



Zbiór Orzeczeń

WYROK TRYBUNAŁU (wielka izba)

z dnia 4 października 2024 r. *

Odesłanie prejudycjalne – Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych – Dyrektywa (UE) 2016/680 – Artykuł 3 pkt 2 – Pojęcie „przetwarzania” – Artykuł 4 – Zasady dotyczące przetwarzania danych osobowych – Artykuł 4 ust. 1 lit. c) – Zasada „minimalizacji danych” – Artykuły 7, 8, 47 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej – Wymóg, zgodnie z którym wszelkie ograniczenia w korzystaniu z praw podstawowych muszą być „przewidziane ustawą” – Proporcjonalność – Ocena proporcjonalności w świetle wszystkich istotnych okoliczności – Uprzednia kontrola sądowa lub niezależnego organu administracyjnego – Artykuł 13 – Informacje udostępniane lub przekazywane osobie, której dane dotyczą – Granice – Artykuł 54 – Prawo do skutecznego środka prawnego przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu – Postępowanie przygotowawcze w sprawie handlu środkami odurzającymi – Próba odblokowania telefonu komórkowego przez organy policyjne w celu uzyskania wglądu do zapisanych w tym telefonie danych na potrzeby tego postępowania

W sprawie C-548/21

mającej za przedmiot wniosek o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożony przez Landesverwaltungsgericht Tirol (regionalny sąd administracyjny w Tyrolu, Austria) postanowieniem z dnia 1 września 2021 r., które wpłynęło do Trybunału w dniu 6 września 2021 r., w postępowaniu:

CG

przeciwko

Bezirkshauptmannschaft Landeck,

TRYBUNAŁ (wielka izba),

w składzie: K. Lenaerts, prezes, L. Bay Larsen, wiceprezes, K. Jürimäe, C. Lycourgos, E. Regan, T. von Danwitz, Z. Csehi i O. Spineanu-Matei, prezesi izb, P.G. Xuereb (sprawozdawca), I. Jarukaitis, A. Kumin, N. Jääskinen i M. Gavalec, sędziowie,

rzecznik generalny: M. Campos Sánchez-Bordona,

sekretarz: C. Di Bella, administrator,

* Język postępowania: niemiecki.

uwzględniając pisemny etap postępowania i po przeprowadzeniu rozprawy w dniu 16 stycznia 2023 r.,

rozważywszy uwagi, które przedstawili:

- w imieniu rządu austriackiego – A. Posch, J. Schmoll, K. Ibili i E. Riedl, w charakterze pełnomocników,
- w imieniu rządu duńskiego – M.P.B. Jespersen, V. Pasternak Jørgensen, M. Søndahl Wolff i Y.T. Thyregod Kollberg, w charakterze pełnomocników,
- w imieniu rządu niemieckiego – J. Möller i M. Hellmann, w charakterze pełnomocników,
- w imieniu rządu estońskiego – M. Kriisa, w charakterze pełnomocnika,
- w imieniu Irlandii – M. Browne, Chief State Solicitor, A. Joyce i M. Lane, w charakterze pełnomocników, których wspierali R. Farrell, SC, D. Fennelly, BL, i D. O'Reilly, solicitor,
- w imieniu rządu francuskiego – R. Bénard, A. Daniel, A.-L. Desjonquères i J. Illouz, w charakterze pełnomocników,
- w imieniu rządu cypryjskiego – I. Neophytou, w charakterze pełnomocnika,
- w imieniu rządu węgierskiego – Z. Biró-Tóth i M.Z. Fehér, w charakterze pełnomocników,
- w imieniu rządu niderlandzkiego – M.K. Bulterman, A. Hanje i J. Langer, w charakterze pełnomocników,
- w imieniu rządu polskiego – B. Majczyna, w charakterze pełnomocnika,
- w imieniu rządu fińskiego – A. Laine, w charakterze pełnomocnika,
- w imieniu rządu szwedzkiego – J. Lundberg, H. Eklinder, C. Meyer-Seitz, A.M. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson, H. Shev i O. Simonsson, w charakterze pełnomocników,
- w imieniu rządu norweskiego – F. Bergsjø, H. Busch, K. Moe Winther i P. Wennerås, w charakterze pełnomocników,
- w imieniu Komisji Europejskiej – G. Braun, S.L. Kalèda, H. Kranenborg i F. Wilman, w charakterze pełnomocników,

po zapoznaniu się z opinią rzecznika generalnego na posiedzeniu w dniu 20 kwietnia 2023 r.,

wydaje następujący

Wyrok

- 1 Wniosek o wydanie orzeczenia w trybie prejudycjalnym dotyczy wykładni art. 5 i art. 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywy o prywatności i łączności elektronicznej) (Dz.U. 2002, L 201, s. 37; sprostowania: Dz.U. 2013, L 241, s. 9; Dz.U. 2017, L 162, s. 56), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. (Dz.U. 2009, L 337, s. 11) (zwanej dalej „dyrektywą 2002/58”), w związku z art. 7, 8, 11, 41, 47 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „Kartą”).
- 2 Wniosek ten został złożony w ramach sporu pomiędzy CG a Bezirkshauptmannschaft Landeck (organem administracji publicznej okręgu Landeck, Austria) w przedmiocie zatrzymania przez organy policyjne telefonu komórkowego CG i podjętych przez te organy prób odblokowania telefonu komórkowego w celu uzyskania wglądu do zapisanych w nim danych w ramach postępowania przygotowawczego w sprawie handlu środkami odurzającymi.

Ramy prawne

Prawo Unii

Dyrektywa 2002/58

- 3 Artykuł 1 dyrektywy 2002/58, zatytułowany „Zakres i cel”, stanowi:

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

[...]
3. Niniejsza dyrektywa nie ma zastosowania do działalności, która wykracza poza zakres [traktatu FUE], takiej jak działalność określona w tytułach V i VI [traktatu UE], 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”.
- 4 Artykuł 3 tej dyrektywy, zatytułowany „Usługi”, przewiduje:

„Niniejsza dyrektywa ma zastosowanie do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności we Wspólnocie, włącznie z publicznymi sieciami łączności służącymi do zbierania danych i obsługi urządzeń identyfikacyjnych”.

- 5 Artykuł 5 tej dyrektywy, zatytułowany „Poufność komunikacji”, stanowi w ust. 1:

„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 omawianej dyrektywy, zatytułowany „Stosowanie niektórych przepisów dyrektywy 95/46/WE”, głosi w ust. 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 [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)]. W tym celu, państwa członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 [TUE]”.

Dyrektywa (UE) 2016/680

- 7 Motywy 2, 4, 7, 10, 11, 15, 26, 37, 44, 46 i 104 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 uchyłającej decyzję ramową Rady 2008/977/WSiSW (Dz.U. 2016, L 119, s. 89; sprostowanie: Dz.U. 2018, L 127, s. 10) głoszą:

„(2) Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych powinny – niezależnie od ich obywatelstwa czy miejsca zamieszkania – przestrzegać ich podstawowych praw i wolności, zwłaszcza prawa do ochrony danych osobowych. Niniejsza dyrektywa ma przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

[...]

(4) Należy ułatwić swobodny przepływ danych osobowych między właściwymi organami do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom na terytorium Unii oraz przekazywania takich danych osobowych do państw trzecich

i organizacji międzynarodowych, zapewniając przy tym wysoki stopień ochrony danych osobowych. Przemiany te wymagają stworzenia stabilnych i spójniejszych ram dla ochrony danych osobowych w Unii oraz zdecydowanego egzekwowania ich przepisów.

[...]

- (7) Zapewnienie spójnego, wysokiego stopnia ochrony danych osobowych osób fizycznych oraz ułatwienie wymiany danych osobowych między właściwymi organami państw członkowskich ma zasadnicze znaczenie dla zapewnienia skutecznej współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. W tym celu należy we wszystkich państwach członkowskich zapewnić równorzędny stopień ochrony praw i wolności 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 do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Aby ochrona danych osobowych w Unii była skuteczna, należy wzmocnić prawa osób, których dane dotyczą, oraz obowiązki podmiotów, które przetwarzają dane osobowe, jak i odpowiadające im uprawnienia w zakresie monitorowania i egzekwowania przepisów o ochronie danych osobowych w państwach członkowskich.

[...]

- (10) W deklaracji nr 21 w sprawie ochrony danych osobowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej – załączonej do Aktu końcowego konferencji międzyrządowej, która przyjęła Traktat z Lizbony – konferencja uznała, że ze względu na szczególny charakter współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej konieczne może okazać się przyjęcie – na podstawie art. 16 TFUE – szczególnych przepisów o ochronie danych osobowych i swobodnym przepływie danych osobowych w tych dziedzinach.
- (11) Należy zatem odnieść się do tych dziedzin w odrębnej dyrektywie, która stanowi szczególne 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 do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, z zachowaniem szczególnego charakteru takich czynności. Do takich właściwych organów mogą należeć nie tylko organy publiczne – takie jak organy sądowe, policja lub inne organy ścigania – ale też wszelkie inne organy lub podmioty, którym prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów niniejszej dyrektywy. Jeżeli taki organ lub podmiot przetwarza dane osobowe do celów innych niż cele niniejszej dyrektywy, zastosowanie ma rozporządzenie [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 (ogólne rozporządzenie o ochronie danych)] (Dz.U. 2016, L 119, s. 1; sprostowania: Dz.U. 2018, L 127, s. 2; Dz.U. 2021, L 74, s. 35]. Rozporządzenie [2016/679] ma zatem zastosowanie wtedy, gdy organ lub podmiot zbiera dane osobowe do innych celów, a następnie dalej te dane przetwarza w celu realizacji obowiązku prawnego, któremu podlega. [...]

[...]

- (15) Aby zapewnić jednakowy stopień ochrony osób fizycznych poprzez prawnie wykonalne prawa obowiązujące w całej Unii oraz aby zapobiec różnicom utrudniającym wymianę danych osobowych między właściwymi organami, niniejsza dyrektywa powinna przewidywać zharmonizowane zasady ochrony i swobodnego przepływu danych osobowych przetwarzanych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Zbliżenie przepisów państw członkowskich nie powinno skutkować osłabieniem gwarantowanej przez nie ochrony danych osobowych, a wręcz przeciwnie – powinno służyć zapewnieniu wysokiego stopnia ochrony w całej Unii. Państwa członkowskie powinny także móc ustanawiać gwarancje wyższe od przewidzianych w niniejszej dyrektywie dla ochrony praw i wolności osoby, której dane dotyczą, w związku z przetwarzaniem danych osobowych przez właściwe organy.

[...]

- (26) [...] Dane osobowe powinny być adekwatne i właściwe w stosunku do celów przetwarzania. Należy w szczególności zapewnić, by zebrane dane osobowe nie były nadmierne i by okres ich przechowywania był nie dłuższy, niż jest to niezbędne do osiągnięcia celu ich przetwarzania. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. [...]

[...]

- (37) Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko naruszenia podstawowych praw i wolności. Do takich danych osobowych powinny zaliczać się dane osobowe ujawniające pochodzenie rasowe lub etniczne, przy czym użycie w niniejszej dyrektywie terminu »pochodzenie rasowe« nie oznacza, że Unia akceptuje teorie sugerujące istnienie osobnych ras ludzkich. Takich danych nie należy przetwarzać, chyba że przetwarzanie podlega odpowiednim, określonym prawem gwarancjom praw i wolności osoby, której dane dotyczą, i jest dozwolone w przypadkach dopuszczonych prawem, a jeżeli nie jest dotąd dopuszczone takim prawem – jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, albo też dotyczy danych w sposób oczywisty upublicznionych przez samą osobę, której dane dotyczą. Odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą, mogą obejmować możliwość zbierania takich danych tylko w połączeniu z innymi danymi dotyczącymi danej osoby fizycznej, możliwość odpowiedniego zabezpieczenia takich danych, ściślejsze uregulowanie dostępu pracowników właściwego organu do danych lub zakaz przesyłania danych. Przetwarzanie takich danych powinno być także dozwolone prawem, gdy osoba, której dane dotyczą, udzieliła wyraźnej zgody na szczególnie dla niej inwazyjne przetwarzanie. Niemniej sama zgoda osoby, której dane dotyczą, nie powinna stanowić podstawy prawnej przetwarzania takich wrażliwych danych osobowych przez właściwe organy.

[...]

- (44) Państwa członkowskie powinny mieć możliwość przyjmowania aktów prawnych pozwalających opóźnić, ograniczyć lub pominąć informowanie osób, których dane dotyczą, lub ograniczyć, w całości lub w części, dostęp tych osób do ich własnych danych osobowych w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym – przy należyтым uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej – tak aby uniemożliwić zakłócanie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub czynności procesowych, aby uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, aby chronić bezpieczeństwo publiczne lub narodowe lub aby chronić prawa i wolności innych osób. Administrator powinien dokonywać oceny – badając konkretnie i indywidualnie każdy przypadek – czy prawo dostępu powinno zostać częściowo lub całkowicie ograniczone.

[...]

- (46) Każde ograniczenie praw osoby, której dane dotyczą, musi być zgodne z Kartą i [europejską Konwencją o ochronie praw człowieka i podstawowych wolności, podpisaną w Rzymie dnia 4 listopada 1950 r.], w myśl wykładni zawartej, odpowiednio, w orzecznictwie Trybunału Sprawiedliwości [Unii Europejskiej] i Europejskiego Trybunału Praw Człowieka, a zwłaszcza musi odbywać się z poszanowaniem istoty tych praw i wolności.

[...]

- (104) Niniejsza dyrektywa nie narusza praw podstawowych i jest zgodna z zasadami uznanymi w Karcie umocowanej [traktacie FUE], w szczególności z prawem do poszanowania życia prywatnego i rodzinnego, prawem do ochrony danych osobowych oraz prawem do skutecznego środka prawnego i do rzetelnego procesu. Ograniczenia tych praw są zgodne z art. 52 ust. 1 Karty, ponieważ są niezbędne do realizacji celów leżących w interesie ogólnym i uznanych przez Unię lub do ochrony praw i wolności innych osób”.

8 Artykuł 1 tej dyrektywy, zatytułowany „Przedmiot i cele”, stanowi w ust. 1 i 2:

„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
- b) zapewniają, by wymiana danych osobowych przez właściwe organy w Unii, jeżeli wynika z prawa Unii lub prawa krajowego, nie była ograniczana ani zakazywana z powodów dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych”.

9 Artykuł 2 tej dyrektywy, zatytułowany „Zakres zastosowania”, stanowi w ust. 1 i 3:

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

[...]

3. Niniejsza dyrektywa nie ma zastosowania do przetwarzania danych osobowych:

a) w ramach działalności nieobjętej zakresem prawa Unii;

[...]”.

10 Zgodnie z art. 3 tej dyrektywy, zatytułowanym „Definicje”:

„Na użytek niniejszej dyrektywy:

1) »dane osobowe« oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (»osobie, której dane dotyczą«); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy bądź jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

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

b) inny organ lub podmiot, któremu prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych 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 4 dyrektywy 2016/680, zatytułowany „Zasady dotyczące przetwarzania danych osobowych”, stanowi w ust. 1:

„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;

[...]”.

- 12 Artykuł 6 tej dyrektywy, zatytułowany „Rozróżnianie poszczególnych kategorii osób, których dane dotyczą”, stanowi:

„Państwa członkowskie zapewniają, by administrator – w stosownym przypadku i w miarę możliwości – wyraźnie rozróżniał dane osobowe poszczególnych kategorii osób, których dane dotyczą, takich jak:

- a) osoby, w stosunku do których istnieją poważne podstawy, by przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony;
- b) osoby skazane za czyn zabroniony;
- c) pokrzywdzeni czynem zabronionym lub osoby, w przypadku których określone fakty wskazują, że mogą stać się ofiarą czynu zabronionego; oraz
- d) osoby inne w stosunku do czynu zabronionego, takie jak osoby, które mogą zostać wezwane do złożenia zeznań w ramach postępowania przygotowawczego w sprawie czynu zabronionego lub na dalszych etapach postępowania karnego, osoby, które mogą dostarczyć informacji o czynach zabronionych, lub osoby, które mają kontakty lub powiązania z jedną z osób, o których mowa w lit. a) i b)”.

- 13 Artykuł 10 wspomnianej dyrektywy, zatytułowany „Przetwarzanie szczególnych kategorii danych osobowych”, ma następujące brzmienie:

„Przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe lub przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia lub danych dotyczących seksualności i orientacji seksualnej osoby fizycznej jest dozwolone wyłącznie wtedy, jeżeli jest bezwzględnie niezbędne, podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, oraz:

- a) jest dopuszczone prawem Unii lub prawem państwa członkowskiego;
- b) jest niezbędne dla ochrony żywotnych interesów osoby fizycznej, której dane dotyczą, lub innej osoby; lub

- c) takie przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą”.
- 14 Artykuł 13 dyrektywy 2016/680, zatytułowany „Informacje udostępniane lub przekazywane osobie, której dane dotyczą”, stanowi:
- „1. Państwa członkowskie zapewniają, by administrator udostępniał osobie, której dane dotyczą, przynajmniej następujące informacje:
- a) tożsamość i dane kontaktowe administratora;
 - b) dane kontaktowe inspektora ochrony danych, w razie potrzeby;
 - c) cele przetwarzania, do których mają posłużyć dane osobowe;
 - d) informacje o prawie do wniesienia skargi do organu nadzorczego oraz dane kontaktowe organu nadzorczego;
 - e) informacje o prawie żądania od administratora dostępu do danych osobowych, sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych odnoszącego się do osoby, której dane dotyczą.
2. Państwa członkowskie zapewniają, by oprócz informacji, o których mowa w ust. 1, w konkretnych przypadkach administrator przekazywał osobie, której dane dotyczą, następujące dalsze informacje umożliwiające wykonywanie przysługujących jej praw:
- a) podstawa prawna przetwarzania;
 - b) okres przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteria służące określeniu tego okresu;
 - c) w stosownym przypadku kategorie odbiorców danych osobowych, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
 - d) w razie potrzeby dalsze informacje, zwłaszcza gdy dane osobowe są zbierane bez wiedzy osoby, której dane dotyczą.
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 należyтым 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.

[...]”.

- 15 Artykuł 54 tej dyrektywy, zatytułowany „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”.

Prawo austriackie

- 16 Paragraf 27 ust. 1 Suchtmittelgesetz (ustawy o środkach odurzających) z dnia 5 września 1997 r. (BGBl. I, 112/1997), w brzmieniu mającym zastosowanie do sporu w postępowaniu głównym, stanowi:

„Kto niezgodnie z prawem

1. Nabywa, posiada, wytwarza, przewozi, przywozi, wywozi lub oferuje, przekazuje lub dostarcza środki odurzające innej osobie,

[...]

podlega karze pozbawienia wolności do roku lub karze grzywny do wysokości 360 stawek dziennych.

[...]”.

- 17 Paragraf 17 Strafgesetzbuch (kodeksu karnego) z dnia 1 stycznia 1975 r. (BGBl., 60/1974), w brzmieniu mającym zastosowanie do sporu w postępowaniu głównym (zwanego dalej „StGB”), głosi:

„(1) Zbrodnią jest czyn umyślny zagrożony karą dożywotniego pozbawienia wolności lub karą pozbawienia wolności na czas nie krótszy od trzech lat.

(2) Wszystkie pozostałe przestępstwa są występками”.

- 18 Paragraf 18 Strafgesetzbuch (kodeksu postępowania karnego) z dnia 30 grudnia 1975 r. (BGBl., 631/1975), w brzmieniu mającym zastosowanie do sporu w postępowaniu głównym (zwanego dalej „StPO”), przewiduje:

„(1) Policja kryminalna wykonuje zadania w służbie wymiaru sprawiedliwości w sprawach karnych (§ 10 ust. 1 pkt 6 Bundes-Verfassungsgesetz) [(federalnej ustawy konstytucyjnej)].

(2) Postępowania przygotowawcze prowadzone przez policję kryminalną należą do obowiązków organów bezpieczeństwa, których organizacja i właściwość miejscowa są regulowane przepisami Sicherheitspolizeigesetzes [(ustawy o policji bezpieczeństwa)] regulującej ustrój administracji bezpieczeństwa publicznego.

(3) Organy służby bezpieczeństwa publicznego (§ 5 ust. 2 Sicherheitspolizeigesetz) [(ustawy o policji bezpieczeństwa)] prowadzą czynności wykonawcze policji kryminalnej obejmujące prowadzenie postępowania przygotowawczego i ściganie przestępstw zgodnie z przepisami niniejszej ustawy.

[...]”.

19 Paragraf 99 ust. 1 StPO stanowi:

„Policja kryminalna prowadzi postępowanie przygotowawcze z urzędu lub na podstawie zawiadomienia pod nadzorem prokuratora i sądu (§ 105 ust. 2)”.

Postępowanie główne i pytania prejudycjalne

- 20 W dniu 23 lutego 2021 r., podczas kontroli na obecność narkotyków, urzędnicy urzędu celnego w Innsbrucku (Austria) przejęli adresowaną do CG paczkę, która zawierała 85 gramów marihuany. Przesyłka została przekazana do zbadania Centralnemu Komisariatowi Policji w St. Anton am Arlberg (Austria).
- 21 W dniu 6 marca 2021 r. dwaj funkcjonariusze policji tego komisariatu dokonali przeszukania miejsca zamieszkania CG, w trakcie którego przesłuchali go na okoliczność nadawcy wspomnianej przesyłki oraz przeszukali jego mieszkanie. W trakcie tego przeszukania funkcjonariusze policji zażądali wglądu do danych dotyczących połączeń zapisanych w telefonie komórkowym CG. Wobec odmowy funkcjonariusze policji zatrzymali jego telefon komórkowy wraz z kartą SIM i kartą SD oraz wręczyli CG protokół zatrzymania przedmiotów.
- 22 Wspomniany telefon komórkowy został następnie przekazany do laboratorium kryminalistycznego posterunku policji okręgu Landeck (Austria) w celu jego odblokowania. Ponieważ próba odblokowania telefonu komórkowego zakończyła się niepowodzeniem, telefon został wysłany do Bundeskriminalamt (głównego urzędu policji kryminalnej) w Wiedniu (Austria), gdzie ponownie podjęto próbę jego odblokowania.
- 23 Zatrzymanie telefonu komórkowego CG oraz późniejsze próby jego wykorzystania zostały podjęte z inicjatywy funkcjonariuszy policji, bez uprzedniego uzyskania przez nich zgody prokuratora lub sądu.
- 24 W dniu 31 marca 2021 r. CG wniósł do Landesverwaltungsgericht Tirol (regionalnego sądu administracyjnego w Tyrolu, Austria), będącego sądem odsyłającym, zażalenie, w którym zakwestionował zgodność z prawem zatrzymania jego telefonu komórkowego. Telefon został zwrócony CG w dniu 20 kwietnia 2021 r.
- 25 CG nie został od razu powiadomiony o próbach wykorzystania z jego telefonu komórkowego. Dowiedział się o tym dopiero po przesłuchaniu w ramach postępowania toczącego się przed sądem odsyłającym funkcjonariusza policji, który zatrzymał jego telefon komórkowy, a następnie

podjął próbę uzyskania wglądu do zapisanych na nim danych cyfrowych, w charakterze świadka. Próba ta nie została również odnotowana w aktach sprawy prowadzonych przez policję kryminalną.

- 26 Wobec tych okoliczności sąd odsyłający zastanawia się w pierwszej kolejności, czy w świetle pkt 52–61 wyroku z dnia 2 października 2018 r., *Ministerio Fiscal* (C-207/16, EU:C:2018:788), i orzecznictwa przytoczonego w tych punktach art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7 i 8 Karty należy interpretować w ten sposób, że pełny i niekontrolowany wgląd do wszystkich danych zapisanych w telefonie komórkowym, w tym danych dotyczących połączeń, treści komunikatów, zdjęć i historii przeglądanych stron internetowych, na podstawie których można uzyskać bardzo dokładny i szczegółowy obraz prawie wszystkich aspektów życia prywatnego osoby, której dane dotyczą, stanowią na tyle poważną ingerencję w prawa podstawowe zagwarantowane w art. 7 i 8 Karty, że w kontekście zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępstw wgląd ten powinien być ograniczony tylko do przypadków zwalczania poważnej przestępczości.
- 27 W tym względzie sąd ten wyjaśnia, że przestępstwo zarzucane CG w ramach postępowania przygotowawczego rozpatrywanego w postępowaniu głównym jest przewidziane w § 27 ust. 1 ustawy o środkach odurzających i zagrożone karą pozbawienia wolności do jednego roku, przy czym w świetle kwalifikacji zawartej w § 17 StGB stanowi ono jedynie występpek.
- 28 W drugiej kolejności, po przypomnieniu wniosków płynących z pkt 48–54 wyroku z dnia 2 marca 2021 r., *Prokuratuur* (Warunki dostępu do danych dotyczących łączności elektronicznej) (C-746/18, EU:C:2021:152), a także z przytoczonego w tych punktach orzecznictwa, wspomniany sąd zastanawia się, czy art. 15 ust. 1 dyrektywy 2002/58 stoi na przeszkodzie uregulowaniu krajowemu takiemu jak to zawarte w § 18 StPO w związku z § 99 ust. 1 StPO, zgodnie z którym w toku postępowania przygotowawczego policja kryminalna może uzyskać, bez zgody sędziego lub niezależnego organu administracyjnego, pełny i niekontrolowany wgląd do wszystkich danych cyfrowych zapisanych w telefonie komórkowym.
- 29 W trzeciej i ostatniej kolejności, podkreśliwszy, że § 18 StPO w związku z § 99 ust. 1 StPO nie nakłada na organy policyjne obowiązku udokumentowania podjętych czynności cyfrowego wykorzystania telefonu komórkowego ani powiadomienia jego właściciela o takich czynnościach, tak aby mógł on w stosownym wypadku sprzeciwić się temu w drodze prewencyjnej lub następczej kontroli sądowej, sąd odsyłający zastanawia się nad zgodnością tych przepisów StPO z zasadą równości stron procesowych i z prawem do skutecznego środka prawnego w rozumieniu art. 47 Karty.
- 30 W tych okolicznościach Landesverwaltungsgericht Tirol (regionalny sąd administracyjny w Tyrolu) postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:
„1) Czy art. 15 ust. 1 (ewentualnie w związku z art. 5) dyrektywy [2002/58] w świetle art. 7 i 8 [Karty] 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 świetle art. 7, 8 i 11 oraz art. 52 ust. 1 [Karty] 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 [krajowe] 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 [Karty] 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?”.

Postępowanie przed Trybunałem

- 31 W dniu 20 października 2021 r. Trybunał zwrócił się do sądu odsyłającego z wnioskiem o udzielenie informacji, w którym zwrócił się do tego sądu o wskazanie, czy dyrektywa 2016/680 może mieć znaczenie dla sprawy w postępowaniu głównym, oraz ewentualnie o przedstawienie mu przepisów prawa krajowego transponujących tę dyrektywę, które mogłyby mieć zastosowanie w niniejszej sprawie.
- 32 W dniu 11 listopada 2021 r. sąd odsyłający odpowiedział na ten wniosek, stwierdzając w szczególności, że w niniejszej sprawie należy przestrzegać wymogów wspomnianej dyrektywy. Odpowiedź ta została doręczona wraz z postanowieniem odsyłającym zainteresowanym stronom, o których mowa w art. 23 statutu Trybunału Sprawiedliwości Unii Europejskiej.
- 33 W dniu 8 listopada 2022 r. na podstawie art. 61 regulaminu postępowania przed Trybunałem Trybunał wezwał uczestników ustnego etapu postępowania do skoncentrowania się w swoich wystąpieniach na dyrektywie 2016/680 i do udzielenia na rozprawie odpowiedzi na niektóre pytania dotyczące tej dyrektywy.

W przedmiocie wniosku o otwarcie ustnego etapu postępowania na nowo

- 34 Po przedstawieniu opinii rzecznika generalnego pismem złożonym w sekretariacie Trybunału w dniu 17 maja 2023 r. rząd austriacki złożył wniosek o sprostowanie tej opinii, twierdząc, że błędnie przedstawiono w niej jego stanowisko wyrażone w jego uwagach na piśmie i uwagach ustnych oraz że zawiera ona błędy w ustaleniach faktycznych.
- 35 Zdaniem tego rządu, po pierwsze, pkt 50 opinii rzecznika generalnego w związku z przypisem 14 do tej opinii sugeruje bowiem, że zdaniem tego rządu próba uzyskania wglądu do danych zapisanych w telefonie komórkowym, taka jak rozpatrywana w postępowaniu głównym, nie może stanowić przetwarzania danych osobowych w rozumieniu art. 3 pkt 2 dyrektywy 2016/680. Jednakże na rozprawie przed Trybunałem rząd ten twierdził coś przeciwnego, wyraźnie popierając wyrażone przez Komisję Europejską w jej uwagach na piśmie stanowisko, zgodnie z którym z wykładni systemowej tej dyrektywy, interpretowanej w świetle jej celów, wynika, że reguluje ona nie tylko przetwarzanie w ścisłym znaczeniu tego pojęcia, lecz również czynności dokonywane na wcześniejszym etapie przetwarzania, takie jak próba dokonania przetwarzania, przy czym stosowanie wspomnianej dyrektywy nie jest obwarowane warunkiem, że ta próba przetwarzania zakończyła się sukcesem.

- 36 Po drugie, rząd austriacki podnosi, że pkt 27 opinii rzecznika generalnego opiera się na błędnych ustaleniach faktycznych, ponieważ sugeruje, że wskazane w pkt 22 niniejszego wyroku próby przetwarzania nie zostały udokumentowane w aktach policji kryminalnej. W tym względzie rząd ten wyjaśnia, że wbrew temu, co wynika ze wspomnianego pkt 27 oraz z wniosku o wydanie orzeczenia w trybie prejudycjalnym, w swoich uwagach na piśmie wskazał on, że owe próby przetwarzania zostały odnotowane w dwóch protokołach sporządzonych przez funkcjonariuszy policji prowadzących postępowanie przygotowawcze w sprawie w postępowaniu głównym i że owe protokoły zostały następnie załączone do akt prokuratury.
- 37 Postanowieniem prezesa Trybunału z dnia 23 maja 2023 r. wniosek rządu austriackiego o sprostowanie opinii rzecznika generalnego został przekształcony we wniosek o otwarcie ustnego etapu postępowania na nowo w rozumieniu art. 83 regulaminu postępowania.
- 38 W tym względzie należy przypomnieć, po pierwsze, że statut Trybunału Sprawiedliwości Unii Europejskiej oraz regulamin postępowania przed Trybunałem nie dają zainteresowanym, o których mowa w art. 23 tego statutu, możliwości przedkładania uwag w odpowiedzi na opinię przedstawioną przez rzecznika generalnego. Po drugie, na podstawie art. 252 akapit drugi TFUE rzecznik generalny przedstawia publicznie, przy zachowaniu całkowitej bezstronności i niezależności, uzasadnioną opinię w sprawach, które zgodnie z tym statutem wymagają jego zaangażowania. Trybunał nie jest związany ani tą opinią, ani uzasadnieniem, w oparciu o które rzecznik generalny dochodzi do zawartych w opinii wniosków. W konsekwencji okoliczność, że jedna z zainteresowanych stron nie zgadza się z opinią rzecznika generalnego, bez względu na to, jakie kwestie rzecznik generalny porusza w swojej opinii, nie może sama w sobie stanowić uzasadnienia dla otwarcia ustnego etapu postępowania na nowo (wyrok z dnia 14 marca 2024 r., f6 Cigarettenfabrik, C-336/22, EU:C:2024:226, pkt 25 i przytoczone tam orzecznictwo).
- 39 Prawdą jest, że zgodnie z art. 83 regulaminu postępowania Trybunał może w każdej chwili, po zapoznaniu się ze stanowiskiem rzecznika generalnego, postanowić o otwarciu ustnego etapu postępowania na nowo, w szczególności jeśli uzna, że okoliczności zawisłej przed nim sprawy nie są wystarczająco wyjaśnione, lub jeśli po zamknięciu ustnego etapu postępowania strona przedstawiła nowy fakt mogący mieć decydujące znaczenie dla rozstrzygnięcia Trybunału, lub też jeśli sprawa ma zostać rozstrzygnięta na podstawie argumentu, który nie był przedmiotem dyskusji między zainteresowanymi stronami.
- 40 Jednakże w niniejszej sprawie Trybunał staje na stanowisku, że w następstwie pisemnego etapu postępowania oraz przeprowadzonej przed Trybunałem rozprawy dysponuje on wszystkimi informacjami koniecznymi do wydania wyroku w przedmiocie rozpatrywanego tu wniosku o wydanie orzeczenia w trybie prejudycjalnym. Ponadto okoliczności powołane przez rząd austriacki na poparcie jego wniosku o otwarcie ustnego etapu postępowania na nowo nie stanowią nowych okoliczności faktycznych mogących mieć decydujący wpływ na rozstrzygnięcie, które Trybunał ma wydać w niniejszej sprawie.
- 41 Co się tyczy konkretnie okoliczności faktycznych wskazanych w pkt 36 niniejszego wyroku, należy przypomnieć, że w ramach postępowania prejudycjalnego do Trybunału nie należy ustalenie, czy podnoszone okoliczności faktyczne zostały wykazane, lecz jedynie dokonanie wykładni odpowiednich przepisów prawa Unii (zob. podobnie wyrok z dnia 31 stycznia 2023 r., Puig Gordi i in., C-158/21, EU:C:2023:57, pkt 36). Zgodnie bowiem z utrwalonym orzecznictwem pytania dotyczące wykładni prawa Unii, z którymi zwrócił się sąd krajowy na gruncie stanu prawnego i faktycznego, za którego ustalenie jest on odpowiedzialny, przy czym prawidłowość tych ustaleń

nie podlega ocenie Trybunału, korzystają z domniemania, iż mają one znaczenie dla sprawy [zob. podobnie wyrok z dnia 18 czerwca 2024 r., Bundesrepublik Deutschland (Skutek decyzji o nadaniu statusu uchodźcy), C-753/22, EU:C:2024:524, pkt 44 i przytoczone tam orzecznictwo].

- 42 W tych okolicznościach Trybunał, po zapoznaniu się ze stanowiskiem rzecznika generalnego, uznaje, że nie ma potrzeby zarządzenia otwarcia ustnego etapu postępowania na nowo.

W przedmiocie dopuszczalności wniosku o wydanie orzeczenia w trybie prejudycjalnym

- 43 Kilkoro uczestników niniejszego postępowania, którzy złożyli uwagi na piśmie, zakwestionowało dopuszczalność wniosku o wydanie orzeczenia w trybie prejudycjalnym w całości lub niektórych z pytań przedłożonych przez sąd odsyłający.
- 44 W pierwszej kolejności rządy austriacki, francuski i szwedzki podnoszą, że postanowienie odsyłające nie spełnia wymogów przewidzianych w art. 94 regulaminu postępowania, ponieważ nie zawiera okoliczności faktycznych i prawnych niezbędnych do udzielenia temu sądowi użytecznej odpowiedzi.
- 45 W drugiej kolejności rząd austriacki podnosi, po pierwsze, że poprzez pytania prejudycjalne drugie i trzecie sąd odsyłający zmierza w istocie do ustalenia, czy przepisy §§ 18 i 99 StPO rozpatrywane łącznie są zgodne z prawem Unii. Ponieważ przepisy te nie określają warunków korzystania z zatrzymanych nośników danych, pytania te nie mają żadnego związku z przedmiotem sporu w postępowaniu głównym. Rząd ten podnosi też, po drugie, że zgodnie z prawem austriackim do dokonania zatrzymania telefonu komórkowego lub próby uzyskania wglądu do zapisanych w tym telefonie danych konieczne jest zarządzenie prokuratora. Sąd ten powinien zatem stwierdzić naruszenie prawa austriackiego, w związku z czym zadane przez wspomniany sąd pytania nie są konieczne do rozstrzygnięcia tego sporu i w związku z tym nie ma potrzeby orzekania w przedmiocie wniosku o wydanie orzeczenia w trybie prejudycjalnym.
- 46 Na wstępie należy przypomnieć, że zgodnie z utrwalonym orzecznictwem w ramach ustanowionej w art. 267 TFUE współpracy między Trybunałem i sądami krajowymi wyłącznie do sądu krajowego, przed którym zawisł spór i który powinien przyjąć na siebie odpowiedzialność za mające zapaść orzeczenie sądowe, należy dokonanie oceny, w świetle szczególnych okoliczności sprawy, zarówno konieczności wydania orzeczenia w trybie prejudycjalnym po to, aby tenże sąd krajowy był w stanie wydać swoje orzeczenie, jak i znaczenia dla sprawy pytań zadanych Trybunałowi. W związku z tym, jeśli postawione pytania dotyczą wykładni prawa Unii, Trybunał jest w zasadzie zobowiązany do wydania orzeczenia (wyrok z dnia 24 lipca 2023 r., Lin, C-107/23 PPU, EU:C:2023:606, pkt 61 i przytoczone tam orzecznictwo).
- 47 Wynika stąd, że pytania dotyczące prawa Unii korzystają z domniemania posiadania znaczenia dla sprawy. Odmowa wydania przez Trybunał orzeczenia w przedmiocie złożonego przez sąd krajowy pytania prejudycjalnego jest możliwa tylko wtedy, gdy jest oczywiste, że wykładnia prawa Unii, o którą wniesiono, nie ma żadnego związku ze stanem faktycznym lub z przedmiotem postępowania głównego, gdy problem jest natury hipotetycznej bądź gdy Trybunał nie dysponuje informacjami w zakresie stanu faktycznego lub prawnego niezbędnymi do udzielenia użytecznej odpowiedzi na postawione mu pytania (wyrok z dnia 24 lipca 2023 r., Lin, C-107/23 PPU, EU:C:2023:606, pkt 62 i przytoczone tam orzecznictwo).

- 48 Co się tyczy w pierwszej kolejności argumentu dotyczącego naruszenia wymogów przewidzianych w art. 94 regulaminu postępowania, należy zauważyć, iż zgodnie z utrwalonym orzecznictwem, które znalazło już odzwierciedlenie w art. 94 lit. a) i b) owego regulaminu, konieczność dokonania wykładni prawa Unii, która byłaby użyteczna dla sądu krajowego, wymaga, aby sąd krajowy określił ramy stanu faktycznego i prawnego, w jakie wpisują się zadawane przez niego pytania, lub aby przynajmniej wyjaśnił on okoliczności faktyczne, na jakich opierają się owe pytania. Ponadto – jak stanowi art. 94 lit. c) regulaminu postępowania przed Trybunałem – jest niezbędne, 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 ów sąd dostrzega między tymi przepisami a uregulowaniami krajowymi, które znajdują zastosowanie w postępowaniu głównym (wyrok z dnia 21 grudnia 2023 r., *European Superleague Company*, C-333/21, EU:C:2023:1011, pkt 59 i przytoczone tam orzecznictwo).
- 49 W niniejszej sprawie, co się tyczy stanu faktycznego, sąd odsyłający wyjaśnił we wniosku o wydanie orzeczenia w trybie prejudycjalnym, że austriackie organy policji, po zatrzymaniu telefonu komórkowego CG w ramach postępowania przygotowawczego prowadzonego przez funkcjonariuszy policji w sprawie handlu środkami odurzającymi, dwukrotnie próbowały uzyskać wgląd do zapisanych w tym telefonie danych, z własnej inicjatywy, bez uprzedniego uzyskania zgody prokuratora lub sądu w tym zakresie. Sąd ten wyjaśnił również, że CG dowiedział się o próbach uzyskania wglądu do danych zapisanych w jego telefonie komórkowym dopiero po zapoznaniu się z zeznaniami funkcjonariusza policji. Sąd odsyłający wskazał wreszcie, że owe próby uzyskania wglądu nie zostały również udokumentowane w aktach sprawy sporządzonych przez policję kryminalną.
- 50 Co się tyczy ram prawnych, sąd ten wyjaśnił, że przepisy krajowe, które wymienił on w postanowieniu odsyłającym, pozwalają na podjęcie próby uzyskania wglądu do danych zapisanych w telefonie komórkowym do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępstw, nie ograniczając tej możliwości wyłącznie do celów walki z poważną przestępczością, nie uzależniając tej próby od uprzedniej kontroli sądu lub niezależnego organu administracyjnego ani nie przewidując, że zainteresowane osoby winny zostać o tej próbie powiadomione, w szczególności po to, by móc się temu sprzeciwić poprzez wniesienie środka zaskarżenia do sądu.
- 51 Wspomniany sąd wyjaśnił ponadto, jak wynika z pkt 26–29 niniejszego wyroku, powody, dla których zwrócił się do Trybunału z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym, oraz związek, jaki jego zdaniem istnieje między przepisami prawa Unii i Karty, o których mowa w tym wniosku, a przepisami prawa austriackiego, które jego zdaniem mają zastosowanie do sporu w postępowaniu głównym.
- 52 Okoliczności, o których mowa w pkt 49–51 niniejszego wyroku, pozwalają zatem uznać, że wniosek o wydanie orzeczenia w trybie prejudycjalnym spełnia wymogi określone w art. 94 regulaminu postępowania.
- 53 W drugiej kolejności, odnosząc się do argumentacji, że przepisy prawa austriackiego, o których mowa w pytaniach prejudycjalnych drugim i trzecim, nie mają znaczenia dla sprawy i że sąd odsyłający powinien był stwierdzić naruszenie tego prawa, należy przypomnieć, że do Trybunału nie należy orzekanie w przedmiocie wykładni przepisów krajowych ani orzekanie, czy wykładnia lub stosowanie ich przez sąd krajowy są prawidłowe, ponieważ taka wykładnia należy do

wyłącznej właściwości tego sądu [wyrok z dnia 15 czerwca 2023 r., Getin Noble Bank (Zawieszenie wykonania umowy kredytu), C-287/22, EU:C:2023:491, pkt 32 i przytoczone tam orzecznictwo].

- 54 W niniejszej sprawie z wniosku o wydanie orzeczenia w trybie prejudycjalnym, a w szczególności z brzmienia pytań prejudycjalnych wynika, że sąd odsyłający uważa, po pierwsze, że owe przepisy prawa austriackiego mają zastosowanie do sporu w postępowaniu głównym, a po drugie, że próba uzyskania wglądu do danych zapisanych w telefonie komórkowym bez uprzedniego uzyskania zgody prokuratora lub sądu, taka jak rozpatrywana w postępowaniu głównym, jest dozwolona przez prawo austriackie. Zgodnie z orzecznictwem przytoczonym w poprzednim punkcie niniejszego wyroku do Trybunału nie należy orzekanie w przedmiocie takiej wykładni rzeczonych przepisów.
- 55 Z powyższego wynika, że pytania zadane przez sąd odsyłający są dopuszczalne.

Co do istoty

- 56 Rząd austriacki podnosi w swoich uwagach na piśmie, że Trybunał nie jest właściwy do udzielenia odpowiedzi na pytania prejudycjalne pierwsze i drugie, ponieważ pytania te dotyczą wykładni art. 5 i art. 15 ust. 1 dyrektywy 2002/58, jest zaś oczywiste, że dyrektywa ta nie ma zastosowania do sporu w postępowaniu głównym. Na rozprawie kilka rządów podniosło, że nie ma możliwości przeformułowania pytań prejudycjalnych w świetle dyrektywy 2016/680. W szczególności rząd austriacki podkreślił, że takiemu przeformułowaniu stoi na przeszkodzie fakt, iż ta ostatnia dyrektywa nie zawiera przepisów równoważnych z art. 5 i art. 15 ust. 1 dyrektywy 2002/58. Rząd francuski podniósł z kolei, że uprawnienie do przeformułowania pytań prejudycjalnych jest ograniczone przez prawo państw członkowskich do przedstawienia uwag na piśmie. Otóż zdaniem tego rządu prawo to zostałoby pozbawione wszelkiej skuteczności, gdyby ramy prawne postępowania mogły zostać radykalnie zmienione wskutek przeformułowania pytań prejudycjalnych przez Trybunał.
- 57 W tym względzie należy przypomnieć, iż Trybunał orzekł, opierając się w szczególności na art. 1 ust. 1 i 3 oraz art. 3 dyrektywy 2002/58, 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, nie jest objęta dyrektywą 2002/58, a jedynie prawem krajowym, z zastrzeżeniem stosowania dyrektywy 2016/680 (wyroki z dnia 6 października 2020 r.: Privacy International, C-623/17, EU:C:2020:790, pkt 48; a także La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 103).
- 58 Tymczasem nie ma wątpliwości, że spór w postępowaniu głównym dotyczy próby uzyskania przez funkcjonariuszy policji bezpośredniego wglądu do danych osobowych zapisanych w telefonie komórkowym, bez jakiegokolwiek interwencji ze strony dostawcy usług łączności elektronicznej.
- 59 Jest zatem oczywiste, że spór ten nie jest objęty zakresem stosowania dyrektywy 2002/58, do której odnoszą się pytania prejudycjalne pierwsze i drugie.
- 60 Należy jednak pamiętać, że zgodnie z utrwalonym orzecznictwem w ramach ustanowionej w art. 267 TFUE procedury współpracy między sądami krajowymi a Trybunałem do tego ostatniego należy udzielenie sądowi krajowemu użytecznej odpowiedzi, która umożliwi mu rozstrzygnięcie zawisłego przed nim sporu. Mając to na uwadze, Trybunał powinien w razie

potrzeby przeformułować przedłożone mu pytania. Ponadto Trybunał może wziąć pod rozwagę normy prawa Unii, na które sąd krajowy nie powołał się w swoich pytaniach prejudycjalnych [wyroki: z dnia 15 lipca 2021 r., *Ministrstvo za obrambo*, C-742/19, EU:C:2021:597, pkt 31 i przytoczone tam orzecznictwo; a także z dnia 18 czerwca 2024 r., *Generalstaatsanwaltschaft Hamm* (Wniosek o ekstradycję uchodźcy do Turcji), C-352/22, EU:C:2024:521, pkt 47].

- 61 Okoliczność, iż sąd krajowy powołał się formalnie w pytaniu prejudycjalnym na określone przepisy prawa Unii, nie stoi bowiem na przeszkodzie temu, by Trybunał przekazał temu sądowi wszelkie wskazówki dotyczące wykładni, które mogą być pomocne w rozstrzygnięciu rozpatrywanej przez niego sprawy, niezależnie od tego, czy sąd krajowy powołał się na nie w treści pytań. W tym względzie Trybunał powinien wyprowadzić z całości informacji przedstawionych przez sąd krajowy, a w szczególności z uzasadnienia postanowienia odsyłającego, elementy prawa Unii, które wymagają wykładni w świetle przedmiotu sporu rozpatrywanego w postępowaniu głównym (wyrok z dnia 22 czerwca 2022 r., *Volvo i DAF Trucks*, C-267/20, EU:C:2022:494, pkt 28 i przytoczone tam orzecznictwo).
- 62 Ponadto informacje zawarte w postanowieniu odsyłającym powinny nie tylko pozwolić Trybunałowi na udzielenie użytecznych odpowiedzi, ale także umożliwić rządów państw członkowskich oraz innym zainteresowanym stronom przedstawienie uwag zgodnie z art. 23 statutu Trybunału Sprawiedliwości Unii Europejskiej (wyrok z dnia 21 grudnia 2023 r., *Royal Antwerp Football Club*, C-680/21, EU:C:2023:1010, pkt 32 i przytoczone tam orzecznictwo).
- 63 Jednakże, jak wynika z pkt 31–33 niniejszego wyroku, w odpowiedzi na wniosek o udzielenie informacji skierowany przez Trybunał do sądu odsyłającego ten ostatni wskazał, że dyrektywa 2016/680 ma zastosowanie do sporu w postępowaniu głównym. Zainteresowane strony miały możliwość zająć w swoich uwagach na piśmie stanowisko w przedmiocie wykładni tej dyrektywy i jej znaczenia dla sprawy w postępowaniu głównym. Ponadto na potrzeby rozprawy Trybunał zwrócił się do uczestników ustnego etapu postępowania o udzielenie na rozprawie odpowiedzi na pewne pytania dotyczące wspomnianej dyrektywy. W szczególności wezwał ich do zajęcia stanowiska w przedmiocie znaczenia art. 4 tej dyrektywy dla udzielenia odpowiedzi na pierwsze pytanie prejudycjalne oraz art. 13 i 54 tej dyrektywy w celu udzielenia odpowiedzi na trzecie pytanie prejudycjalne.
- 64 W konsekwencji okoliczność, że pytania prejudycjalne pierwsze i drugie dotyczą wykładni art. 5 i art. 15 ust. 1 dyrektywy 2002/58, a nie dyrektywy 2016/680, nie stoi na przeszkodzie przeformułowaniu pytań zadanych przez sąd odsyłający w świetle mających znaczenie dla niniejszej sprawy przepisów tej ostatniej dyrektywy, a tym samym – nie stoi na przeszkodzie przyznaniu właściwości Trybunału do udzielenia odpowiedzi na te pytania.
- 65 Wniosku tego nie podważa argument Irlandii oraz rządów francuskiego i norweskiego, zgodnie z którym próba uzyskania wglądu do danych osobowych nie jest objęta zakresem stosowania dyrektywy 2016/680, ponieważ dyrektywa ta ma zastosowanie wyłącznie do faktycznego przetwarzania danych.
- 66 Rządy te podnoszą w tym względzie, że wykładnia przepisów tej dyrektywy nie byłaby użyteczna dla rozstrzygnięcia sporu w postępowaniu głównym, podobnie jak wykładnia przepisów Karty, ponieważ ma ona zastosowanie jedynie w przypadku, gdy państwa członkowskie stosują prawo Unii.

- 67 Jednakże w sytuacji gdy nie jest oczywiste, że wykładnia aktu prawa Unii nie ma wpływu na rzeczywistość lub na przedmiot postępowania głównego, jak ma to miejsce w przypadku dyrektywy 2016/680, zarzut, że akt ten nie ma zastosowania do postępowania głównego, należy do istoty pytań prejudycjalnych (zob. analogicznie wyrok z dnia 24 lipca 2023 r., Lin, C-107/23 PPU, EU:C:2023:606, pkt 66 i przytoczone tam orzecznictwo).
- 68 Na wstępie należy zatem zbadać, czy próba uzyskania przez funkcjonariuszy policji wglądu do danych zapisanych w telefonie komórkowym jest objęta przedmiotowym zakresem stosowania tej dyrektywy.

W przedmiocie stosowania dyrektywy 2016/680 do próby uzyskania wglądu do danych zapisanych w telefonie komórkowym

- 69 Artykuł 2 ust. 1 dyrektywy 2016/680 określa przedmiotowy zakres stosowania tej dyrektywy. W myśl tego przepisu dyrektywa ta „ma zastosowanie do przetwarzania danych osobowych przez właściwe organy do celów określonych w [jej] art. 1 ust. 1”, a konkretnie między innymi do „zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych”.
- 70 Artykuł 3 pkt 2 tej dyrektywy definiuje pojęcie „przetwarzania” jako oznaczające „operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak [...] pobieranie, przeglądanie” lub „rozpowszechnianie lub innego rodzaju udostępnianie”.
- 71 Z samego brzmienia art. 3 pkt 2 dyrektywy 2016/680, a w szczególności z użycia wyrażen „operacja”, „zestaw operacji” i „innego rodzaju udostępnianie” wynika zatem, że prawodawca Unii zamierzał ująć pojęcie „przetwarzania”, a tym samym zakres przedmiotowy stosowania tej dyrektywy, szeroko. Taką wykładnię potwierdza niewyczerpujący charakter czynności wymienionych we wspomnianym przepisie, wyrażony poprzez użycie sformułowania „takich jak” [zob. analogicznie wyrok z dnia 24 lutego 2022 r., Valsts ienēmumu dienests (Przetwarzanie danych osobowych do celów podatkowych), C-175/20, EU:C:2022:124, pkt 35].
- 72 Wskazane wyżej sformułowania przemawiają zatem za wykładnią, zgodnie z którą w przypadku zatrzymania telefonu przez organy policyjne i podjęcia przez nie próby uzyskania do niego wglądu w celu pobrania i przejrzania zapisanych w tym telefonie danych osobowych organy te dokonują przetwarzania w rozumieniu art. 3 pkt 2 dyrektywy 2016/680, nawet jeśli owe organy ostatecznie nie zdołały, ze względów technicznych, uzyskać wglądu do tych danych.
- 73 Wykładnię tę potwierdza kontekst, w jaki wpisuje się art. 3 pkt 2 dyrektywy 2016/680. Otóż w myśl art. 4 ust. 1 lit. b) tej dyrektywy państwa członkowskie zapewniają, aby dane osobowe były gromadzone do określonych, jednoznacznych i legalnych celów oraz aby nie były poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem. Ten ostatni przepis wprowadza zasadę ograniczenia celów [zob. podobnie wyrok z dnia 26 stycznia 2023 r., Ministerstvo na vatreshnite raboti (Rejestracja danych biometrycznych i genetycznych przez policję), C-205/21, EU:C:2023:49, pkt 122]. Tymczasem skuteczność tej zasady z konieczności wymaga, aby cel gromadzenia danych był określony od momentu, w którym właściwe organy podejmują próbę uzyskania wglądu do danych osobowych, ponieważ taka próba, jeśli okaże się skuteczna, może pozwolić tym organom w szczególności na natychmiastowe gromadzenie, pobranie i przejrzanie danych.

- 74 Co się tyczy celów dyrektywy 2016/680, akt ten zmierza w szczególności, jak wynika z jego motywów 4, 7 i 15, do zapewnienia wysokiego poziomu ochrony danych osobowych osób fizycznych.
- 75 Tymczasem gdyby próba uzyskania wglądu do danych osobowych zapisanych w telefonie komórkowym nie mogła zostać uznana za „przetwarzanie” tych danych, cel ten zostałby udaremniony. Taka wykładnia dyrektywy 2016/680 narażałaby bowiem osoby, których dotyczy taka próba uzyskania wglądu, na znaczne ryzyko, że naruszenia zasad ustanowionych w tej dyrektywie nie można będzie już uniknąć.
- 76 Należy jeszcze zauważyć, że taka wykładnia jest zgodna z zasadą pewności prawa, która zgodnie z utrwalonym orzecznictwem Trybunału wymaga, aby stosowanie norm prawa było przewidywalne dla jednostek, w szczególności gdy normy te mogą mieć dla nich niekorzystne konsekwencje (wyrok z dnia 27 czerwca 2024 r., *Gestore dei Servizi Energetici*, C-148/23, EU:C:2024:555, pkt 42 i przytoczone tam orzecznictwo). Wykładnia, zgodnie z którą stosowanie dyrektywy 2016/680 zależałoby od powodzenia próby uzyskania wglądu do danych osobowych zapisanych w telefonie komórkowym, powodowałaby bowiem niepewność zarówno po stronie właściwych organów krajowych, jak i po stronie jednostek, co jest niezgodne z tą zasadą.
- 77 Z powyższego wynika, że próba uzyskania przez organy policyjne wglądu do danych zapisanych w telefonie komórkowym na potrzeby postępowania przygotowawczego w sprawach karnych, taka jak rozpatrywana w postępowaniu głównym, wchodzi, jak stwierdził rzecznik generalny w pkt 53 opinii, w zakres stosowania dyrektywy 2016/680.

W przedmiocie pytań pierwszego i drugiego

- 78 Sąd odsyłający w pytaniach pierwszym i drugim wyraźnie odniósł się, po pierwsze, do art. 15 ust. 1 dyrektywy 2002/58, wymagającego w szczególności, aby środki ustawodawcze, na których przyjęcie dyrektywa ta zezwala państwom członkowskim i które ograniczają zakres praw i obowiązków przewidzianych w wielu przepisach tej dyrektywy, były niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego – czyli bezpieczeństwa państwa – obronności i bezpieczeństwa publicznego oraz zapobiegania przestępstwom kryminalnym lub niedozwolonemu używaniu systemów łączności elektronicznej, ich dochodzenia, wykrywania i ścigania, jak i, po drugie, do art. 52 ust. 1 Karty, który ustanawia zasadę proporcjonalności w kontekście ograniczeń w korzystaniu z praw i wolności uznanych w Karcie.
- 79 Tymczasem w myśl art. 4 ust. 1 lit. c) dyrektywy 2016/680 państwa członkowskie powinny zapewnić, by dane osobowe były adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane. Przepis ten wymaga zatem przestrzegania przez państwa członkowskie zasady „minimalizacji danych”, która wyraża zasadę proporcjonalności (wyrok z dnia 30 stycznia 2024 r., *Direktor na Glavna direktsia „Natsionalna politisia” pri MVR – Sofia*, C-118/22, EU:C:2024:97, pkt 41 i przytoczone tam orzecznictwo).
- 80 Wynika z tego w szczególności, że zbieranie danych osobowych w ramach postępowania karnego i przechowywanie ich przez organy policyjne do celów określonych w art. 1 ust. 1 tej dyrektywy powinno być zgodne z powyższą zasadą, podobnie jak każde inne przetwarzanie objęte zakresem stosowania tej dyrektywy (wyrok z dnia 30 stycznia 2024 r., *Direktor na Glavna direktsia „Natsionalna politisia” pri MVR – Sofia*, C-118/22, EU:C:2024:97, pkt 42 i przytoczone tam orzecznictwo).

- 81 Należy zatem uznać, że poprzez pytania pierwsze i drugie, które należy rozpatrzyć łącznie, sąd odsyłający dąży w istocie do ustalenia, czy art. 4 ust. 1 lit. c) dyrektywy 2016/680 w związku z art. 7 i 8 oraz z art. 52 ust. 1 Karty stoi na przeszkodzie uregulowaniu krajowemu, które przyznaje właściwym organom możliwość uzyskania wglądu do danych zapisanych w telefonie komórkowym w celu zapobiegania przestępstwom w ogólności, ich dochodzenia, wykrywania i ścigania oraz które nie uzależnia tej możliwości od uprzedniej kontroli sądowej lub kontroli niezależnego organu administracyjnego.
- 82 Na wstępie należy zauważyć, że jak wynika z motywów 2 i 4 dyrektywy 2016/680, ustanawiając solidne i spójne ramy ochrony danych osobowych w celu zapewnienia poszanowania podstawowego prawa do ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych, zagwarantowanego w art. 8 ust. 1 Karty i w art. 16 ust. 1 TFUE, dyrektywa ta ma na celu przyczynienie się do realizacji przestrzeni wolności, bezpieczeństwa i sprawiedliwości w Unii [zob. podobnie wyrok z dnia 25 lutego 2021 r., Komisja/Hiszpania (Dyrektywa o danych osobowych – Dziedzina karna), C-658/19, EU:C:2021:138, pkt 75].
- 83 W tym celu dyrektywa 2016/680 zmierza w szczególności, jak wskazano w pkt 74 niniejszego wyroku, do zapewnienia wysokiego poziomu ochrony danych osobowych osób fizycznych.
- 84 W tym względzie należy przypomnieć, że jak podkreślono w motywie 104 dyrektywy 2016/680, ograniczenia wprowadzone tą dyrektywą w odniesieniu do prawa do ochrony danych osobowych przewidzianego w art. 8 Karty, a także prawa do poszanowania życia prywatnego i rodzinnego chronionego w art. 7 Karty, należy interpretować zgodnie z wymogami art. 52 ust. 1 Karty, które obejmują poszanowanie zasady proporcjonalności (zob. podobnie wyrok z dnia 30 stycznia 2024 r., Direktor na Glavna direktsia „Natsionalna politsia” pri MVR – Sofia, C-118/22, EU:C:2024:97, pkt 33).
- 85 Prawa podstawowe nie są bowiem prerogatywami o charakterze absolutnym, lecz należy je postrzegać w świetle ich funkcji społecznej i wyważyć względem innych praw podstawowych. Wszelkie ograniczenia w korzystaniu z tych praw podstawowych muszą zgodnie z art. 52 ust. 1 Karty być przewidziane ustawą i szanować istotę wspomnianych praw podstawowych oraz zasadę proporcjonalności. Na podstawie tej ostatniej zasady ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. Powinny one odbywać się w granicach tego, co absolutnie konieczne, a uregulowanie tych ograniczeń musi zawierać jasne i precyzyjne zasady regulujące ich zakres i stosowanie (wyrok z dnia 30 stycznia 2024 r., Direktor na Glavna direktsia „Natsionalna politsia” pri MVR – Sofia, C-118/22, EU:C:2024:97, pkt 39 i przytoczone tam orzecznictwo).
- 86 Co się tyczy w pierwszej kolejności celu interesu ogólnego mogącego uzasadniać ograniczenie w korzystaniu z praw podstawowych zagwarantowanych w art. 7 i 8 Karty, takie jak ograniczenie wynikające z uregulowania rozpatrywanego w postępowaniu głównym, należy podkreślić, że przetwarzanie danych osobowych w ramach postępowania przygotowawczego prowadzonego przez policję w sprawie przestępstwa, takie jak próba uzyskania wglądu do danych zapisanych w telefonie komórkowym, należy co do zasady uznać za faktycznie odpowiadające celowi interesu ogólnego uznanemu przez Unię w rozumieniu art. 52 ust. 1 Karty.
- 87 Co się tyczy w drugiej kolejności wymogu niezbędności takiego ograniczenia, jak podkreślono w istocie w motywie 26 dyrektywy 2016/680, wymóg ten nie jest spełniony, jeżeli zamierzony cel interesu ogólnego można racjonalnie osiągnąć w równie skuteczny sposób za pomocą innych

środków, w mniejszym stopniu naruszających prawa podstawowe osób, których dane dotyczą (zob. podobnie wyrok z dnia 30 stycznia 2024 r., Direktor na Glavna direktsia „Natsionalna politisia” pri MVR – Sofia, C-118/22, EU:C:2024:97, pkt 40 i przytoczone tam orzecznictwo).

- 88 Natomiast wymóg konieczności jest spełniony, gdy cel zamierzony w ramach przetwarzania danych nie może zostać racjonalnie osiągnięty w sposób równie skuteczny za pomocą innych środków, w mniejszym stopniu naruszających prawa podstawowe osób, których dane dotyczą, w szczególności prawo do poszanowania życia prywatnego i prawo do ochrony danych osobowych, zagwarantowane w art. 7 i 8 Karty [wyrok z dnia 26 stycznia 2023 r., Ministerstvo na vatreshnite raboti (Rejestracja danych biometrycznych i genetycznych przez policję), C-205/21, EU:C:2023:49, pkt 126 i przytoczone tam orzecznictwo].
- 89 Co się tyczy w trzeciej kolejności proporcjonalności ograniczenia w korzystaniu z praw zagwarantowanych w art. 7 i 8 Karty, wynikającego z takiego przetwarzania, wymaga ona wyważenia wszystkich istotnych okoliczności danego przypadku (zob. podobnie wyrok z dnia 30 stycznia 2024 r., Direktor na Glavna direktsia „Natsionalna politisia” pri MVR – Sofia, C-118/22, EU:C:2024:97, pkt 62, 63 i przytoczone tam orzecznictwo).
- 90 Okoliczności te obejmują w szczególności wagę wprowadzonego w ten sposób ograniczenia w korzystaniu z rozpatrywanych praw podstawowych, która zależy od charakteru i wrażliwości danych, do których właściwe organy policyjne mogą mieć wgląd, od znaczenia celu interesu ogólnego realizowanego przez to ograniczenie, związku między posiadaczem telefonu komórkowego a danym przestępstwem oraz znaczenia spornych danych dla ustalenia stanu faktycznego.
- 91 Co się tyczy, po pierwsze, wagi ograniczenia praw podstawowych wynikającego z uregulowania takiego jak to rozpatrywane w postępowaniu głównym, z postanowienia odsyłającego wynika, że uregulowanie to pozwala właściwym organom policyjnym na wgląd, bez konieczności uzyskania uprzedniej zgody, do danych zapisanych w telefonie komórkowym.
- 92 Taki wgląd może dotyczyć, w zależności od zawartości danego telefonu komórkowego i decyzji tych organów policyjnych, nie tylko danych o ruchu i lokalizacji, lecz również zdjęć i historii przeglądania Internetu za pomocą tego telefonu, a nawet fragmentów treści komunikacji prowadzonej za pomocą tego telefonu, w szczególności poprzez uzyskanie wglądu do zapisanych w nim wiadomości.
- 93 Uzyskanie wglądu do ogółu tego rodzaju danych może dostarczyć bardzo szczegółowych informacji na temat życia prywatnego zainteresowanej osoby, takich jak jej codzienne nawyki, miejsce stałego lub czasowego pobytu, codziennie lub sporadycznie pokonywane trasy, podejmowane czynności, relacje społeczne i środowisko społeczne, w jakim taka osoba się obraca.
- 94 Nie można wreszcie wykluczyć, że dane zawarte w telefonie komórkowym mogą obejmować dane szczególnie wrażliwe, takie jak dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przy czym ta wrażliwość uzasadnia szczególną ochronę, jakiej wymaga w odniesieniu do nich art. 10 dyrektywy 2016/680, a która rozciąga się również na dane ujawniane w wyniku przeprowadzenia intelektualnego procesu dedukcji lub kontroli krzyżowej [zob. analogicznie wyrok z dnia 5 czerwca 2023 r., Komisja/Polska (Niezawisłość i życie prywatne sędziów), C-204/21, EU:C:2023:442, pkt 344].

- 95 Ingerencję w prawa podstawowe zagwarantowane w art. 7 i 8 Karty, do której może prowadzić stosowanie przepisów takich jak te rozpatrywane w postępowaniu głównym, należy zatem uznać za poważną, a nawet szczególnie poważną ingerencję w te prawa.
- 96 Co się tyczy, po drugie, znaczenia realizowanego celu, należy podkreślić, że waga przestępstwa, w którego sprawie prowadzone jest postępowanie przygotowawcze, jest jednym z kluczowych elementów badania proporcjonalności poważnej ingerencji, jaką stanowi wgląd do danych osobowych zapisanych w telefonie komórkowym, pozwalających na wyciągnięcie precyzyjnych wniosków co do życia prywatnego osoby, której dane dotyczą.
- 97 Jednakże uznanie, że tylko zwalczanie poważnej przestępczości może uzasadniać wgląd do danych zapisanych w telefonie komórkowym, ograniczałoby uprawnienia dochodzeniowe właściwych organów w rozumieniu dyrektywy 2016/680 w odniesieniu do ogólnie pojętej przestępczości. Zwiększyłoby to ryzyko bezkarności w przypadku takich przestępstw, biorąc pod uwagę znaczenie, jakie te dane mogą mieć w kontekście postępowań przygotowawczych w sprawie przestępstw. Takie ograniczenie naruszałoby zatem szczególny charakter zadań wykonywanych przez te organy w celach określonych w art. 1 ust. 1 tej dyrektywy, podkreślony w jej motywach 10 i 11, i szkodziłoby celowi realizacji przestrzeni wolności, bezpieczeństwa i sprawiedliwości w Unii, który prześwieca tej dyrektywie.
- 98 Niemniej jednak rozważania te pozostają bez uszczerbku dla wynikającego z art. 52 ust. 1 Karty wymogu, zgodnie z którym wszelkie ograniczenia w korzystaniu z prawa podstawowego muszą być „przewidziane ustawą”, przy czym wymóg ten oznacza, że podstawa prawna zezwalająca na takie ograniczenie określa jej zakres w sposób wystarczająco jasny i precyzyjny [zob. podobnie wyrok z dnia 26 stycznia 2023 r., Ministerstvo na vatreshnite raboti (Rejestracja danych biometrycznych i genetycznych przez policję), C-205/21, EU:C:2023:49, pkt 65 i przytoczone tam orzecznictwo].
- 99 W celu spełnienia tego wymogu do ustawodawcy krajowego należy określenie w sposób wystarczająco precyzyjny elementów, w szczególności charakteru lub kategorii określonych przestępstw, które należy wziąć pod uwagę.
- 100 Co się tyczy, po trzecie, związku posiadacza telefonu komórkowego z danym przestępstwem oraz znaczenia rozpatrywanych danych dla ustalenia okoliczności faktycznych, z art. 6 dyrektywy 2016/680 wynika, że pojęcie „osoby, której dane dotyczą” obejmuje różne kategorie osób, a mianowicie w istocie osoby, w stosunku do których istnieją poważne podstawy, by przypuszczać, że popełniły one lub zamierzają popełnić czyn zabroniony, osoby skazane za czyn zabroniony, pokrzywdzonych lub potencjalnych pokrzywdzonych czynem zabronionym, a także osoby inne w stosunku do czynu zabronionego, które mogą zostać wezwane do złożenia zeznań w ramach postępowania przygotowawczego w sprawie czynu zabronionego lub na dalszych etapach postępowania karnego. Na gruncie tego artykułu państwa członkowskie mają obowiązek zapewnić, by administrator – w stosownym przypadku i w miarę możliwości – wyraźnie rozróżniał dane osobowe poszczególnych kategorii osób, których dane dotyczą.
- 101 W tym względzie, co się tyczy w szczególności wglądu do danych zapisanych w telefonie komórkowym osoby, wobec której toczy się postępowanie karne, tak jak w sprawie w postępowaniu głównym, ważne jest, by uzasadnione podejrzenie, że osoba ta popełniła przestępstwo, jest w trakcie jego popełniania lub planuje je popełnić, lub jest w jakiś sposób w takie przestępstwo zamieszana, było poparte obiektywnymi i wystarczającymi dowodami.

- 102 To w szczególności w celu upewnienia się, że zasada proporcjonalności jest przestrzegana w każdym konkretnym przypadku poprzez wyważenie wszystkich istotnych czynników, jest istotne, by w sytuacji gdy wgląd właściwych organów krajowych w dane osobowe wiąże się z ryzykiem poważnej, a nawet szczególnie poważnej ingerencji w prawa podstawowe osoby, której dane dotyczą, wgląd ten był uzależniony od uprzedniej kontroli dokonywanej albo przez sąd, albo przez niezależny organ administracyjny.
- 103 Ta uprzednia kontrola wymaga, aby sąd lub niezależny organ administracyjny odpowiedzialny za jej przeprowadzenie dysponował wszelkimi uprawnieniami i gwarancjami niezbędnymi do pogodzenia różnych wchodzących w grę uzasadnionych interesów i praw. Jeśli chodzi w szczególności o postępowanie przygotowawcze w sprawie karnej, taka kontrola wymaga, aby ten sąd lub organ był w stanie zapewnić właściwą równowagę pomiędzy z jednej strony uzasadnionymi interesami związanymi z potrzebami postępowania przygotowawczego w kontekście zwalczania przestępczości a z drugiej strony prawami podstawowymi do poszanowania życia prywatnego i ochrony danych osobowych osób, do których danych uzyskuje się wgląd.
- 104 Ta niezależna kontrola, w sytuacji takiej jak ta, o której mowa w pkt 102 niniejszego wyroku, powinna zostać przeprowadzona przed każdą próbą uzyskania wglądu do określonych danych, z wyjątkiem należycie uzasadnionych pilnych przypadków, w których kontrola ta powinna nastąpić jak najszybciej. Taka późniejsza kontrola nie pozwoliłaby bowiem na realizację celu uprzedniej kontroli, polegającego na uniemożliwieniu udzielania zgody na wgląd do rozpatrywanych danych, który wykracza poza granice tego, co ściśle niezbędne.
- 105 W szczególności sąd lub niezależny organ administracyjny, działając w ramach uprzedniej kontroli przeprowadzonej w następstwie uzasadnionego wniosku o uzyskanie wglądu wchodzącego w zakres stosowania dyrektywy 2016/680, powinien być uprawniony do odmowy lub ograniczenia tego wglądu, jeżeli stwierdzi on, że w świetle wszystkich istotnych okoliczności ingerencja w prawa podstawowe, jaką stanowi wspomniany wgląd, byłaby nieproporcjonalna.
- 106 Właściwym organom policyjnym należy też odmówić wglądu do danych zapisanych w telefonie komórkowym lub ograniczyć ten wgląd, jeżeli, biorąc pod uwagę wagę przestępstwa i potrzeby prowadzonego postępowania, wgląd do treści komunikatów lub danych szczególnie chronionych nie wydaje się uzasadniony.
- 107 Co się tyczy w szczególności przetwarzania danych wrażliwych, należy wziąć pod uwagę wymogi ustanowione w art. 10 dyrektywy 2016/680, którego celem jest zapewnienie zwiększonej ochrony w odniesieniu do takiego przetwarzania, które może powodować, jak wynika z motywu 37 tej dyrektywy, poważne zagrożenia dla podstawowych praw i wolności, takich jak prawo do poszanowania życia prywatnego i prawo do ochrony danych osobowych, zagwarantowane w art. 7 i 8 Karty. W tym celu, jak wynika z samego brzmienia tego art. 10, wymóg, zgodnie z którym przetwarzanie takich danych jest dopuszczalne „wyłącznie wtedy, jeżeli jest bezwzględnie niezbędne”, powinien być interpretowany jako definiujący bardziej rygorystyczne warunki zgodności z prawem przetwarzania danych wrażliwych w porównaniu z warunkami wynikającymi z art. 4 ust. 1 lit. b) i c) oraz z art. 8 ust. 1 tej dyrektywy, które odnoszą się jedynie do „niezbędności” przetwarzania danych objętych, w sposób ogólny, zakresem stosowania wspomnianej dyrektywy [wyrok z dnia 26 stycznia 2023 r., Ministerstvo na vatreshnite raboti (Rejestracja danych biometrycznych i genetycznych przez policję), C-205/21, EU:C:2023:49, pkt 116, 117 i przytoczone tam orzecznictwo].

- 108 A zatem, po pierwsze, użycie przysłówka „wyłącznie” przed wyrażeniem „wtedy, jeżeli jest bezwzględnie niezbędne” kładzie nacisk na to, że przetwarzanie szczególnych kategorii danych w rozumieniu art. 10 może być uznane za niezbędne wyłącznie w ograniczonej liczbie wypadków. Po drugie, charakter „bezwzględnej” niezbędności przetwarzania takich danych wymaga, by ta niezbędność była oceniana w sposób szczególnie rygorystyczny [wyrok z dnia 26 stycznia 2023 r., Ministerstvo na vatreshnite raboti (Rejestracja danych biometrycznych i genetycznych przez policję), C-205/21, EU:C:2023:49, pkt 118].
- 109 Tymczasem w niniejszej sprawie sąd odsyłający wskazuje, że w toku postępowania przygotowawczego austriackie organy policji mają prawo wglądu do danych zawartych w telefonie komórkowym. Ponadto wyjaśnia on, że wgląd ten nie jest co do zasady uzależniony od uzyskania uprzedniej zgody sądu lub niezależnego organu administracyjnego. Jednakże wyłącznie do tego sądu należy wyciągnięcie konsekwencji z wyjaśnień dokonanych w szczególności w pkt 102–108 niniejszego wyroku w sporze w postępowaniu głównym.
- 110 Z powyższego wynika, że na pytania pierwsze i drugie należy odpowiedzieć, iż art. 4 ust. 1 lit. c) dyrektywy 2016/680 w związku z art. 7 i 8 oraz z art. 52 ust. 1 Karty należy interpretować w ten sposób, że nie stoi on na przeszkodzie uregulowaniu krajowemu, które przyznaje właściwym organom możliwość uzyskania wglądu do danych zapisanych w telefonie komórkowym w celu zapobiegania przestępstwom w ogólności, ich dochodzenia, wykrywania i ścigania, pod warunkiem że owo uregulowanie:
- w wystarczająco precyzyjny sposób określa charakter lub kategorie przestępstw, których dotyczy,
 - gwarantuje poszanowanie zasady proporcjonalności oraz
 - uzależnia skorzystanie z tej możliwości, z wyjątkiem należycie uzasadnionych pilnych przypadków, od uprzedniej kontroli sądu lub niezależnego organu administracyjnego.

W przedmiocie pytania trzeciego

- 111 Z postanowienia odsyłającego wynika, że poprzez pytanie trzecie sąd odsyłający zmierza w istocie do ustalenia, czy CG powinien być zostać poinformowany o próbach uzyskania wglądu do danych zapisanych w jego telefonie komórkowym, aby mógł on skorzystać z prawa do skutecznego środka prawnego zagwarantowanego w art. 47 Karty.
- 112 W tym względzie właściwymi przepisami dyrektywy 2016/680 są, po pierwsze, art. 13 tej dyrektywy, zatytułowany „Informacje udostępniane lub przekazywane osobie, której dane dotyczą”, a po drugie, art. 54 wspomnianej dyrektywy, zatytułowany „Prawo do skutecznego środka prawnego przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu”.
- 113 Należy również przypomnieć, jak podkreślono w motywie 104 dyrektywy 2016/680, że ograniczenia wprowadzone tą dyrektywą w odniesieniu do prawa do skutecznego środka prawnego i rzetelnego procesu, chronionego na mocy art. 47 Karty, należy interpretować zgodnie z wymogami art. 52 ust. 1 Karty, które obejmują obowiązek poszanowania zasady proporcjonalności.

- 114 Należy zatem uznać, że poprzez pytanie trzecie sąd odsyłający dąży w istocie do ustalenia, czy art. 13 i 54 dyrektywy 2016/680 w związku z art. 47 i z art. 52 ust. 1 Karty należy interpretować w ten sposób, że stoją one na przeszkodzie uregulowaniu krajowemu, które pozwala właściwym organom policyjnym na podjęcie próby uzyskania wglądu do danych zapisanych w telefonie komórkowym bez poinformowania o tym osoby, której dane dotyczą.
- 115 Z art. 13 ust. 2 lit. d) dyrektywy 2016/680 wynika, że oprócz informacji, o których mowa w ust. 1, takich jak tożsamość administratora, cel tego przetwarzania oraz prawo do wniesienia skargi do organu nadzorczego, a które to informacje które należy udostępnić osobie, której dane dotyczą, państwa członkowskie powinny ustawowo przewidzieć, że administrator przekazuje osobie, której dane dotyczą, dalsze informacje umożliwiające jej wykonywanie przysługujących jej praw, zwłaszcza gdy dane osobowe są zbierane bez wiedzy tej osoby.
- 116 Artykuł 13 ust. 3 lit. a) i b) dyrektywy 2016/680 upoważnia jednak ustawodawcę krajowego do ograniczenia udzielania informacji osobie, której dane dotyczą, zgodnie z ust. 2, lub do nieudzielania takich informacji „w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym, z należyтым uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej”, w szczególności aby „uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur” lub „uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar”.
- 117 Należy wreszcie zauważyć, że art. 54 dyrektywy 2016/680, który stanowi wyraz art. 47 Karty, nakłada na państwa członkowskie obowiązek określenia, że w sytuacji gdy dana osoba uważa, iż jej prawa przewidziane w przepisach przyjętych na mocy tej dyrektywy zostały naruszone ze względu na przetwarzanie jej danych osobowych dokonane z naruszeniem wspomnianych przepisów, osoba ta ma prawo do skutecznego środka prawnego.
- 118 Jak wynika z orzecznictwa, prawo do skutecznego środka prawnego, zagwarantowane w art. 47 Karty, wymaga co do zasady, by zainteresowany miał możliwość zapoznania się z powodami decyzji wydanej w stosunku do niego, co pozwoli mu na obronę jego praw w najlepszych możliwych warunkach oraz na w pełni świadome podjęcie decyzji, czy celowe jest wniesienie sprawy do właściwego sądu, a sądowi w pełni umożliwi dokonanie kontroli zgodności z prawem tej decyzji [wyrok z dnia 16 listopada 2023 r., Ligue des droits humains (Weryfikacja przetwarzania danych dokonywana przez organ nadzorczy), C-333/22, EU:C:2023:874, pkt 58].
- 119 O ile prawo to nie jest prawem bezwzględnym i zgodnie z art. 52 ust. 1 Karty dopuszcza się wprowadzenie ograniczeń tego prawa, o tyle jest tak pod warunkiem, że ograniczenia te są przewidziane w ustawie, szanują istotę tych praw i wolności oraz, w zgodzie z zasadą proporcjonalności, są one konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznanym przez Unię lub potrzebom ochrony praw i wolności innych osób [wyrok z dnia 16 listopada 2023 r., Ligue des droits humains (Weryfikacja przetwarzania danych dokonywana przez organ nadzorczy), C-333/22, EU:C:2023:874, pkt 59].
- 120 W związku z tym z przepisów przytoczonych w pkt 115–119 niniejszego wyroku wynika, że do właściwych organów krajowych, które zostały upoważnione przez sąd lub niezależny organ administracyjny do wglądu do przechowywanych danych, należy poinformowanie osób, których dane dotyczą, w ramach mających zastosowanie procedur krajowych, o powodach, na których opiera się ta zgoda, z chwilą gdy przestało to zagrażać prawidłowemu przebiegowi postępowania

przygotowawczego prowadzonego przez te organy, i udostępnienie im wszystkich informacji, o których mowa w art. 13 ust. 1 dyrektywy 2016/680. Informacje te są bowiem konieczne, aby umożliwić tym osobom skorzystanie w szczególności z prawa do środka prawnego, wyraźnie przewidzianego w art. 54 dyrektywy 2016/680 [zob. podobnie wyrok z dnia 17 listopada 2022 r., Spetsializirana prokuratura (Zatrzymywanie danych o ruchu i o lokalizacji), C-350/21, EU:C:2022:896, pkt 70 i przytoczone tam orzecznictwo].

- 121 Natomiast uregulowanie krajowe, które zasadniczo całkowicie wyklucza prawo do uzyskania takich informacji, nie jest zgodne z prawem Unii [zob. podobnie wyrok z dnia 17 listopada 2022 r., Spetsializirana prokuratura (Zatrzymywanie danych o ruchu i o lokalizacji), C-350/21, EU:C:2022:896, pkt 71].
- 122 W niniejszym wypadku z postanowienia odsyłającego wynika, że CG dowiedział się o zatrzymaniu jego telefonu komórkowego, w chwili gdy funkcjonariusze austriackiej policji podjęli nieudaną próbę jego odblokowania w celu uzyskania wglądu do przechowywanych na nim danych. W tych okolicznościach nie wydaje się, aby poinformowanie CG o próbie uzyskania wglądu do tych danych przez wspomnianych funkcjonariuszy mogło zagrażać prawidłowemu przebiegowi prowadzonego postępowania, w związku z czym powinno to być nastąpić przed podjęciem takiej próby.
- 123 Z powyższego wynika, że na pytanie trzecie należy odpowiedzieć, iż art. 13 i 54 dyrektywy 2016/680 w związku z art. 47 i z art. 52 ust. 1 Karty należy interpretować w ten sposób, że stoją one na przeszkodzie uregulowaniu krajowemu, które zezwala właściwym organom na podjęcie próby uzyskania wglądu do danych zapisanych w telefonie komórkowym bez poinformowania osoby, której dane dotyczą, w ramach mających zastosowanie procedur krajowych, o powodach, na których opiera się zgoda na wgląd do takich danych wydana przez sąd lub niezależny organ administracyjny, z chwilą gdy przekazanie tych informacji przestało zagrażać prawidłowemu wykonywaniu zadań spoczywających na tych organach na gruncie przepisów tej dyrektywy.

W przedmiocie kosztów

- 124 Dla stron w postępowaniu głównym niniejsze postępowanie ma charakter incydentalny, dotyczy bowiem kwestii podniesionej przed sądem odsyłającym, do niego zatem należy rozstrzygnięcie o kosztach. Koszty poniesione w związku z przedstawieniem uwag Trybunałowi, inne niż koszty stron w postępowaniu głównym, nie podlegają zwrotowi.

Z powyższych względów Trybunał (wielka izba) orzeka, co następuje:

- 1) Artykuł 4 ust. 1 lit. c) 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 uchyłającej decyzję ramową Rady 2008/977/WSiSW, rozpatrywany w świetle art. 7, 8 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej,

należy interpretować w ten sposób, że:

nie stoi on na przeszkodzie uregulowaniu krajowemu, które przyznaje właściwym organom możliwość uzyskania wglądu do danych zapisanych w telefonie komórkowym w celu zapobiegania przestępstwom w ogólności, ich dochodzenia, wykrywania i ścigania, pod warunkiem że owo uregulowanie:

- w wystarczająco precyzyjny sposób określa charakter lub kategorie przestępstw, których dotyczy,**
- gwarantuje poszanowanie zasady proporcjonalności oraz**
- uzależnia skorzystanie z tej możliwości, z wyjątkiem należycie uzasadnionych pilnych przypadków, od uprzedniej kontroli sądu lub niezależnego organu administracyjnego.**

2) Artykuły 13 i 54 dyrektywy 2016/680 w związku z art. 47 i z art. 52 ust. 1 Karty praw podstawowych

należy interpretować w ten sposób, że

stoją one na przeszkodzie uregulowaniu krajowemu, które zezwala właściwym organom na podjęcie próby uzyskania wglądu do danych zapisanych w telefonie komórkowym bez poinformowania osoby, której dane dotyczą, w ramach mających zastosowanie procedur krajowych, o powodach, na których opiera się zgoda na wgląd do takich danych wydana przez sąd lub niezależny organ administracyjny, z chwilą gdy przekazanie tych informacji przestało zagrażać prawidłowemu wykonywaniu zadań spoczywających na tych organach na gruncie przepisów tej dyrektywy.

Podpisy