniu 11 listopada 2021 r. sąd odsyłający odpowiedział, że dyrektywa 2016/680 ma zastosowanie w postępowaniu głównym.

32. Uwagi na piśmie zostały przedstawione przez rządy niemiecki, austriacki, cypryjski, duński, estoński, francuski, węgierski, irlandzki, niderlandzki, norweski, polski i szwedzki, jak również przez Komisję Europejską.

33. Na rozprawie jawnej, która odbyła się w dniu 16 stycznia 2023 r., stawili się, z wyjątkiem rządów niemieckiego, węgierskiego i polskiego, uczestnicy postępowania, którzy przedstawili uwagi na piśmie, oraz rząd fiński. Wszyscy zostali wezwani przez Trybunał Sprawiedliwości o przedstawienie stanowisk przede wszystkim w odniesieniu do dyrektywy 2016/680 oraz o udzielenie ustnych odpowiedzi na określone pytania z nią związane.

## IV. Analiza

### *A. Niedopuszczalność*

34. Sąd odsyłający początkowo tak sformułował swoje pytania, że zwracał się w nich o dokonanie wykładni jedynie dyrektywy 2002/58. Jednakże praktycznie wszyscy interwenienci w postępowaniu zgadzają się, że dyrektywa ta nie ma zastosowania w niniejszej sprawie, zatem jej wykładnia nie jest konieczna dla rozstrzygnięcia sporu.

35. Zgodnie z art. 3 dyrektywy 2002/58 ma ona zastosowanie do „przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności [w Unii], włącznie z publicznymi sieciami łączności służącymi do zbierania danych i obsługi urządzeń identyfikacyjnych".

36. Trybunał Sprawiedliwości uznał, że „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]" [7].

37. W niniejszej sprawie próba dostępu do danych została podjęta bezpośrednio przez organy policji w ramach postępowania przygotowawczego. Nie miały miejsca żadne działania ze strony dostawców usług łączności elektronicznej, którzy nie zostali zobowiązani do przekazywania danych osobowych. Z tego względu dyrektywa 2002/58 nie ma zastosowania.

38. Aktem prawa Unii regulującym taki przypadek jest dyrektywa 2016/680, bowiem zgodnie z art. 2 ust. 1 tej dyrektywy ma ona zastosowanie do przetwarzania danych osobowych przez organy właściwe do „celów prowadzenia […] postępowań przygotowawczych [w sprawie] […] czynów zabronionych".

39. Powyższe wystarczałoby zatem do stwierdzenia, że odesłanie prejudycjalne, tak jak sformułował je sąd odsyłający, jest niedopuszczalne, ponieważ przepis prawa Unii, o którego wykładnię wniesiono, nie ma zastosowania w tej sprawie.

40. Nie ma wątpliwości co tego, że art. 267 TFUE pozwala Trybunałowi Sprawiedliwości na przeformułowanie przedstawionych mu pytań prejudycjalnych lub na wskazanie istnienia innych przepisów prawa Unii, które mogą mieć znaczenie dla sprawy, w celu udzielenia krajowemu sądowi odsyłającemu użytecznej odpowiedzi [8].

41. Trybunał Sprawiedliwości zwrócił się do sądu odsyłającego, aby ten wypowiedział się w przedmiocie ewentualnego wpływu dyrektywy 2016/680 na sprawę. Dał mu zatem możliwość uzupełnienia lub przeformułowania swoich pytań. Zamiast tego sąd odsyłający poprzestał na stwierdzeniu, że „w niniejszej sprawie należy w każdym razie przestrzegać wymogów ustanowionych w dyrektywie (UE) 2016/680", jednak nie wskazał przepisów dyrektywy, w przedmiocie których powziął wątpliwości, ani nie przedstawił innych rozważań merytorycznych [9].

42. Trybunał Sprawiedliwości stwierdził wielokrotnie, że „[j]est […] niezbędne, jak stanowi art. 94 lit. c) regulaminu postępowania, by wniosek o wydanie orzeczenia w trybie prejudycjalnym zawierał omówienie powodów, dla których sąd odsyłający rozpatruje kwestię wykładni lub ważności określonych przepisów prawa Unii, jak również związku, jaki dostrzega on między tymi przepisami a uregulowaniami krajowymi, które znajdują zastosowanie w postępowaniu głównym" [10].

[7] Wyrok 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", pkt 103).

[8] Zobacz w szczególności wyrok z dnia 28 kwietnia 2016 r., Oniors Bio (C-233/15, EU:C:2016:305, pkt 30).

[9] Trybunał Sprawiedliwości uznał za konieczne zwrócić się do stron o wskazanie, „jakie są, ich zdaniem, istotne przepisy dyrektywy 2016/680, w świetle których Trybunał powinien, w razie potrzeby, przeformułować trzy pytania prejudycjalne przedstawione przez sąd odsyłający" (pytanie czwarte przedstawione do ustnej odpowiedzi na rozprawie).

[10] Wyrok z dnia 6 października 2021 r., Consorzio Italian Management i Catania Multiservizi (C-561/19, EU:C:2021:799, pkt 69).

43. Jak wynika zatem z powyższego, uchybienie wymogom art. 94 regulaminu postępowania jest w niniejszym przypadku oczywiste. Chociaż Trybunał Sprawiedliwości wykazuje w tym zakresie pewną elastyczność, to współpraca z sądem odsyłającym musi być wzajemna: w przypadku nieuzasadnionego braku współpracy ze strony tego ostatniego w zakresie przedstawienia jego wątpliwości w przedmiocie wykładni prawa Unii, które uznaje on za mające zastosowanie (w tym przypadku dyrektywy 2016/680), logiczne wydaje mi się uznanie wniosku o wydanie orzeczenia w trybie prejudycjalnym za niedopuszczalny [11].

44. Do powyższego dochodzi fakt, że sąd ten:

– nie sprecyzował charakteru przetwarzania, planowanego przez organy policji ani faktycznie poszukiwanych danych osobowych. Początkowo zdaje się on wskazywać, że ograniczono się do danych o połączeniach (to jest danych o ruchu i lokalizacji), lecz następnie nie wyklucza, że odblokowanie telefonu miało prowadzić do uzyskania dostępu do „wszystkich danych cyfrowych zapisanych na telefonie komórkowym” [12], a nawet do treści komunikatów i wiadomości elektronicznych wymienianych przez telefon [13];

– dotyczy to zarówno zatrzymania telefonu oraz dostępu lub próby dostępu do zawartych w nim danych, jak i ich późniejszego „wykorzystania” (*Auswertung*), to jest ich analizy i odczytu. To ostatnie, dodaje, „oznacza całkowity i niekontrolowany dostęp do wszystkich cyfrowych komunikatów danej osoby”, co pozwala „odtworzyć bardzo szczegółowy i dogłębny obraz niemal wszystkich obszarów życia prywatnego”.

45. W tych okolicznościach, zamiast *przeformułować* pytania sądu odsyłającego, Trybunał Sprawiedliwości powinien dokonać rzeczywistej *rekonstrukcji* odesłania prejudycjalnego, opartej zresztą częściowo na rozważaniach hipotetycznych, a nie na ustalonych faktach. Wszystko to, powtarzam, po umożliwieniu sądowi odsyłającemu samodzielnego uzupełnienia lub przeformułowania jego własnych pytań.

46. Proponuję zatem, aby wniosek o wydanie orzeczenia w trybie prejudycjalnym został uznany za niedopuszczalny, jak podniosło kilka państw będących interwenientami w sprawie.

47. Do uznania wniosku o wydanie orzeczenia w trybie prejudycjalnym za niedopuszczalny powinna również prowadzić wskazana na rozprawie okoliczność, że przed sądem odsyłającym nie toczy się już rzeczywiste postępowanie, które wymagałoby wykładni przepisów prawa Unii.

48. Rząd austriacki (będący zwierzchnikiem organów policji prowadzących postępowanie przygotowawcze) przyznał bowiem, że działania tych organów były niezgodne z prawem i stanowiły one naruszenie praw skarżącego. Jako że zgodnie z postanowieniem odsyłającym żądanie skarżącego rozpoznawane przez sąd administracyjny skierowane było właśnie przeciwko działaniom organów policji, które to działania organ administracji, będący drugą stroną postępowania, uznał za niezgodne z prawem, nie istnieje już spór przed sądem odsyłającym.

[11] Zgadzam się w tej ocenie z rządem francuskim (pkt 36–41 jego uwag na piśmie).

[12] Tak w drugim pytaniu prejudycjalnym.

[13] Sąd odsyłający stwierdza, że „w odniesieniu do danych dotyczących połączeń można odtworzyć prawie wszystkie kontakty, w zależności od częstotliwości, czasu i okresu trwania połączenia; w odniesieniu do komunikacji za pośrednictwem SMS-ów i innych usług przesyłania wiadomości tekstowych można również odtworzyć ich treść; a analiza przechowywanych fotografii i historii przeglądania stron internetowych dostarcza bardzo intymnej wiedzy o życiu prywatnym osoby, której dane dotyczą”.

49. W każdym razie, na wypadek gdyby Trybunał Sprawiedliwości nie podzielał mojego stanowiska, w dalszej części rozważę, pomocniczo, kwestie merytoryczne leżące u podstaw pytań prejudycjalnych.

50. W pierwszej kolejności wydaje mi się jednak konieczne wykluczenie istnienia innej podstawy niedopuszczalności podnoszonej przez niektórych interwenientów w niniejszym postępowaniu [14]. Ich zdaniem, z tego względu, że dyrektywa 2016/680 dotyczy ochrony osób fizycznych w odniesieniu do *przetwarzania* ich danych, nie ma ona zastosowania w przypadkach takich jak niniejszy, w którym nie miało miejsca przetwarzanie, a jedynie *próba uzyskania dostępu* do danych, których ostatecznie nie uzyskano.

51. Komisja wyraża całkowicie odmienne stanowisko i uważa, że skuteczność dyrektywy 2016/680 powinna sprzyjać takiej wykładni jej przedmiotu, która nie ogranicza się do przetwarzania danych w ścisłym znaczeniu, ale obejmuje również kwestie bezpośrednio z nim związane. Jedną z nich jest próba uzyskania dostępu do danych, które zamierza się przetwarzać [15].

52. Moim zdaniem, bez potrzeby przesuwania granic zakresu zastosowania dyrektywy 2016/680 [16], jej stosowanie w niniejszej sprawie uzasadnia nie fakt zatrzymania telefonu komórkowego [17], lecz późniejsze działania organów policji zmierzające do uzyskania z niego określonych danych osobowych osoby, której dane dotyczą, w którym to celu podjęły one próbę jego odblokowania i umożliwienia dostępu do jego zawartości.

53. Do operacji dokonywanych w toku postępowania przygotowawczego, a objętych zawartą w art. 3 pkt 2 dyrektywy 2016/680 definicją „przetwarzania", zalicza się „innego rodzaju udostępniania" danych osobowych. Uważam, że kiedy organ policji dokonuje zatrzymania telefonu, w którym przechowywane są owe dane, i manipuluje nim w celu ich wydobycia, rozpoczyna „operację" przetwarzania, nawet jeśli zostanie ona udaremniona z przyczyn technicznych dotyczących bezpieczeństwa kryptograficznego.

54. Nieudana próba uzyskania w toku postępowania przygotowawczego dostępu do danych osobowych przechowywanych w telefonie komórkowym jest regulowana dyrektywą 2016/680 z powodów podobnych do tych, które skłoniły Trybunał Sprawiedliwości do uznania, że dyrektywa 2002/58 ma zastosowanie do (również nieudanej) *próby* uzyskania zezwolenia sądu na dostęp do określonych danych osoby, przeciwko której toczy się postępowanie, a które to dane znajdowały się w posiadaniu operatora łączności elektronicznej [18].

[14] Mam na myśli w szczególności rządy austriacki, francuski, niderlandzki i norweski.

[15] Zdaniem Komisji, „nie ma znaczenia, czy próby te były skuteczne, czy nie. Wystąpienie trudności technicznych uniemożliwiających skuteczne próby dostępu jest okolicznością, której nie można przewidzieć z wyprzedzeniem, i która nie ma wpływu na ryzyka związane z ochroną danych osobowych".

[16] Wydaje mi się, w szczególności, że nie ma potrzeby, aby powoływać się na art. 27 i 28 dyrektywy 2016/680, co sugeruje Komisja w swoich uwagach na piśmie. „Ocena skutków dla ochrony danych", o której mowa w art. 27, odnosi się, zasadniczo, do „rodzaju przetwarzania", a nie do konkretnych lub szczególnych czynności przetwarzania. Tak wynika z motywu 58 tej dyrektywy: „Oceny skutków powinny dotyczyć stosownych systemów i procesów związanych z czynnościami przetwarzania danych osobowych, lecz *nie indywidualnych przypadków*" (kursywa moja). Na rozprawie Komisja zawęziła odniesienie do tych dwóch przepisów, które miała przytoczyć jedynie w celu wskazania, że dyrektywa 2016/680 obejmuje również sytuacje poprzedzające faktyczne przetwarzanie danych.

[17] Dyrektywa 2016/680 nie reguluje kwestii zatrzymania telefonu tytułem środka dowodowego w ramach postępowania przygotowawczego.

[18] Wyrok z dnia 2 października 2018 r., Ministerio Fiscal (C-207/16, EU:C:2018:788).

55. W związku z powyższym, gdyby sąd odsyłający miał orzec w przedmiocie niezgodności z prawem czynności dokonanej przez organ policji (co, jak już wskazałem, przyznał rząd austriacki), jego ocena mogłaby być uzależniona od zgodności z prawem zamierzonego celu tej czynności, jak również od tego, czy czynność ta okazała się skuteczna, czy też zaczęto jej dopiero, bezskutecznie, dokonywać.

## *B. Co do istoty*

### *1. Pierwsze pytanie prejudycjalne*

56. Sąd odsyłający zmierza do ustalenia, czy zgodnie z art. 15 ust. 1 dyrektywy 2002/58 (ewentualnie w związku z jej art. 5) oraz w świetle art. 7 i 8 karty, „dostęp organów władzy publicznej do danych zapisanych na telefonach komórkowych stanowi ingerencję w prawa podstawowe opisane w przywołanych postanowieniach karty, która to ingerencja jest na tyle poważna, by pociągnąć za sobą ograniczenie dostępu w kontekście zapobiegania, dochodzenia, wykrywania i ścigania przestępstw do zwalczania poważnej przestępczości".

57. W przypadku dopuszczalności wniosku o wydanie orzeczenia w trybie prejudycjalnym brak możliwości stosowania dyrektywy 2002/58 wymagałby przeformułowania pytania pierwszego w ten sposób, aby odpowiedź Trybunału Sprawiedliwości dotyczyła wykładni dyrektywy 2016/680.

58. Odpowiedź ta powinna z kolei wyjaśnić, czy w przypadkach takich jak w niniejszej sprawie możemy mówić o ingerencji, a jeśli do niej doszło, to czy dyrektywa 2016/680 wymaga, aby dostęp do danych został ograniczony do przypadków zwalczania poważnej przestępczości.

59. Operacje przetwarzania danych z definicji mogą naruszać prawo do poszanowania życia prywatnego (art. 7 karty) i prawo do ochrony danych osobowych (art. 8 karty). Organy publiczne muszą zatem spełniać warunki określone w art. 52 ust. 1 karty, aby uzasadnić swoją ingerencję w wykonywanie tych praw podstawowych.

60. Ingerencja w prawa chronione na podstawie art. 7 i 8 karty będzie tym poważniejsza, że przez nią: a) dąży się do uzyskania dostępu do tych szczególnie chronionych danych, zazwyczaj zapisywanych w telefonach komórkowych, których znajomość może ujawnić różne aspekty życia ich właścicieli, a tym samym powinny one pozostać nieujawnione dla osób trzecich; oraz b) umożliwia się dostęp do treści komunikatów.

61. Z ogólnej perspektywy i w świetle treści dyrektywy 2016/680 nie można zatem interpretować jej w ten sposób, że przetwarzanie danych, których ona dotyczy, ogranicza się jedynie do przypadków zwalczania poważnej przestępczości.

62. Przedmiotem dyrektywy 2016/680 są wszelkie operacje przetwarzania [19] danych osobowych dokonywane przez organy właściwe do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania *wszelkiego rodzaju* czynów zabronionych.

[19] Typologia „operacji" zawarta w art. 3 pkt 2 dyrektywy 2016/680 ma bardzo szeroki zakres. Zobacz jego treść w pkt 9 niniejszej opinii.

63. Z zasad, które ustanowiono w dyrektywie 2016/680 w odniesieniu do przetwarzania danych osobowych w tych celach (art. 4), ani z warunków zgodności z prawem przetwarzania danych osobowych (art. 8) nie wynika, aby przetwarzanie danych osobowych było, co do zasady, możliwe jedynie w przypadku poważnych przestępstw.

64. Ograniczenie sprowadzające się jedynie do przypadków zwalczania poważnych przestępstw nie może również opierać się na zwykłym zastosowaniu orzecznictwa Trybunału Sprawiedliwości dotyczącego dyrektywy 2002/58 [20] do przypadków takich, jak rozpatrywany w niniejszej sprawie.

65. Moim zdaniem nie jest to możliwe, ponieważ – bez uszczerbku dla tego, co wyjaśnię później – orzecznictwo to dotyczy uogólnionego i niezróżnicowanego zatrzymywania danych osobowych rodzajowej i nieokreślonej grupy, dokonywanego systematycznie przez dostawców usług łączności elektronicznej. Skala ingerencji, jaką ten rodzaj zatrzymywania stanowi dla całego społeczeństwa, wyjaśnia, z jakiego powodu Trybunał Sprawiedliwości w sposób szczególnie rygorystyczny podchodził do kwestii zarówno zakazania go, jak i określenia wyjątków od tego zakazu.

66. Inaczej jest w przypadku, w którym zamierzony dostęp nie dotyczy ogółu lub dużych grup ludności (tj. danych osobowych rodzajowej i nieokreślonej grupy), lecz informacji przechowywanych w danym telefonie komórkowym w ramach konkretnego postępowania przygotowawczego, do czego zastosowanie ma w szczególności dyrektywa 2016/680.

67. Przedmiotem dyrektywy 2016/680 jest właśnie przetwarzanie danych osobowych przez organy właściwe do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych. Co dotyczy wszystkich rodzajów czynów zabronionych, a nie jedynie tych o poważnym charakterze.

68. Ponadto, jak wskazali niektórzy interwenienci w postępowaniu prejudycjalnym, wobec braku w dyrektywie 2016/680 jakichkolwiek wskazówek co do powagi czynów zabronionych, dyrektywa ta może nie być stosowana w jednolity sposób w państwach członkowskich, ponieważ oceny co do większej lub mniejszej wagi czynu karalnego, dokonywane z perspektywy każdego krajowego porządku prawnego, istotnie się różnią [21].

69. Podsumowując, w dyrektywie 2016/680 nie wprowadzono, jako warunku zgodności z prawem, obowiązku, aby przetwarzanie regulowanych w niej danych osobowych było możliwe wyłącznie w celu zwalczania poważnej przestępczości.

70. Niemniej jednak przy zastosowaniu zasady proporcjonalności i w poszczególnych przypadkach przetwarzanie danych, którego właściwe organy zamierzają dokonać na podstawie dyrektywy 2016/680, musi być dostosowane do: a) charakteru ściganych czynów zabronionych oraz b) jakości danych osobowych, których dotyczy to przetwarzanie.

71. Zgadzam się w tym sensie z niektórymi twierdzeniami rządu niemieckiego w przedmiocie ograniczenia dostępu do danych pochodzących z telefonów, które zostały zatrzymane, jeżeli dane te pozwalają, w oparciu o zawartość cyfrową telefonu, na ustalenie pełnego profilu osobowości jego posiadacza. Zdaniem rządu niemieckiego dostęp ten powinien zostać ograniczony do

[20] Wyroki: La Quadrature du Net; z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970; zwany dalej „wyrokiem Tele2 Sverige i Watson”); z dnia 2 października 2018 r., Ministerio Fiscal (C-207/16, EU:C:2018:788); z dnia 6 października 2020 r., Privacy International (C-623/17, EU:C:2020:790); a także z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej) (C-746/18, EU:C:2021:152; zwany dalej „wyrokiem Prokuratuur”).

[21] Rząd francuski podaje jako przykład przestępstwa związane z posiadaniem narkotyków i handlu nimi, których waga w ustawodawstwie karnym Austrii i Francji jest odmienna. Rząd szwedzki jest podobnego zdania.

danych, których posiadanie jest konieczne jako środek dowodowy w konkretnej sprawie, lecz nie można uznać go za właściwy w takich przypadkach, jak „znikoma waga przestępstwa będącego przedmiotem postępowania przygotowawczego lub niewielka wartość dowodowa danych, które mają być uzyskane” [22].

72. *Zasadniczo*, z dyrektywy 2016/680 nie wynika zatem, że dostęp do danych osobowych przechowywanych w telefonie komórkowym w celu ułatwienia postępowania przygotowawczego w sprawie czynów mogących wchodzić w zakres kategorii przestępstw zwykłych, czy też pospolitych, jest systematycznie uznawany za niezgodny z prawem. Kwestia, czy *w danej sprawie* można uzyskać taki dostęp, będzie kwestią, którą organ właściwy musi w każdym przypadku ocenić, uwzględniając konieczność uzyskania takiego dostępu oraz kryterium proporcjonalności, do którego właśnie się odniosłem.

73. Można to, moim zdaniem, wywieść z przepisów dyrektywy 2016/680, które określają warunki zgodności z prawem przetwarzania danych osobowych w ramach zwalczania przestępczości:

– art. 4 ust. 1 lit. a), zgodnie z którym dane należy przetwarzać „zgodnie z prawem”;

– art. 8 ust. 1, w którym wskazano, że przetwarzanie musi być *niezbędne* i mieć podstawę w prawie Unii lub państwa członkowskiego.

### *2. Drugie pytanie prejudycjalne*

74. W drugim pytaniu prejudycjalnym sąd odsyłający zmierza do ustalenia, czy art. 15 ust. 1 dyrektywy 2002/58, w związku z art. 7, 8, 11 i art. 52 ust. 1 karty, „stoi […] na przeszkodzie uregulowaniu krajowemu, takiemu jak § 18 w związku z § 99 ust. 1 [StPO], które skutkuje tym, że organy bezpieczeństwa same, w trakcie postępowania karnego, bez zezwolenia sądu lub niezależnego organu administracyjnego zapewniają sobie obszerny i niekontrolowany dostęp do wszystkich danych cyfrowych zapisanych na telefonie komórkowym”.

75. Brzmienie tego pytania nie jest jednoznaczne. Sąd odsyłający:

– przyznaje, że § 110 ust. 2 StPO stanowi, iż zatrzymanie lub zajęcie rzeczy wymaga, co do zasady, zarządzenia prokuratora. Organ policji może dokonać zatrzymania rzeczy bez zarządzenia prokuratora jedynie w nadzwyczajnych okolicznościach przewidzianych w ust. 3 tego paragrafu (które, jak się wydaje, nie występują w niniejszej sprawie);

– jednakże, dodaje on, że dostęp do informacji przechowywanych w telefonach komórkowych „nie został uregulowany [w StPO] w sposób jednoznaczny” oraz, że organy bezpieczeństwa mogą zapewnić go z własnej inicjatywy bez uprzedniego zarządzenia.

76. Rząd austriacki przedstawił treść uregulowania krajowego w wersji, która nie odpowiada jego wersji przedstawionej w postanowieniu odsyłającym. W szczególności podnosi on, że zgodnie z prawem krajowym zarówno zatrzymanie telefonu (z wyjątkiem pilnych przypadków), jak

[22] Uwagi na piśmie rządu niemieckiego, pkt 20.

i dostęp do przechowywanych w nim danych jest możliwy jedynie na podstawie zarządzenia prokuratora [23]. Wykorzystanie przez organy policji danych przechowywanych w telefonie bez nakazu prokuratora jest niezgodne z prawem.

77. Do sądu odsyłającego należy weryfikacja pojęć zawartych w uregulowaniu krajowym. W ramach procedury przewidzianej w art. 267 TFUE Trybunał nie jest właściwy do dokonywania wykładni prawa krajowego, a wyłącznie do sądu odsyłającego należy ustalenie dokładnego zakresu stosowania krajowych przepisów ustawowych, wykonawczych i administracyjnych [24].

78. Nie zamierzam wdawać się w polemikę w przedmiocie wykładni prawa austriackiego, jednak wydaje mi się, że jedynie na podstawie treści przepisów prawa wskazanych przez sąd odsyłający (§ 18 StPO w związku z § 99 ust. 1 tej ustawy) trudno wywieść wniosek, do którego doszedł sąd odsyłający. Powtarzam jednak, że jest to kwestia, którą może rozstrzygnąć tylko ten sąd.

79. W każdym razie sąd odsyłający uważa, że orzecznictwo dotyczące uprzedniej kontroli przez sąd lub niezależny organ dostępu do przechowywanych danych, zawarte w wyroku Prokuratuur [25], może znaleźć zastosowanie w sprawie takiej jak rozpatrywana.

80. Zdaniem rządu niderlandzkiego, przeciwnie, orzecznictwo to należy rozumieć w kontekście uregulowania krajowego, które zezwala właściwym organom na *ogólnie* pojęty dostęp do *wszystkich* przechowywanych danych o ruchu i lokalizacji. Wyjaśniałoby to wymóg uzyskania uprzedniego zezwolenia sądu, który jednak mógłby nie być uzasadniony w przypadku dostępu do danych przechowywanych w konkretnym telefonie komórkowym.

81. Rząd norweski podnosi podobnie, że wśród wielu gwarancji ustanowionych w dyrektywie 2016/680 [26] nie wymieniono wyraźnie gwarancji dotyczącej konieczności uzyskania uprzedniego zezwolenia organu sądowego lub niezależnego organu administracyjnego.

82. Wychodząc z założenia, że przepisy dyrektywy 2016/680 należy interpretować w świetle karty, Komisja podnosi, że obowiązek nałożony na państwa członkowskie w art. 8 ust. 1 tej dyrektywy (warunki zgodności przetwarzania z prawem) wiąże się z koniecznością poszanowania praw podstawowych zagwarantowanych w art. 7 i 8 karty.

83. Zgadzam się z Komisją, że ustawodawcy krajowi są zobowiązani do określenia, przy poszanowaniu przywołanych przepisów karty, niezbędnych zasad w celu zapewnienia, aby dostęp do danych był w każdym przypadku uzasadniony i ograniczał się do tego, co jest ściśle niezbędne i proporcjonalne.

[23] Punkt 19 uwag na piśmie rządu austriackiego. Przytacza on orzeczenie Oberster Gerichtshof (sądu najwyższego, Austria) z dnia 13 października 2020 r. (sprawa 11 Os 56/20z), w którym uznano uzyskanie przez policję kryminalną dostępu do danych znajdujących się w telefonie komórkowym bez zarządzenia prokuratora za niezgodne z prawem, jako stanowiące naruszenie praw podmiotowych osoby, której dane dotyczą.

[24] Zobacz w szczególności wyrok z dnia 28 kwietnia 2022 r., SeGEC i in. (C-277/21, EU:C:2022:318, pkt 21).

[25] Wyrok Prokuratuur, pkt 51: „Ważne jest, aby dostęp właściwych organów państwowych do zatrzymanych danych był 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 karanie przestępstw".

[26] Oprócz gwarancji zawartych w art. 4 i 8 chodzi również o gwarancje zawarte w rozdziałach III („Prawa osoby, której dane dotyczą"), IV („Administrator i podmiot przetwarzający"), VI („Niezależne organy nadzorcze") i VIII („Środki ochrony prawnej, odpowiedzialność prawna i sankcje").

84. Tego rodzaju przepisy prawa krajowego nie muszą jednak dotyczyć wprost dostępu do danych osobowych zawartych, jak w niniejszym przypadku, w telefonie komórkowym, lecz mogą to być przewidziane w prawie krajowym przepisy o charakterze ogólnym dotyczące przeprowadzania dowodów.

85. W tym względzie przytoczyłem już pkt 103 wyroku La Quadrature du Net w odniesieniu do środków państw członkowskich mających wpływ na poufność łączności elektronicznej bez nakładania obowiązku przetwarzania na dostawców takich usług łączności [27].

86. Bez konieczności wywodzenia z dyrektywy 2016/680 *szczegółowych* przepisów o charakterze proceduralnym gwarantujących zgodność z prawem dostępu do danych przechowywanych w telefonie komórkowym [28], będą miały zatem zastosowanie przepisy prawa krajowego regulujące wykonywanie uprawnień do przeszukania i zatrzymania rzeczy w ramach postępowań przygotowawczych w sprawach karnych [29].

87. Odesłanie do przepisów prawa krajowego w celu zapewnienia, w oparciu o dyrektywę 2016/680, zgodności dostępu z prawem jest ponadto zgodne z orzecznictwem ETPC. To właśnie bowiem w sprawie dotyczącej Republiki Austrii w związku z art. 8 EKPC (prawo do poszanowania życia prywatnego i rodzinnego, domu i korespondencji) ETPC stwierdził, że ustawodawstwo austriackie dotyczące zatrzymania przedmiotów, w szczególności dokumentów, ma zastosowanie do przeszukania i zatrzymania danych przechowywanych na nośnikach elektronicznych [30].

88. Jeżeli, jak utrzymuje rząd austriacki, powołując się na orzecznictwo Oberster Gerichtshof (sądu najwyższego, Austria), organy policji nie są uprawnione do dostępu do danych przechowywanych w danym telefonie komórkowym bez zarządzenia prokuratora, drugie pytanie prejudycjalne traci w znacznym stopniu swoje znaczenie.

89. W każdym razie odpowiedź na to pytanie nie wyklucza możliwości, że dostęp do danych osobowych przechowywanych w zatrzymanym telefonie pozwalałby „odtworzyć bardzo szczegółowy i dogłębny obraz niemal wszystkich obszarów życia prywatnego" osoby, której dane dotyczą [31]. Jeśli tak jest, to organy policji nie mogłyby działać bez uprzedniego zezwolenia, o którym mowa w wyroku Prokuratuur.

90. Na pierwszy rzut oka twierdzenie to wydawałoby się sprzeczne z niestosowaniem w niniejszej sprawie dyrektywy 2002/58 (której wykładni dokonano w wyroku Prokuratuur), co uzasadniłem powyżej. Uważam jednak, że uzasadnienie tego wyroku przemawia za takim samym rozwiązaniem.

27 Zobacz pkt 36 niniejszej opinii.

28 Dobrym przykładem trudności tego zadania są starania Komisji w pkt 34–39 jej uwag na piśmie mające na celu przyczynienie się do określenia jasnych i precyzyjnych zasad ustalania granic i odpowiednich zabezpieczeń dostępu do danych z telefonu komórkowego.

29 Przepisy, które – jak wskazują np. rządy duński i irlandzki – znajdują się poza zakresem stosowania prawa Unii, lecz mogą służyć zaspokojeniu wymogu wynikającego z tego prawa.

30 Wyrok ETPC z dnia 16 października 2007 r. w sprawie Wieser I Bicos Beteiligungen przeciwko Austrii (CE:ECHR:2007:1016JUD007433601), § 54: „the Austrian Code of Criminal Procedure does not contain specific provisions for the search and seizure of electronic data. However, it contains detailed provisions for the seizure of objects and, in addition, specific rules for the seizure of documents. It is established in the domestic courts' case-law that these provisions also apply to the search and seizure of electronic data".

31 Zobacz stanowisko sądu odsyłającego przytoczone w pkt 44 niniejszej opinii.

91. W sprawie, w której wydano wyrok Prokuratuur, chociaż dostęp został zrealizowany poprzez uzyskanie danych (metadanych) od dostawców usług łączności elektronicznej, to chodziło, podobnie jak w niniejszej sprawie, o określone postępowania przygotowawcze prowadzone przeciwko określonej osobie. Celem było uzyskanie „danych dotyczących szeregu numerów telefonów […] i różnych międzynarodowych identyfikatorów urządzenia mobilnego” [32].

92. W wyroku Prokuratuur można, moim zdaniem, wyróżnić dwie płaszczyzny: a) dotyczącą zakwestionowania ogólnego uregulowania państwa członkowskiego w przedmiocie uogólnionego i niezróżnicowanego zatrzymywania oraz późniejszego dostępu do danych znajdujących się w posiadaniu dostawców usług oraz b) dotyczącą uprzedniej kontroli w konkretnym przypadku dostępu do takich metadanych, gdy umożliwiają one sporządzenie dokładnego profilu życia prywatnego danej osoby.

93. Okoliczność, że w niniejszej sprawie dane ujawniające życie prywatne nie znajdują się w posiadaniu dostawców usług, lecz mają zostać uzyskane (czy też próbowano je uzyskać) z pojedynczego zatrzymanego telefonu, wydaje mi się mieć drugorzędne znaczenie dla uzasadnienia wymogu kontroli uprzedniej, do którego odnosi się wyrok Prokuratuur.

94. Owa kontrola uprzednia ma swoją ostateczną podstawę w ochronie zagwarantowanej na podstawie art. 7 i 8 karty. Organ, który jej dokonuje, musi być „w stanie zapewnić właściwą równowagę pomiędzy z jednej strony interesami związanymi z potrzebami dochodzenia w ramach zwalczania przestępczości, a z drugiej strony prawami podstawowymi do poszanowania życia prywatnego i ochrony danych osobowych osób, których dane są udostępniane” [33].

### *3. Trzecie pytanie prejudycjalne*

95. W ramach trzeciego pytania prejudycjalnego sąd odsyłający zmierza do ustalenia, czy art. 47 karty (ewentualnie w związku z art. 41 i 52) stoi na przeszkodzie uregulowaniu takiemu jak uregulowanie austriackie [34], które „zezwala na analizę danych cyfrowych z telefonu komórkowego bez uprzedniego poinformowania o tym zainteresowanego, względnie bez poinformowania go przynajmniej po zastosowaniu środka”.

96. Uważam, że tak sformułowane pytanie może być zbędne dla rozstrzygnięcia sporu, ponieważ osoba, której dane dotyczą, mogła wykonać prawo, o którym mowa w art. 47 karty, zwracając się do sądu odsyłającego o stwierdzenie nieważności czynności dokonanej przez organ policji w odniesieniu do zatrzymanego telefonu, która to czynność obejmowała późniejsze (nieudane) wykorzystanie danych przechowywanych w tym telefonie.

97. W odniesieniu do tych dwóch elementów czynności organu policji należy dokonać następującego rozróżnienia:

– w odniesieniu do samej czynności zatrzymania telefonu, z informacji zawartych w aktach sprawy wynika, że osoba, której dane dotyczą, wiedziała o tym zatrzymaniu oraz odmówiła wydania organom policji kodu odblokowującego w momencie zatrzymania;

[32] Wyrok Prokuratuur, pkt 17.

[33] Wyrok Prokuratuur, pkt 52.

[34] Ponownie odnosi się do § 18 StPO w związku z § 99 StPO.

– w odniesieniu do próby analizy danych wszystko wskazuje na to, że administrator nie poinformował osoby, której dane dotyczą, o tej operacji przetwarzania danych, mimo że rząd austriacki twierdzi, że osoba, której dane dotyczą, wiedziała o raporcie, w którym stwierdzono, że policja kryminalna podjęła takie czynności w odniesieniu do jej telefonu [35].

98. Istnieją zatem pewne niejasności co do wykorzystania danych i wiedzy o tym osoby, której dane dotyczą, które – jak już wskazałem – powinny były zostać wyjaśnione przez sąd odsyłający w postanowieniu odsyłającym, a które uniemożliwiają udzielenie użytecznej odpowiedzi na trzecie pytanie prejudycjalne.

99. W każdym razie, na wypadek gdyby Trybunał Sprawiedliwości nie uznał tego pytania za niedopuszczalne, wypowiem się w jego przedmiocie. W zaistniałej sytuacji, biorąc pod uwagę niemożność zastosowania dyrektywy 2002/58, należałoby to pytanie przeformułować w świetle dyrektywy 2016/680, której art. 13, 15 i 54 dostarczają wskazówek w celu udzielenia na nie odpowiedzi.

100. Zgodnie z dyrektywą 2016/680 informacjami na temat przetwarzania danych osobowych, jakie należy udostępnić osobie, której dane dotyczą, są między innymi informacje dotyczące: a) wniesienie skargi do organu nadzorczego [art. 13 ust. 1 lit. d)] oraz b) uzyskanie skutecznego środka prawnego przed sądem w przypadku naruszenia praw zagwarantowanych dyrektywą 2016/680, bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej (art. 54).

101. Nie można jednak zapominać, że zarówno art. 13 ust. 3, jak i art. 15 ust. 1 dyrektywy 2016/680 upoważniają państwa członkowskie do przyjęcia aktów prawnych pozwalających:

– opóźnić, ograniczyć lub zaniechać udostępniania informacji osobie, której dane dotyczą, zgodnie z art. 13 ust. 2;

– ograniczyć w całości lub w części prawo dostępu osoby, której dane dotyczą, do przetwarzanych danych, pod warunkiem że takie ograniczenie stanowi niezbędny i proporcjonalny środek w celu, *między innymi*, uniknięcia utrudniania dochodzeń lub postępowań urzędowych lub sądowych, bądź utrudniania postępowań w sprawie przestępstw karnych [36].

102. W każdym razie zgodność przetwarzania danych osobowych z prawem nie jest uzależniona od wypełnienia przez właściwe organy (dalszych) obowiązków nałożonych na nie w art. 13 dyrektywy 2016/680, lecz od zgodności z prawem celu, w jakim zostało ono dokonane, to jest od tego, czy organy administracji były uprawnione do przetwarzania danych osobowych.

103. W tym kontekście okoliczność, że osoba, której dane dotyczą, została poinformowana o próbach uzyskania dostępu do danych przechowywanych w zatrzymanym telefonie, sama w sobie pozostaje bez związku z materialną zgodnością z prawem danej czynności organów policji. Zachowanie administratora danych, które może być sprzeczne z obowiązkami nałożonymi na niego w art. 13 dyrektywy 2016/680, może wywoływać inne konsekwencje, lecz – powtarzam – samo w sobie nie wpływa na zgodność lub niezgodność z prawem danej operacji przetwarzania.

[35] Punkt 37 jego uwag na piśmie.

[36] Zobacz podobnie wyrok Tele2 Sverige i Watson, pkt 121. Zawarte w nim stanowisko dotyczące dyrektywy 2002/58 można zastosować do dyrektywy 2016/680 w kontekście zapewnienia środka prawnego w zakresie ochrony praw osób, których dane są przetwarzane.

104. Do sądu odsyłającego należy ustalenie, czy uregulowanie krajowe umożliwia skuteczne wykonywanie tych praw przez osobę, której dane dotyczą.

## V. Wnioski

105. W świetle powyższego proponuję, aby Trybunał Sprawiedliwości uznał za niedopuszczalny wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Landesverwaltungsgericht Tirol (regionalny sąd administracyjny w Tyrolu, Austria).

Ewentualnie, proponuję, aby odpowiedział na ten wniosek następująco:

1) Artykuł 4 ust. 1 lit. a) i art. 8 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. 7, 8 i 52 Karty praw podstawowych Unii Europejskiej

   należy interpretować w ten sposób, że

   dostęp organów publicznych do danych osobowych przechowywanych w telefonie komórkowym w celu ich przetwarzania w ramach postępowania przygotowawczego nie jest ograniczony do przypadków zwalczania poważnej przestępczości.

   Dostęp taki musi być w każdym przypadku uzasadniony i ograniczony do tego, co ściśle niezbędne i proporcjonalne w zależności od charakteru ściganych czynów zabronionych oraz danych osobowych, do których ma być uzyskany dostęp.

   W ramach postępowania przygotowawczego organy policji nie mogą samodzielnie, bez uprzedniego zezwolenia organu sądowego, uzyskać pełnego i niekontrolowanego dostępu do wszystkich danych przechowywanych w telefonie komórkowym, jeżeli na podstawie tych danych można uzyskać dokładny obraz życia prywatnego danej osoby.

2) Artykuły 13, 15 i 54 dyrektywy 2016/680 w związku z art. 47 i 52 karty

   należy interpretować w ten sposób, że

   bez uszczerbku dla ograniczeń dozwolonych na mocy art. 15 ust. 1 dyrektywy 2016/680 lub innych dostępnych administracyjnych lub pozasądowych środków prawnych, właściciel telefonu komórkowego powinien zostać poinformowany o przetwarzaniu danych osobowych przechowywanych w telefonie komórkowym przez właściwe organy w takim czasie i na takich warunkach, jakie mogą być niezbędne do zapewnienia mu skutecznego wykonania jego prawa do środka prawnego w przypadku ewentualnego naruszenia praw przyznanych dyrektywą 2016/680.